# Contents

**Chapter 1 About Oracle Cloud Infrastructure** ................................................. 22

- Prefer Online Help? ................................................................. 24
- Need API Documentation? .......................................................... 24

**Chapter 2 Welcome to Oracle Cloud Infrastructure** .................................... 26

- Getting Started ........................................................................ 26
- About the Services ................................................................. 26
- Accessing Oracle Cloud Infrastructure ........................................ 29
- How Do I Get Started? .............................................................. 29
- Key Concepts and Terminology .................................................. 29
- Request and Manage Free Oracle Cloud Promotions .................. 32
- Buy an Oracle Cloud Subscription ........................................... 36
- Request and Manage the Oracle Startup Program ................... 38
- Understanding the Sign-In Options ........................................... 39
- Signing In to the Console .......................................................... 41
- Using the Console ................................................................. 42
- Using the Mobile App ............................................................ 49
- Changing Your Password .......................................................... 52
- Checking Your Expenses and Usage .......................................... 55
- Adding Users ........................................................................ 57
- Oracle Cloud Infrastructure Tutorials ....................................... 60
- Tutorial - Launching Your First Linux Instance ......................... 61
- Tutorial - Launching Your First Windows Instance .................. 73
- Putting Data into Object Storage .............................................. 82
- Getting Started with the Command Line Interface ................... 83
- Getting Started ....................................................................... 102
- Getting Started with Load Balancing ....................................... 103
- Getting Started with Audit ...................................................... 116
- Getting Started with Oracle Platform Services ......................... 119
- Getting Started with Oracle Applications ................................ 121
- Setting Up Your Tenancy .......................................................... 122
- Getting Help and Contacting Support ....................................... 125
- Task Mapping from My Services .............................................. 132
- Frequently Asked Questions ..................................................... 135

**Chapter 3 Oracle Cloud's Free Tier** ............................................................... 140

- Free Trial ............................................................................ 140
- Always Free Resources .......................................................... 140
- To provision your Always Free using Terraform and Resource Manager ........................................ 141
- Upgrading to a Paid Account .................................................... 141
- Additional Information ............................................................. 142
- Details of the Always Free Resources ........................................ 142
- Compute ............................................................................ 142
- Database .............................................................................. 142
- Load Balancing ..................................................................... 143
- Block Volume ........................................................................ 143
- Object Storage ...................................................................... 144
# Table of contents

- Resource Manager................................................................. 144
- Service Connector Hub........................................................... 145
- Vault..................................................................................... 145
- Frequently Asked Questions: Oracle Cloud Infrastructure Free Tier......................................................... 145
  - How do I change which resources I want to designate as Always Free?......................................................... 145
  - What happens when my Free Trial expires or my credits are used up?......................................................... 145
  - If I upgrade, do I keep my Free Trial credit balance?.................................................................................. 146
  - After I upgrade my account, can I downgrade?.......................................................................................... 146
  - My resources no longer appear. How can I restore them?.......................................................................... 146
  - I get an "out of host capacity" error when I try to create an Always Free Compute instance. What can I do?.......................................................................................................................... 146
  - Is it possible to extend my Free Trial?........................................................................................................ 146
  - Is my Free Tier account eligible for support?........................................................................................... 146

## Chapter 4 Oracle Cloud Infrastructure Government Cloud................. 148

- Oracle Cloud Infrastructure US Government Cloud....................................................................................... 148
- Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization........................................ 157
- Oracle Cloud Infrastructure US Government Cloud with DISA Impact Level 5 Authorization.................. 162
- Oracle Cloud Infrastructure United Kingdom Government Cloud........................................................................... 171
- Regions.................................................................................... 171
- Console Sign-in URLs................................................................................................................................. 171
- API Reference and Endpoints...................................................... 171
- Services Not Supported in Oracle Cloud Infrastructure United Kingdom Government Cloud..................... 175
- SMTP Authentication and Connection Endpoints........................................................................................ 175
- SPF Record Syntax.................................................................................. 176

## Chapter 5 Service Essentials.......................................................... 178

- Security Credentials............................................................................................................................... 179
- Console Password................................................................................................................................. 179
- API Signing Key................................................................................................................................. 179
- Instance SSH Key............................................................................................................................... 179
- Auth Token...................................................................................... 180
- Regions and Availability Domains........................................................................................................ 180
- About Regions and Availability Domains............................................................................................ 180
- Fault Domains................................................................................ 182
- Subscribed Region Limits.................................................................................................................. 183
- Service Availability Across Regions.................................................................................................. 183
- Resource Availability.......................................................................................................................... 184
- Dedicated Regions............................................................................................... 186
- IP Address Ranges.......................................................................................... 193
- Public IP Addresses for VCNs and the Oracle Services Network............................................................ 193
- Public IP Addresses for the Oracle YUM Repos......................................................................................... 196
- Resource Identifiers............................................................................................................................ 197
- Oracle Cloud IDs (OCIDs).................................................................................................................. 197
- Where to Find Your Tenancy's OCID.................................................................................................. 198
- Name and Description (IAM Only)..................................................................................................... 198
- Display Name................................................................................................................................. 198
- Resource Monitoring.......................................................................................................................... 199
- Prerequisites.......................................................................................... 199
- Working with Resource Monitoring.................................................................................................. 199
- Using the API.......................................................................................... 211
- Resource Tags.......................................................................................... 211
- Working with Resource Tags........................................................................ 212
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Limits</td>
<td>215</td>
</tr>
<tr>
<td>About Service Limits and Usage</td>
<td>215</td>
</tr>
<tr>
<td>Compartment Quotas</td>
<td>215</td>
</tr>
<tr>
<td>Viewing Your Service Limits, Quotas, and Usage</td>
<td>216</td>
</tr>
<tr>
<td>When You Reach a Service Limit</td>
<td>217</td>
</tr>
<tr>
<td>Requesting a Service Limit Increase</td>
<td>217</td>
</tr>
<tr>
<td>Limits by Service</td>
<td>218</td>
</tr>
<tr>
<td>Service Logs</td>
<td>235</td>
</tr>
<tr>
<td>Working with Service Logs</td>
<td>235</td>
</tr>
<tr>
<td>Using the API</td>
<td>235</td>
</tr>
<tr>
<td>Tenancy Explorer</td>
<td>235</td>
</tr>
<tr>
<td>Tenancy Explorer Highlights</td>
<td>235</td>
</tr>
<tr>
<td>Work Requests</td>
<td>236</td>
</tr>
<tr>
<td>Resources Supported by the Tenancy Explorer</td>
<td>236</td>
</tr>
<tr>
<td>Required IAM Policy to Work with Resources in the Tenancy Explorer</td>
<td>241</td>
</tr>
<tr>
<td>Navigating to the Tenancy Explorer and Viewing Resources</td>
<td>241</td>
</tr>
<tr>
<td>Filtering Displayed Resources</td>
<td>242</td>
</tr>
<tr>
<td>Opening the Resource Details Page</td>
<td>242</td>
</tr>
<tr>
<td>Moving Resources to a Different Compartment</td>
<td>242</td>
</tr>
<tr>
<td>Deleting Resources</td>
<td>243</td>
</tr>
<tr>
<td>Using the API</td>
<td>243</td>
</tr>
<tr>
<td>Compartment Quotas</td>
<td>243</td>
</tr>
<tr>
<td>About Compartment Quotas</td>
<td>243</td>
</tr>
<tr>
<td>Using the Console</td>
<td>245</td>
</tr>
<tr>
<td>Available Quotas by Service</td>
<td>246</td>
</tr>
<tr>
<td>Work Requests</td>
<td>258</td>
</tr>
<tr>
<td>Required IAM Policy</td>
<td>259</td>
</tr>
<tr>
<td>Work Request States</td>
<td>259</td>
</tr>
<tr>
<td>Using the Console to View Work Requests</td>
<td>260</td>
</tr>
<tr>
<td>Using the API</td>
<td>260</td>
</tr>
<tr>
<td>Console Announcements</td>
<td>260</td>
</tr>
<tr>
<td>Types of Announcements</td>
<td>261</td>
</tr>
<tr>
<td>Required IAM Policy</td>
<td>261</td>
</tr>
<tr>
<td>Email Delivery</td>
<td>261</td>
</tr>
<tr>
<td>Viewing Announcements</td>
<td>262</td>
</tr>
<tr>
<td>Using the Command Line Interface (CLI)</td>
<td>263</td>
</tr>
<tr>
<td>Using the API</td>
<td>265</td>
</tr>
<tr>
<td>Prerequisites for Oracle Platform Services on Oracle Cloud Infrastructure</td>
<td>265</td>
</tr>
<tr>
<td>Accessing Oracle Cloud Infrastructure</td>
<td>265</td>
</tr>
<tr>
<td>Required Identity and Access Management (IAM) Policy</td>
<td>265</td>
</tr>
<tr>
<td>Resources Created in Your Tenancy by Oracle</td>
<td>266</td>
</tr>
<tr>
<td>Prerequisites for Oracle Platform Services</td>
<td>266</td>
</tr>
<tr>
<td>Setting Up the Prerequisites</td>
<td>266</td>
</tr>
<tr>
<td>Information About Supported Platform Services</td>
<td>271</td>
</tr>
<tr>
<td>Renaming a Cloud Account</td>
<td>272</td>
</tr>
<tr>
<td>Billing and Payments</td>
<td>273</td>
</tr>
<tr>
<td>Budgets Overview</td>
<td>274</td>
</tr>
<tr>
<td>Cost and Usage Reports Overview</td>
<td>278</td>
</tr>
<tr>
<td>Cost Analysis Overview</td>
<td>282</td>
</tr>
<tr>
<td>Unified Billing Overview</td>
<td>296</td>
</tr>
<tr>
<td>My Services Use Cases</td>
<td>300</td>
</tr>
<tr>
<td>Service Discovery Use Case</td>
<td>300</td>
</tr>
<tr>
<td>Exadata Use Cases</td>
<td>303</td>
</tr>
<tr>
<td>Managing Exadata Instances</td>
<td>314</td>
</tr>
<tr>
<td>Using Access Token Authorization with My Services API</td>
<td>328</td>
</tr>
</tbody>
</table>
# Table of contents

## Chapter 6 API Gateway

- API Gateway
  - Ways to Access Oracle Cloud Infrastructure
  - Resource Identifiers
  - Authentication and Authorization
  - API Gateway Capabilities and Limits
  - Required IAM Service Policy
  - API Gateway Concepts
  - Preparing for API Gateway
  - Creating an API Gateway
  - Creating an API Resource with an API Description
  - Creating an API Deployment Specification
  - Deploying an API on an API Gateway by Creating an API Deployment
  - Setting Up Custom Domains and TLS Certificates
  - Adding Path Parameters and Wildcards to Route Paths
  - Adding Context Variables to Policies and HTTP Back End Definitions
  - Calling an API Deployed on an API Gateway
  - Listing API Gateways and API Deployments
  - Updating API Gateways and API Deployments
  - Moving API Gateways and API Deployments Between Compartments
  - Deleting API Gateways and API Deployments
  - Adding Logging to API Deployments
  - Adding an HTTP or HTTPS URL as an API Gateway Back End
  - Adding a Function in Oracle Functions as an API Gateway Back End
  - Adding Stock Responses as an API Gateway Back End
  - Adding Request Policies and Response Policies to API Deployment Specifications
  - Limiting the Number of Requests to API Gateway Back Ends
  - Adding CORS support to API Deployments
  - Adding Authentication and Authorization to API Deployments
  - Transforming Incoming Requests and Outgoing Responses
  - Troubleshooting API Gateway
  - API Gateway Internal Limits
  - API Gateway Metrics

## Chapter 7 Archive Storage

- Archive Storage
  - Using Archive Storage
  - Ways to Access Archive Storage
  - Authentication and Authorization
  - WORM Compliance
  - Limits on Archive Storage Resources

## Chapter 8 Audit

- Audit
  - Version 2 Audit Log Schema
  - Ways to Access Oracle Cloud Infrastructure
  - Authentication and Authorization
  - Contents of an Audit Log Event
  - Viewing Audit Log Events
  - Bulk Export of Audit Log Events
# Table of contents

## Chapter 9 Block Volume........................................................................................................... 500

*Block Volume................................................................. 500*

- Typical Block Volume Scenarios.................................................. 500
- Volume Attachment Types.......................................................... 501
- Volume Access Types............................................................... 502
- Device Paths............................................................................. 502
- Regions and Availability Domains.............................................. 502
- Resource Identifiers................................................................. 503
- Ways to Access Oracle Cloud Infrastructure............................ 503
- Authentication and Authorization.............................................. 503
- Monitoring Resources.............................................................. 503
- Moving Resources................................................................. 503
- Tagging Resources................................................................. 503
- Creating Automation with Events........................................... 504
- Block Volume Encryption.......................................................... 504
- Block Volume Data Eradication................................................ 504
- Block Volume Performance...................................................... 504
- Block Volume Durability........................................................... 505
- Block Volume Capabilities and Limits...................................... 505
- iSCSI Information...................................................................... 505
- Volume Groups......................................................................... 506
- Creating a Volume................................................................. 515
- Attaching a Volume............................................................... 517
- Attaching a Volume to Multiple Instances.............................. 520
- Connecting To a Volume......................................................... 524
- Listing Volumes....................................................................... 529
- Listing Volume Attachments..................................................... 530
- Renaming a Volume............................................................... 530
- Editing a Volume's Settings..................................................... 531
- Resizing a Volume................................................................. 532
- Overview of Block Volume Backups....................................... 540
- Cloning a Volume..................................................................... 560
- Disconnecting From a Volume.................................................. 562
- Detaching a Volume............................................................... 563
- Deleting a Volume.................................................................... 563
- Move Block Volume Resources Between Compartments........ 564
- Block Volume Performance...................................................... 567
- Block Volume Metrics............................................................. 585

## Chapter 10 Compliance Documents...................................................................................... 588

*Compliance Documents........................................................... 588*

- Types of Compliance Documents.............................................. 588
- Types of Environments......................................................... 588
- Regions and Availability Domains............................................ 588
- Ways to Access Oracle Cloud Infrastructure............................ 589
- Viewing and Downloading Compliance Documents.................. 589

## Chapter 11 Compute.............................................................................................................. 590

*Compute................................................................. 590*

- Instance Types........................................................................ 590
- Components for Launching Instances..................................... 591
- Creating Automation with Events........................................... 592
Table of contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Identifiers</td>
<td>592</td>
</tr>
<tr>
<td>Work Requests</td>
<td>592</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>592</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>593</td>
</tr>
<tr>
<td>Storage for Compute Instances</td>
<td>593</td>
</tr>
<tr>
<td>Limits on Compute Resources</td>
<td>593</td>
</tr>
<tr>
<td>Best Practices for Your Compute Instance</td>
<td>594</td>
</tr>
<tr>
<td>Protecting Data on NVMe Devices</td>
<td>601</td>
</tr>
<tr>
<td>Boot Volumes</td>
<td>609</td>
</tr>
<tr>
<td>Oracle-Provided Images</td>
<td>629</td>
</tr>
<tr>
<td>Compute Shapes</td>
<td>655</td>
</tr>
<tr>
<td>Installing and Running Oracle Ksplice</td>
<td>664</td>
</tr>
<tr>
<td>Managing Custom Images</td>
<td>665</td>
</tr>
<tr>
<td>Image Import/Export</td>
<td>670</td>
</tr>
<tr>
<td>Bring Your Own Image (BYOI)</td>
<td>675</td>
</tr>
<tr>
<td>Configuring Image Capabilities for Custom Images</td>
<td>687</td>
</tr>
<tr>
<td>OS Kernel Updates</td>
<td>691</td>
</tr>
<tr>
<td>Managing Key Pairs on Linux Instances</td>
<td>693</td>
</tr>
<tr>
<td>Creating an Instance</td>
<td>695</td>
</tr>
<tr>
<td>Managing Compute Instances</td>
<td>708</td>
</tr>
<tr>
<td>Autoscaling</td>
<td>718</td>
</tr>
<tr>
<td>Managing Cluster Networks</td>
<td>726</td>
</tr>
<tr>
<td>Dedicated Virtual Machine Hosts</td>
<td>729</td>
</tr>
<tr>
<td>Connecting to an Instance</td>
<td>733</td>
</tr>
<tr>
<td>Adding Users on an Instance</td>
<td>737</td>
</tr>
<tr>
<td>Displaying the Console for an Instance</td>
<td>739</td>
</tr>
<tr>
<td>Managing Plugins with Oracle Cloud Agent</td>
<td>740</td>
</tr>
<tr>
<td>Running Commands on an Instance</td>
<td>752</td>
</tr>
<tr>
<td>Getting Instance Metadata</td>
<td>757</td>
</tr>
<tr>
<td>Updating Instance Metadata</td>
<td>764</td>
</tr>
<tr>
<td>Editing an Instance</td>
<td>765</td>
</tr>
<tr>
<td>Moving a Compute Instance to a New Host</td>
<td>775</td>
</tr>
<tr>
<td>Moving Compute Resources to a Different Compartment</td>
<td>777</td>
</tr>
<tr>
<td>Stopping and Starting an Instance</td>
<td>779</td>
</tr>
<tr>
<td>Terminating an Instance</td>
<td>783</td>
</tr>
<tr>
<td>Enabling Monitoring for Compute Instances</td>
<td>783</td>
</tr>
<tr>
<td>Compute Metrics</td>
<td>788</td>
</tr>
<tr>
<td>Compute NVMe Performance</td>
<td>799</td>
</tr>
<tr>
<td>Compute Health Monitoring for Bare Metal Instances</td>
<td>801</td>
</tr>
<tr>
<td>Microsoft Licensing on Oracle Cloud Infrastructure</td>
<td>803</td>
</tr>
<tr>
<td>Troubleshooting Compute Instances</td>
<td>813</td>
</tr>
<tr>
<td>Updating the Linux iSCSI Service to Restart Automatically</td>
<td>828</td>
</tr>
</tbody>
</table>

Chapter 12 Container Engine .............................................................................. 832

Container Engine ............................................................................................... 832
Ways to Access Oracle Cloud Infrastructure .................................................. 832
Creating Automation with Events ........................................................................ 832
Resource Identifiers ......................................................................................... 833
Authentication and Authorization ........................................................................ 833
Container Engine for Kubernetes Capabilities and Limits .............................. 833
Required IAM Service Policy .............................................................................. 833
Container Engine and Kubernetes Concepts .................................................... 833
Preparing for Container Engine for Kubernetes .............................................. 835
Creating a Kubernetes Cluster ........................................................................... 871
Setting Up Cluster Access .................................................................................. 876
### Table of contents

Modifying Kubernetes Cluster Properties.......................................................... 881
Modifying Node Pool and Worker Node Properties........................................ 883
Updating Worker Nodes by Creating a New Node Pool................................. 885
Deleting a Kubernetes Cluster........................................................................... 885
Monitoring Clusters.......................................................................................... 886
Viewing Work Requests and Kubernetes API Server Audit Logs.................. 888
Viewing Application Logs on Worker Nodes.................................................. 888
Accessing a Cluster Using Kubectl................................................................. 890
Accessing a Cluster Using the Kubernetes Dashboard..................................... 891
Adding a Service Account Authentication Token to a Kubeconfig File........... 894
Deploying a Sample Nginx App on a Cluster Using Kubectl......................... 896
Pulling Images from Registry during Deployment......................................... 897
Supported Labels for Different Usecases......................................................... 898
Encrypting Kubernetes Secrets at Rest in Etcd.............................................. 900
Connecting to Worker Nodes Using SSH....................................................... 903
Using Pod Security Polices with Container Engine for Kubernetes.............. 905
Autoscaling Kubernetes Clusters..................................................................... 910
About Access Control and Container Engine for Kubernetes......................... 920
Supported Images (Including Custom Images) and Shapes for Worker Nodes... 923
Supported Admission Controllers................................................................. 924
Kubernetes Versions and Container Engine for Kubernetes......................... 926
Supported Versions of Kubernetes................................................................. 926
Upgrading Clusters to Newer Kubernetes Versions....................................... 929
Configuring DNS Servers for Kubernetes Clusters....................................... 932
Creating Load Balancers to Distribute Traffic Between Cluster Nodes.......... 937
Creating a Persistent Volume Claim............................................................... 947
Adding OCI Service Broker for Kubernetes to Clusters............................... 952
Example: Setting Up an Ingress Controller on a Cluster.............................. 953
Example: Installing Calico and Setting Up Network Policies......................... 960
Frequently Asked Questions About Container Engine for Kubernetes........... 962
Container Engine for Kubernetes Metrics................................................... 963

### Chapter 13 Data Transfer............................................................................. 968

Data Transfer.................................................................................................. 968
Supported Regions......................................................................................... 968
Limits on Data Transfer Service Resources.................................................. 969
Tagging Resources......................................................................................... 969
Automation for Objects Using the Events Service........................................ 969
Notifications................................................................................................. 969
Inputting Text into Data Transfer................................................................... 969
What's Next..................................................................................................... 969
Data Import - Disk......................................................................................... 970
Data Import - Appliance................................................................................. 1015
Data Export................................................................................................... 1082
Troubleshooting............................................................................................ 1122
Help Sheets.................................................................................................... 1127

### Chapter 14 Database.................................................................................. 1140

Database......................................................................................................... 1140
License Types and Bring Your Own License (BYOL) Availability................ 1140
Always Free Database Resources................................................................. 1141
Moving Database Resources to a Different Compartment........................... 1141
Monitoring Resources................................................................................... 1142
Creating Automation with Events............................................................... 1142
### Table of contents

<table>
<thead>
<tr>
<th>Chapter 15 DNS and Traffic Management</th>
<th>1674</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS and Traffic Management</td>
<td>1674</td>
</tr>
<tr>
<td>DNS</td>
<td>1674</td>
</tr>
<tr>
<td>Traffic Management</td>
<td>1705</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 16 Email Delivery</th>
<th>1738</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Delivery</td>
<td>1738</td>
</tr>
<tr>
<td>Email Delivery Service Components</td>
<td>1738</td>
</tr>
<tr>
<td>Regions and Availability Domains</td>
<td>1739</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>1739</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>1739</td>
</tr>
<tr>
<td>SMTP Authentication and Connection Endpoints</td>
<td>1740</td>
</tr>
<tr>
<td>Monitoring Resources</td>
<td>1741</td>
</tr>
<tr>
<td>Email Delivery Service Capabilities and Limits</td>
<td>1741</td>
</tr>
<tr>
<td>Required IAM Service Policy</td>
<td>1742</td>
</tr>
<tr>
<td>Dedicated IP Addresses</td>
<td>1742</td>
</tr>
<tr>
<td>Tagging Resources</td>
<td>1743</td>
</tr>
<tr>
<td>Integration with Oracle Cloud Infrastructure Services</td>
<td>1743</td>
</tr>
<tr>
<td>Getting Started with Email Delivery</td>
<td>1743</td>
</tr>
<tr>
<td>Generate SMTP Credentials for a User</td>
<td>1743</td>
</tr>
<tr>
<td>Managing Approved Senders</td>
<td>1750</td>
</tr>
<tr>
<td>Configure SPF</td>
<td>1752</td>
</tr>
<tr>
<td>Managing the Suppression List</td>
<td>1755</td>
</tr>
<tr>
<td>Email Delivery Metrics</td>
<td>1756</td>
</tr>
<tr>
<td>Integrating Oracle Application Express with Email Delivery</td>
<td>1758</td>
</tr>
<tr>
<td>Integrating Postfix with Email Delivery</td>
<td>1759</td>
</tr>
<tr>
<td>Integrating Oracle Enterprise Manager with Email Delivery</td>
<td>1760</td>
</tr>
<tr>
<td>Integrating Mailx with Email Delivery</td>
<td>1761</td>
</tr>
<tr>
<td>Integrating Swaks with Email Delivery</td>
<td>1763</td>
</tr>
<tr>
<td>Integrating JavaMail with Email Delivery</td>
<td>1764</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resource Identifiers</th>
<th>1142</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>1142</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>1142</td>
</tr>
<tr>
<td>Security Zone Integration</td>
<td>1143</td>
</tr>
<tr>
<td>Limits on the Database Service</td>
<td>1143</td>
</tr>
<tr>
<td>Work Requests Integration</td>
<td>1143</td>
</tr>
<tr>
<td>Getting Oracle Support Help for Your Database Resources</td>
<td>1149</td>
</tr>
<tr>
<td>Autonomous Databases</td>
<td>1149</td>
</tr>
<tr>
<td>Exadata Cloud Service</td>
<td>1221</td>
</tr>
<tr>
<td>Bare Metal and Virtual Machine DB Systems</td>
<td>1352</td>
</tr>
<tr>
<td>External Database Service</td>
<td>1558</td>
</tr>
<tr>
<td>Oracle Database Software Images</td>
<td>1567</td>
</tr>
<tr>
<td>Oracle Maximum Availability Architecture in Oracle Cloud Infrastructure</td>
<td>1569</td>
</tr>
<tr>
<td>Security Zone Integration</td>
<td>1574</td>
</tr>
<tr>
<td>DB System Time Zone</td>
<td>1575</td>
</tr>
<tr>
<td>Database Metrics</td>
<td>1578</td>
</tr>
<tr>
<td>Using the Oracle Database Service Overview to Manage Resources</td>
<td>1594</td>
</tr>
<tr>
<td>Using Performance Hub to Analyze Database Performance</td>
<td>1597</td>
</tr>
<tr>
<td>Migrating Databases to the Cloud</td>
<td>1607</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>1645</td>
</tr>
<tr>
<td>Deprecated Database Service APIs</td>
<td>1672</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deprecated Database Service APIs</th>
<th>1672</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bare Metal and Virtual Machine DB Systems</td>
<td>1352</td>
</tr>
<tr>
<td>Exadata Cloud Service</td>
<td>1221</td>
</tr>
<tr>
<td>Getting Oracle Support Help for Your Database Resources</td>
<td>1149</td>
</tr>
<tr>
<td>Autonomous Databases</td>
<td>1149</td>
</tr>
<tr>
<td>Resource Identifiers</td>
<td>1142</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>1142</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>1142</td>
</tr>
<tr>
<td>Security Zone Integration</td>
<td>1143</td>
</tr>
<tr>
<td>Limits on the Database Service</td>
<td>1143</td>
</tr>
<tr>
<td>Work Requests Integration</td>
<td>1143</td>
</tr>
<tr>
<td>Integrating JavaMail with Email Delivery</td>
<td>1764</td>
</tr>
</tbody>
</table>
## Table of contents

<table>
<thead>
<tr>
<th>Chapter 19 Functions</th>
<th>2032</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>2032</td>
</tr>
<tr>
<td>Creating Automation with Events</td>
<td>2033</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 18 File Storage</th>
<th>1920</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Automation with Events</td>
<td>1948</td>
</tr>
<tr>
<td>Mounting File Systems</td>
<td>1954</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 17 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Automation with Events</td>
<td>2033</td>
</tr>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 16 Events</th>
<th>1817</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 15 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 14 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 1 Events</th>
<th>1784</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting Your File System</td>
<td>2010</td>
</tr>
<tr>
<td>File System Usage and Metering</td>
<td>2007</td>
</tr>
<tr>
<td>Paths in File Systems</td>
<td>2006</td>
</tr>
<tr>
<td>File System Metrics</td>
<td>1997</td>
</tr>
<tr>
<td>Using File Storage Parallel Tools</td>
<td>1994</td>
</tr>
<tr>
<td>Managing Snapshots</td>
<td>1990</td>
</tr>
<tr>
<td>Managing Mount Targets</td>
<td>1980</td>
</tr>
<tr>
<td>Managing File Systems</td>
<td>1970</td>
</tr>
<tr>
<td>Creating File Systems</td>
<td>1948</td>
</tr>
<tr>
<td>about Security</td>
<td>1925</td>
</tr>
<tr>
<td>Chapter 20 Health Checks</td>
<td>2112</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Health Checks Service Components</td>
<td>2112</td>
</tr>
<tr>
<td>Ways to Access the Health Checks Service</td>
<td>2112</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>2113</td>
</tr>
<tr>
<td>Health Checks Service Capabilities and Limits</td>
<td>2113</td>
</tr>
<tr>
<td>Required IAM Service Policy</td>
<td>2113</td>
</tr>
<tr>
<td>Moving Health Checks to a Different Compartment</td>
<td>2113</td>
</tr>
<tr>
<td>Tagging Resources</td>
<td>2113</td>
</tr>
<tr>
<td>Getting Started With the Health Checks API</td>
<td>2114</td>
</tr>
<tr>
<td>Managing Health Checks</td>
<td>2118</td>
</tr>
<tr>
<td>Health Checks Metrics</td>
<td>2121</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 21 IAM</th>
<th>2124</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>2124</td>
</tr>
<tr>
<td>Components of IAM</td>
<td>2124</td>
</tr>
<tr>
<td>Services You Can Control Access To</td>
<td>2125</td>
</tr>
<tr>
<td>The Administrators Group and Policy</td>
<td>2125</td>
</tr>
<tr>
<td>Example Scenario</td>
<td>2126</td>
</tr>
<tr>
<td>Viewing Resources by Compartment in the Console</td>
<td>2134</td>
</tr>
<tr>
<td>The Scope of IAM Resources</td>
<td>2134</td>
</tr>
<tr>
<td>Creating Automation with Events</td>
<td>2134</td>
</tr>
<tr>
<td>Resource Identifiers</td>
<td>2134</td>
</tr>
</tbody>
</table>
Chapter 22 Load Balancing ................................................................. 2480

Load Balancing .................................................................................. 2480
How Load Balancing Works.............................................................. 2480
Load Balancing Concepts................................................................. 2483
Resource Identifiers........................................................................ 2487
Ways to Access Oracle Cloud Infrastructure................................. 2487
Monitoring Resources.................................................................... 2487
Authentication and Authorization...................................................... 2488
Limits on Load Balancing Resources.............................................. 2488
How Load Balancing Policies Work............................................... 2488
Connection Management............................................................... 2489
HTTP "X-" Headers.......................................................................... 2490
Session Persistence........................................................................ 2491
Managing Load Balancers.............................................................. 2494
Managing Backend Sets................................................................. 2510
Managing Backend Servers........................................................... 2515
Managing Listeners....................................................................... 2522
Managing Cipher Suites............................................................... 2525
Managing Request Routing........................................................... 2534
Managing Rule Sets...................................................................... 2541
Managing SSL Certificates............................................................ 2551
Editing Health Check Policies......................................................... 2558
Viewing the State of a Work Request........................................... 2565
Load Balancing Metrics................................................................. 2567

Chapter 23 Logging.............................................................................. 2574
# Table of contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logging</strong></td>
<td>2574</td>
</tr>
<tr>
<td>How Logging Works</td>
<td>2574</td>
</tr>
<tr>
<td>Logging Concepts</td>
<td>2575</td>
</tr>
<tr>
<td>Limits on Logging</td>
<td>2576</td>
</tr>
<tr>
<td>Resource Identifiers</td>
<td>2576</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>2576</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>2576</td>
</tr>
<tr>
<td>Managing Logs and Log Groups</td>
<td>2577</td>
</tr>
<tr>
<td>Service Logs</td>
<td>2591</td>
</tr>
<tr>
<td>Audit Logs</td>
<td>2617</td>
</tr>
<tr>
<td>Custom Logs</td>
<td>2619</td>
</tr>
<tr>
<td>Searching Logs</td>
<td>2634</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 24 Marketplace</strong></td>
<td>2650</td>
</tr>
<tr>
<td>Marketplace</td>
<td>2650</td>
</tr>
<tr>
<td>Resource Identifiers</td>
<td>2650</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>2650</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>2650</td>
</tr>
<tr>
<td>Working with Listings</td>
<td>2651</td>
</tr>
<tr>
<td>Publishing Listings</td>
<td>2657</td>
</tr>
<tr>
<td>Viewing Accepted Terms of Use Agreements</td>
<td>2657</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 25 Monitoring</strong></td>
<td>2660</td>
</tr>
<tr>
<td>Monitoring</td>
<td>2660</td>
</tr>
<tr>
<td>How Monitoring Works</td>
<td>2660</td>
</tr>
<tr>
<td>Monitoring Concepts</td>
<td>2665</td>
</tr>
<tr>
<td>Availability</td>
<td>2669</td>
</tr>
<tr>
<td>Supported Services</td>
<td>2669</td>
</tr>
<tr>
<td>Resource Identifiers</td>
<td>2670</td>
</tr>
<tr>
<td>Ways to Access Monitoring</td>
<td>2670</td>
</tr>
<tr>
<td>Moving Alarms to a Different Compartment</td>
<td>2670</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>2671</td>
</tr>
<tr>
<td>Limits on Monitoring</td>
<td>2671</td>
</tr>
<tr>
<td>Viewing Default Metric Charts</td>
<td>2671</td>
</tr>
<tr>
<td>Building Metric Queries</td>
<td>2700</td>
</tr>
<tr>
<td>Publishing Custom Metrics</td>
<td>2717</td>
</tr>
<tr>
<td>Managing Alarms</td>
<td>2719</td>
</tr>
<tr>
<td>Best Practices for Your Alarms</td>
<td>2739</td>
</tr>
<tr>
<td>Monitoring Query Language (MQL) Reference</td>
<td>2741</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 26 Networking</strong></td>
<td>2746</td>
</tr>
<tr>
<td>Networking</td>
<td>2746</td>
</tr>
<tr>
<td>Features</td>
<td>2746</td>
</tr>
<tr>
<td>Networking Overview</td>
<td>2748</td>
</tr>
<tr>
<td>Networking Scenarios</td>
<td>2756</td>
</tr>
<tr>
<td>Virtual Networking Quickstart</td>
<td>2820</td>
</tr>
<tr>
<td>VCNs and Subnets</td>
<td>2821</td>
</tr>
<tr>
<td>Access and Security</td>
<td>2830</td>
</tr>
<tr>
<td>Virtual Network Interface Cards (VNICs)</td>
<td>2855</td>
</tr>
<tr>
<td>IP Addresses and DNS in Your VCN</td>
<td>2864</td>
</tr>
<tr>
<td>DHCP Options</td>
<td>2917</td>
</tr>
<tr>
<td>Route Tables</td>
<td>2921</td>
</tr>
<tr>
<td>Dynamic Routing Gateways (DRGs)</td>
<td>2927</td>
</tr>
</tbody>
</table>
Table of contents

Chapter 27 Notifications.................................................................3350
Notifications..................................................................................3350
How Notifications Works..............................................................3350
Notifications Concepts.................................................................3350
Flow of Message Publication.........................................................3353
Availability....................................................................................3354
Service Comparison for Sending Email Messages.......................3354
Resource Identifiers.......................................................................3355
Moving Topics and Subscriptions to a Different Compartment.....3355
Ways to Access Notifications.........................................................3355
Authentication and Authorization..................................................3355
Limits on Notifications.................................................................3356
Best Practices for Your Subscriptions and Topics........................3356
Managing Topics and Subscriptions..............................................3356
Publishing Messages....................................................................3365
Scenarios.......................................................................................3366
Troubleshooting Notifications......................................................3385
Notifications Metrics....................................................................3389

Chapter 28 Object Storage............................................................3392
Object Storage..............................................................................3392
Object Storage Resources.............................................................3392
Object Storage Features...............................................................3393
Ways to Access Object Storage....................................................3393
Using Object Storage.................................................................3394
Authentication and Authorization..................................................3394
Blocking Access to Object Storage Resources from Unauthorized IP Addresses.................................3395
Object Storage IP Addresses........................................................3395
Limits on Object Storage Resources..............................................3395
Understanding Object Storage Namespaces.................................3395
Understanding Storage Tiers........................................................3396
Managing Buckets.......................................................................3398
Managing Objects.......................................................................3419
Using Replication.......................................................................3440
Using Object Versioning..............................................................3446
Using Retention Rules to Preserve Data.........................................3458
Using Object Lifecycle Management...........................................3466
Using Multipart Uploads...............................................................3477
Using Pre-Authenticated Requests..............................................3482
Copying Objects.........................................................................3487
Using Your Own Keys for Server-Side Encryption........................3491
### Table of contents

Amazon S3 Compatibility API.................................................................................................................. 3493
Designating Compartments for the Amazon S3 Compatibility and Swift APIs........................................ 3497
Object Storage Metrics.......................................................................................................................... 3499
Accessing Object Storage Resources Across Tenancies...................................................................... 3503
Hadoop Support.................................................................................................................................... 3505

**Chapter 29 Registry** .......................................................................................................................... 3506

- Registry..................................................................................................................................................... 3506
- Ways to Access Oracle Cloud Infrastructure...................................................................................... 3506
- Resource Identifiers.............................................................................................................................. 3507
- Authentication and Authorization........................................................................................................ 3507
- Registry Capabilities and Limits........................................................................................................... 3507
- Required IAM Service Policy................................................................................................................ 3507
- Preparing for Registry........................................................................................................................ 3507
- Registry Concepts................................................................................................................................ 3509
- Creating a Repository......................................................................................................................... 3512
- Pushing Images Using the Docker CLI.............................................................................................. 3513
- Pulling Images Using the Docker CLI................................................................................................ 3516
- Pulling Images from Registry during Kubernetes Deployment...................................................... 3518
- Viewing Images and Image Details.................................................................................................... 3519
- Deleting and Undeleting an Image...................................................................................................... 3520
- Untagging Images.................................................................................................................................. 3521
- Retaining and Deleting Images Using Retention Policies................................................................. 3522
- Deleting a Repository....................................................................................................................... 3525
- Moving Repositories Between Compartments.................................................................................. 3526
- Getting an Auth Token....................................................................................................................... 3527
- Policies to Control Repository Access............................................................................................ 3527

**Chapter 30 Resource Manager** ........................................................................................................ 3532

- Resource Manager............................................................................................................................ 3532
- Features................................................................................................................................................ 3532
- Overview of Resource Manager....................................................................................................... 3534
- Getting Started.................................................................................................................................... 3541
- Managing Stacks and Jobs.................................................................................................................. 3557
- Managing Private Templates.............................................................................................................. 3578
- Managing Configuration Source Providers..................................................................................... 3581
- Using Remote Exec............................................................................................................................ 3586
- Templates............................................................................................................................................. 3588
- Using the Deploy to Oracle Cloud Button......................................................................................... 3592
- Terraform Configurations for Resource Manager........................................................................... 3594
- GitHub and GitLab Connection Issues............................................................................................. 3624

**Chapter 31 Search** ............................................................................................................................. 3626

- Search.................................................................................................................................................... 3626
- Search Categories and Ways to Search Them.................................................................................... 3626
- Supported Resources......................................................................................................................... 3626
- Required IAM Permissions................................................................................................................ 3632
- Free Text Search.............................................................................................................................. 3632
- Search Language Syntax.................................................................................................................... 3633
- Sample Queries.................................................................................................................................. 3639
- Querying Resources, Services, and Documentation...................................................................... 3642
- Troubleshooting Search..................................................................................................................... 3647
# Table of contents

**Chapter 32 Security Zones** .............................................................................................................. 3648  
  Security Zones .................................................................................................................................. 3648  
  Managing Security Zones .................................................................................................................... 3649  
  Managing Recipes ............................................................................................................................... 3650  
  Security Zone Policies .......................................................................................................................... 3651  
  Security Zone IAM Policies ................................................................................................................. 3655  

**Chapter 33 Security** ........................................................................................................................................ 3656  
  Oracle Cloud Infrastructure Security Guide .......................................................................................... 3656  
  Security Overview ............................................................................................................................... 3657  
  Security Services and Features ......................................................................................................... 3663  
  Oracle Cloud Testing Policies ............................................................................................................. 3669  
  Security Best Practices ....................................................................................................................... 3673  
  Addressing Basic Configuration Issues ............................................................................................... 3754  
  Oracle Cloud Security Response to Intel L1TF Vulnerabilities .......................................................... 3725  
  Oracle Cloud Infrastructure .................................................................................................................. 3726  
  Oracle Cloud Infrastructure Classic and Oracle Platform Service on Oracle Cloud Infrastructure Classic ........................................................................................................................... 3726  
  Oracle Cloud Infrastructure Customer Advisory for L1TF Impact on the Compute Service ............ 3726  
  Oracle Cloud Infrastructure Customer Advisory for L1TF Impact on the Database Service ............... 3730  
  Oracle Cloud Security Response to Intel Microarchitectural Data Sampling (MDS) Vulnerabilities ....... 3731  
  Oracle Cloud Infrastructure .................................................................................................................. 3731  
  Oracle Cloud Infrastructure Classic and Oracle Platform Service on Oracle Cloud Infrastructure Classic ........................................................................................................................... 3731  
  Oracle Cloud Infrastructure Customer Advisory for MDS Impact on the Compute Service ............... 3732  
  Oracle Cloud Infrastructure Customer Advisory for MDS Impact on the Database Service ............... 3735  

**Chapter 34 Security Advisor** .............................................................................................................. 3738  
  Security Advisor ............................................................................................................................... 3738  
  Authentication and Authorization ....................................................................................................... 3738  
  Regions and Availability Domains ...................................................................................................... 3739  
  Limits on Resources ............................................................................................................................ 3739  
  Creating a Secure Bucket ..................................................................................................................... 3739  
  Creating a Secure File System ............................................................................................................. 3741  
  Creating a Secure Virtual Machine Instance ..................................................................................... 3744  
  Creating a Secure Block Volume ....................................................................................................... 3747  

**Chapter 35 Service Connector Hub** ................................................................................................. 3750  
  Service Connector Hub ....................................................................................................................... 3750  
  How Service Connector Hub Works ................................................................................................... 3750  
  Service Connector Hub Concepts ........................................................................................................ 3750  
  Flow of Data ....................................................................................................................................... 3750  
  Availability ......................................................................................................................................... 3751  
  Resource Identifiers ............................................................................................................................ 3751  
  Ways to Access Service Connector Hub ............................................................................................. 3751  
  Authentication and Authorization ....................................................................................................... 3751  
  Limits on Service Connector Hub ....................................................................................................... 3754  
  Managing Service Connectors ........................................................................................................... 3754  
  Service Connector Hub Scenarios ...................................................................................................... 3762  
  Troubleshooting Service Connectors .................................................................................................. 3775  
  Viewing the State of a Work Request ................................................................................................. 3777
### Chapter 36 Storage Gateway ................................................................. 3790

- Storage Gateway
- Availability
- Storage Gateway and Oracle Cloud Infrastructure Concepts
- How Storage Gateway Works
- Recommended Uses and Workloads
- Uses and Workloads Not Supported
- Security Considerations
- Limits on Storage Gateway Resources
- Storage Gateway Release Notes
- Features of Storage Gateway
- Getting Started With Storage Gateway
- Configuring the Cache for File Systems
- Understanding Storage Gateway Performance
- Interacting With Object Storage
- Installing Storage Gateway
- Logging In to the Storage Gateway Management Console
- Creating Your First File System
- Managing File Systems
- Managing Storage Gateway
- Using Storage Gateway File Management Operations
- Monitoring Storage Gateway
- Using Storage Gateway Cloud Sync
- Best Practices for Using Storage Gateway
- Troubleshooting Storage Gateway
- Upgrading Storage Gateway
- Uninstalling Storage Gateway
- Getting Help with Storage Gateway

### Chapter 37 Streaming .............................................................................. 3852

- Streaming
- About Streaming
- Streaming Concepts
- Streaming Features
- Ways to Access Streaming
- Using Streaming
- Authentication and Authorization
- Limits on Streaming Resources
- Managing Streams
- Managing Stream Pools
- Publishing Messages
- Consuming Messages
- Using Streaming with Apache Kafka
- Using Oracle Cloud Infrastructure SDKs with Streaming
- Accessing Streaming Resources Across Tenancies
- Streaming Metrics
- Troubleshooting Streaming

### Chapter 38 Tagging .................................................................................. 3906
## Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tagging</td>
<td>3906</td>
</tr>
<tr>
<td>How Tagging Works</td>
<td>3906</td>
</tr>
<tr>
<td>Tagging Concepts</td>
<td>3907</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>3908</td>
</tr>
<tr>
<td>Region Availability</td>
<td>3908</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>3908</td>
</tr>
<tr>
<td>Limits on Tags</td>
<td>3908</td>
</tr>
<tr>
<td>Resources That Can Be Tagged</td>
<td>3909</td>
</tr>
<tr>
<td>Managing Tags and Tag Namespaces</td>
<td>3913</td>
</tr>
<tr>
<td>Using Cost-Tracking Tags</td>
<td>3923</td>
</tr>
<tr>
<td>Using Predefined Values</td>
<td>3924</td>
</tr>
<tr>
<td>Using Tag Variables</td>
<td>3926</td>
</tr>
<tr>
<td>Managing Tag Defaults</td>
<td>3927</td>
</tr>
<tr>
<td>Using Tags to Manage Access</td>
<td>3932</td>
</tr>
<tr>
<td>Frequently Asked Questions About Tagging</td>
<td>3950</td>
</tr>
</tbody>
</table>

### Chapter 39 Vault

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vault</td>
<td>3952</td>
</tr>
<tr>
<td>Key and Secret Management Concepts</td>
<td>3953</td>
</tr>
<tr>
<td>Regions and Availability Domains</td>
<td>3955</td>
</tr>
<tr>
<td>Private Access to Vault</td>
<td>3956</td>
</tr>
<tr>
<td>Resource Identifiers</td>
<td>3956</td>
</tr>
<tr>
<td>Ways to Access Oracle Cloud Infrastructure</td>
<td>3956</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>3956</td>
</tr>
<tr>
<td>Limits on Vault Resources</td>
<td>3956</td>
</tr>
<tr>
<td>Managing Vaults</td>
<td>3957</td>
</tr>
<tr>
<td>Managing Keys</td>
<td>3962</td>
</tr>
<tr>
<td>Assigning Keys</td>
<td>3971</td>
</tr>
<tr>
<td>Importing Keys and Key Versions</td>
<td>3986</td>
</tr>
<tr>
<td>Exporting Keys and Key Versions</td>
<td>3994</td>
</tr>
<tr>
<td>Using Keys</td>
<td>3998</td>
</tr>
<tr>
<td>Backing Up Vaults and Keys</td>
<td>4003</td>
</tr>
<tr>
<td>Managing Secrets</td>
<td>4007</td>
</tr>
<tr>
<td>Secret Versions and Rotation States</td>
<td>4018</td>
</tr>
<tr>
<td>Rules for Secrets</td>
<td>4019</td>
</tr>
<tr>
<td>Vault Metrics</td>
<td>4020</td>
</tr>
<tr>
<td>Troubleshooting the Vault Service</td>
<td>4023</td>
</tr>
</tbody>
</table>

### Chapter 40 VMware Solution

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Solution</td>
<td>4026</td>
</tr>
<tr>
<td>Solution Highlights</td>
<td>4026</td>
</tr>
<tr>
<td>SDDC Details</td>
<td>4026</td>
</tr>
<tr>
<td>Supported Shapes</td>
<td>4026</td>
</tr>
<tr>
<td>Oracle Cloud VMware Solution Architecture</td>
<td>4027</td>
</tr>
<tr>
<td>About the VMware Software</td>
<td>4027</td>
</tr>
<tr>
<td>Working with SDDCs</td>
<td>4028</td>
</tr>
<tr>
<td>Additional Documentation Resources</td>
<td>4028</td>
</tr>
<tr>
<td>Setting Up an Oracle Cloud VMware Solution SDDC</td>
<td>4029</td>
</tr>
<tr>
<td>Configuring Networking Connectivity for an SDDC</td>
<td>4032</td>
</tr>
<tr>
<td>Managing Oracle Cloud VMware Solution SDDCs</td>
<td>4035</td>
</tr>
<tr>
<td>Managing Layer 2 Networking Resources for an SDDC</td>
<td>4038</td>
</tr>
<tr>
<td>Security Rules for Oracle Cloud VMware Solution SDDCs</td>
<td>4043</td>
</tr>
</tbody>
</table>
Chapter 41 Web Application Firewall..............................................................4052
  Web Application Firewall..............................................................................................4052
  Web Application Firewall Service Components..........................................................4052
  Ways to Access the WAF Service................................................................................4052
  Authentication and Authorization.................................................................................4053
  Note About The API......................................................................................................4053
  WAF Service Capabilities and Limits...........................................................................4053
  Required IAM Service Policy.........................................................................................4053
  Moving WAF Policies to a Different Compartment.......................................................4054
  Monitoring Resources.................................................................................................4054
  Creating Automation with Events.................................................................................4054
  Tagging Resources.......................................................................................................4054
  Getting Started with WAF............................................................................................4054
  Managing WAF Policies...............................................................................................4061
  Origin Management......................................................................................................4064
  Bot Management..........................................................................................................4071
  WAF Protection Rules.................................................................................................4077
  Access Control............................................................................................................4149
  Caching Rules.............................................................................................................4155
  Threat Intelligence........................................................................................................4158
  Certificates..................................................................................................................4160
  Logs..............................................................................................................................4164
  WAF Metrics................................................................................................................4170
  Layer 7 DDoS Mitigation.............................................................................................4173
  HTTP WAF Headers....................................................................................................4175

Chapter 42 Developer Tools..................................................................................4178
  Developer Resources.....................................................................................................4178
  Developer Guide...........................................................................................................4178

Glossary.........................................................................................................................4398

Release Notes...............................................................................................................4410
Chapter 1

About Oracle Cloud Infrastructure

Oracle Cloud Infrastructure provides bare metal cloud infrastructure that lets you create networking, compute, and storage resources for your enterprise workloads.

If you're new to Oracle Cloud Infrastructure and would like to learn some key concepts and take a quick tutorial, see the Oracle Cloud Infrastructure Getting Started Guide.

If you're ready to create cloud resources such as users, access controls, cloud networks, instances, and storage volumes, this guide is right for you. It provides the following information about using Oracle Cloud Infrastructure:

<table>
<thead>
<tr>
<th>Service</th>
<th>What's Covered</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Migration</td>
<td>Migrating applications from Oracle Cloud Infrastructure Classic to Oracle</td>
<td>See the online documentation:</td>
</tr>
<tr>
<td></td>
<td>Cloud Infrastructure.</td>
<td>Overview of Application Migration</td>
</tr>
<tr>
<td>Archive Storage</td>
<td>Preserving cold data.</td>
<td>Archive Storage on page 484</td>
</tr>
<tr>
<td>Audit</td>
<td>Logging activity in your cloud.</td>
<td>Audit on page 488</td>
</tr>
<tr>
<td>Big Data</td>
<td>Provides enterprise-grade Hadoop as a service.</td>
<td>See the online documentation: Big Data.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>Adding storage capacity to instances.</td>
<td>Block Volume on page 500</td>
</tr>
<tr>
<td>Blockchain Platform</td>
<td>Creating permissioned-blockchain networks for trusted transactions.</td>
<td>See the online documentation: Blockchain Platform.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>Monitoring, identifying, achieving, and maintaining a strong security posture</td>
<td>See the online documentation: Cloud Guard</td>
</tr>
<tr>
<td></td>
<td>on Oracle Cloud.</td>
<td></td>
</tr>
<tr>
<td>Compute</td>
<td>Launching compute instances and connecting to them by using an SSH key pair.</td>
<td>Compute on page 590</td>
</tr>
<tr>
<td>Container Engine for</td>
<td>Defining and creating Kubernetes clusters to enable the deployment, scaling,</td>
<td>Container Engine for Kubernetes on</td>
</tr>
<tr>
<td>Kubernetes</td>
<td>and management of containerized applications.</td>
<td>page 832</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>Find, govern, and track Oracle Cloud data assets.</td>
<td>See the online documentation: Data Catalog.</td>
</tr>
<tr>
<td>Data Flow</td>
<td>Creating, managing, and running Spark applications in a serverless environment.</td>
<td>See the online documentation: Data Flow.</td>
</tr>
<tr>
<td>Data Integration</td>
<td>Design data flows using a visually rich interface to extract, transform, and</td>
<td>See the online documentation: Data Integration.</td>
</tr>
<tr>
<td></td>
<td>load data from data sources to targets.</td>
<td></td>
</tr>
<tr>
<td>Data Science</td>
<td>Build, train, deploy, and manage machine learning models on Oracle Cloud.</td>
<td>See the online documentation: Data Science Overview.</td>
</tr>
<tr>
<td>Service</td>
<td>What's Covered</td>
<td>Chapter</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Data Transfer</td>
<td>Migrating large volumes of data.</td>
<td>Data Transfer on page 968</td>
</tr>
<tr>
<td>Database</td>
<td>Creating and managing database systems and Oracle Databases.</td>
<td>Database on page 1140</td>
</tr>
<tr>
<td>Database Management</td>
<td>Comprehensive database performance diagnostics and management capabilities to monitor and manage Oracle databases.</td>
<td>See the online documentation: Database Management</td>
</tr>
<tr>
<td>Edge Services</td>
<td>Encompasses several services that allow you to manage, secure, and maintain your domains and endpoints.</td>
<td>Edge Services</td>
</tr>
<tr>
<td>Email Delivery</td>
<td>Sending large volume email.</td>
<td>Email Delivery on page 1738</td>
</tr>
<tr>
<td>Events</td>
<td>Creating automation in your tenancy.</td>
<td>Events on page 1784</td>
</tr>
<tr>
<td>File Storage</td>
<td>Managing shared file systems, mount targets, and snapshots.</td>
<td>File Storage on page 1920</td>
</tr>
<tr>
<td>Functions</td>
<td>Building and deploying applications and functions.</td>
<td>Functions on page 2032</td>
</tr>
<tr>
<td>IAM</td>
<td>Setting up administrators, users, and groups and specifying their permissions to access to cloud resources.</td>
<td>IAM on page 2124</td>
</tr>
<tr>
<td>Vault</td>
<td>Creating and managing encryption keys and key vaults to control the encryption of your data.</td>
<td>Vault on page 3952</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>Setting up load balancers, listeners, backend sets, certificate bundles, and managing health check policies.</td>
<td>Load Balancing on page 2480</td>
</tr>
<tr>
<td>Logging Analytics</td>
<td>Rich analysis capabilities based on extensive parsing and enrichment of on-premises or cloud resource logs.</td>
<td>See the online documentation: Logging Analytics</td>
</tr>
<tr>
<td>Management Agent</td>
<td>Providing low latency interactive communication and data collection between Oracle Cloud Infrastructure and any other targets.</td>
<td>See the online documentation: Management Agent Overview.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Querying metrics and managing alarms to monitor the health, capacity, and performance of your cloud resources.</td>
<td>Monitoring on page 2660</td>
</tr>
<tr>
<td>MySQL Database</td>
<td>Creating and managing DB Systems for Oracle MySQL.</td>
<td>See the online documentation: MySQL Database.</td>
</tr>
<tr>
<td>Networking</td>
<td>Setting up cloud networks, subnets, gateways, route tables, and security lists.</td>
<td>Networking on page 2746</td>
</tr>
<tr>
<td>NoSQL Database Cloud</td>
<td>Provisioning for JSON, Table, and Key-Value datatypes using on-demand throughput and a storage basis.</td>
<td>See the online documentation: NoSQL Database</td>
</tr>
<tr>
<td>Notifications</td>
<td>Setting up topics and subscriptions, and publishing messages.</td>
<td>Notifications on page 3350</td>
</tr>
<tr>
<td>Service</td>
<td>What's Covered</td>
<td>Chapter</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Object Storage</td>
<td>Creating and managing buckets to store objects, and uploading and accessing data files.</td>
<td>Object Storage on page 3392</td>
</tr>
<tr>
<td>Operations Insights</td>
<td>Providing 360-degree insight into the resource utilization and capacity of Oracle Autonomous Databases.</td>
<td>See the online documentation: Operations Insights.</td>
</tr>
<tr>
<td>Registry</td>
<td>Storing, sharing, and managing development artifacts like Docker images in an Oracle-managed registry.</td>
<td>Registry on page 3506</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>Using Terraform, installs, configures, and manages Oracle Cloud Infrastructure resources through the &quot;infrastructure-as-code&quot; model.</td>
<td>Resource Manager on page 3532</td>
</tr>
<tr>
<td>Search</td>
<td>Searching for Oracle Cloud Infrastructure resources using free text search or advanced queries.</td>
<td>Search on page 3626</td>
</tr>
<tr>
<td>Service Connector Hub</td>
<td>Describes, executes, and monitors interactions when moving data between Oracle Cloud Infrastructure services.</td>
<td>Service Connector Hub on page 3750</td>
</tr>
<tr>
<td>Tagging</td>
<td>Adding metadata tags to your resources.</td>
<td>Tagging on page 3906</td>
</tr>
</tbody>
</table>

For a description of the terminology used throughout this guide, see the PrintGlossary.

**Prefer Online Help?**

The information in this guide and the Getting Started Guide is also available in the online help at https://docs.cloud.oracle.com/iaas/Content/home.htm.

**Need API Documentation?**

For general information, see REST APIs on page 4368. For links to the detailed service API documentation, see the online help at https://docs.cloud.oracle.com/iaas/Content/home.htm.
Welcome to Oracle Cloud Infrastructure

Chapter 2

Welcome to Oracle Cloud Infrastructure

This chapter provides brief descriptions of Oracle Cloud Infrastructure features and resources.

Introduction

Oracle Cloud Infrastructure is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available hosted environment. Oracle Cloud Infrastructure offers high-performance compute capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network.

About the Services

Analytics Cloud empowers business analysts and consumers with modern, AI-powered, self-service analytics capabilities for data preparation, visualization, enterprise reporting, augmented analysis, and natural language processing.

API Gateway enables you to create governed HTTP/S interfaces for other services, including Oracle Functions, Oracle Cloud Infrastructure Container Engine for Kubernetes, and Oracle Cloud Infrastructure Registry. API Gateway also provides policy enforcement such as authentication and rate-limiting to HTTP/S endpoints.

Application Migration simplifies the migration of applications from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure.

Archive Storage lets you preserve cold data in a cost-efficient manner.

Audit provides visibility into activities related to your Oracle Cloud Infrastructure resources and tenancy. Audit log events can be used for security audits, to track usage of and changes to Oracle Cloud Infrastructure resources, and to help ensure compliance with standards or regulations.

Big Data provides enterprise-grade Hadoop as a service, with end-to-end security, high performance, and ease of management and upgradeability.

Block Volume provides high-performance network storage capacity that supports a broad range of I/O intensive workloads. You can use block volumes to expand the storage capacity of your compute instances, to provide durable and persistent data storage that can be migrated across compute instances, and to host large databases.

Blockchain Platform Cloud enables creation of managed, permissioned-blockchain networks for secure, real-time data sharing and trusted transactions among business partners.

Cloud Advisor finds potential inefficiencies in your tenancy and offers guided solutions that explain how to address them. The recommendations help you maximize cost savings and improve the security of your tenancy.

Cloud Guard is a cloud-native service that helps customers monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Use the service to examine your Oracle Cloud Infrastructure resources for security weakness related to configuration, and your Oracle Cloud Infrastructure operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist, or take corrective actions, based on your configuration.

Use Compute to provision and manage compute instances. You can launch an Oracle bare metal compute resource in minutes. Provision instances as needed to deploy and run your applications, just as you would in your on-premises
Welcome to Oracle Cloud Infrastructure

data center. Managed virtual machine (VM) instances are also available for workloads that don't require dedicated physical servers or the high-performance of bare metal instances.

**Container Engine for Kubernetes** helps you define and create Kubernetes clusters to enable the deployment, scaling, and management of containerized applications.

**Content and Experience** is a cloud-based content hub to drive omni-channel content management and accelerate experience delivery. It offers powerful collaboration and workflow management capabilities to streamline the creation and delivery of content and improve customer and employee engagement.

**Data Catalog** is a collaborative metadata management solution that lets you be more insightful about the data you have in Oracle Cloud and beyond. With Data Catalog, data consumers can easily find, understand, govern, and track Oracle Cloud data assets.

**Data Flow** is a fully managed service with a rich user interface to allow developers and data scientists to create, edit, and run Apache Spark applications at any scale without the need for clusters, an operations team, or highly specialized Spark knowledge. As a fully managed service, there is no infrastructure to deploy or manage. It is entirely driven by REST APIs, giving easy integration with applications or workflows.

**Data Integration** is a fully managed service that helps data engineers and ETL developers with common extract, load, and transform (ETL) tasks such as ingesting data from a variety of data assets, cleansing, transforming, and reshaping that data, and then efficiently loading it to target data assets.

**Data Safe** is a fully-integrated Cloud service focused on the security of your data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. Features include Security Assessment, User Assessment, Data Discovery, Data Masking, and Activity Auditing.

**Data Science** is a platform for data scientists to build, train, and manage machine learning models on Oracle Cloud Infrastructure, using Python and open source machine learning libraries. Teams of data scientists can organize their work and access data and computing resources in this collaborative environment.

**Data Transfer** lets you migrate large volumes of data to Oracle Cloud Infrastructure.

**Database** lets you easily build, scale, and secure Oracle databases with license-included pricing in your Oracle Cloud Infrastructure cloud. You create databases on DB Systems, which are bare metal servers with local NVMe flash storage. You launch a DB System the same way you do a bare metal instance, you just add some additional configuration parameters. You can then use your existing tools, Recovery Manager (RMAN), and the database CLI to manage your databases in the cloud the same way you manage them on-premises. To get started with the Database, see "Overview of the Database Service," in the Oracle Cloud Infrastructure User Guide.

**Database Management** provides comprehensive database performance diagnostics and management capabilities to monitor and manage Oracle databases.

**Digital Assistant** is a platform that allows you to create and deploy digital assistants, which are AI-driven interfaces that help users accomplish a variety of tasks in natural language conversations.

**Edge Services** encompasses several services that allow you to manage, secure, and maintain your domains and endpoints.

**Email Delivery** is an email sending service that provides a fast and reliable managed solution for sending high-volume emails that need to reach your recipients. Email Delivery provides the tools necessary to send application-generated email for mission-critical communications such as receipts, fraud detection alerts, multi-factor identity verification, and password resets.

The **Events** service helps to create automation in your tenancy.

**File Storage** allows you to create a scalable, distributed, enterprise-grade network file system. File Storage supports NFSv3 with NLM for full POSIX semantics, snapshots capabilities, and data at-rest encryption.

The **Functions** service helps you build and deploy applications and functions.

**Fusion Analytics Warehouse** empowers you with industry-leading, AI-powered, self-service analytics capabilities for data preparation, visualization, enterprise reporting, augmented analysis, and natural language processing.
You can control access to Oracle Cloud Infrastructure using IAM Service. Create and manage compartments, users, groups, and the policies that define permissions on resources.

Oracle Integration is a fully managed, preconfigured environment where you can integrate your applications, automate processes, gain insight into your business processes, create visual applications, and support B2B integrations. Use integrations to design, monitor, and manage connections between your applications, selecting from our portfolio of over 60 adapters to connect with Oracle and third-party applications.

Load Balancing allows you to create a highly available load balancer within your virtual cloud network (VCN) so that you can distribute internet traffic to your compute instances within the VCN.

Logging Analytics is a unified, integrated cloud solution that enables users to monitor, aggregate, index, analyze, search, explore, and correlate all log data from their applications and system infrastructure.

Management Agent is a service that provides low latency interactive communication and data collection between Oracle Cloud Infrastructure and any other targets.

Use Monitoring to query metrics and manage alarms. Metrics and alarms help monitor the health, capacity, and performance of your cloud resources.

MySQL Database is a fully managed database service that enables organizations to deploy cloud-native applications using the world’s most popular open source database. It is 100% compatible with On-Premises MySQL for a seamless transition to public or hybrid cloud. Leverage your existing Oracle investments and easily integrate MySQL Database Service with Oracle technologies.

Use Networking to create and manage the network components for your cloud resources. You can configure your virtual cloud network (VCN) with access rules and gateways to support routing of public and private internet traffic.

NoSQL Database Cloud is a high performance data store which is distributed, sharded for horizontal scalability, and highly available. It is optimized for applications requiring predictable low latency (such as fraud detection, gaming, and personalized user experience), very high throughput, or extreme ingestion rates (such as event processing, IoT, and sensor data).

Use Notifications to set up topics and subscriptions for broadcasting messages. Topics are used with alarms.

Operations Insights provides 360-degree insight into the resource utilization and capacity of Oracle Autonomous Databases. You can easily analyze CPU and storage resources, forecast capacity issues, and proactively identify SQL performance issues across a fleet of Autonomous Databases.

OS Management helps you keep operating platforms in your Compute instances secure and up to date with the latest patches and updates from the respective vendor.

Registry helps you store, share, and manage development artifacts like Docker images in an Oracle-managed registry.

Resource Manager helps you install, configure, and manage resources using the "infrastructure-as-code" model.

Search lets you find resources in your tenancy without requiring you to navigate through different services and compartments.

Security Zones let you be confident that your resources comply with Oracle security principles. If any resource operation violates a security zone policy, then the operation is denied.

Service Connector Hub is a cloud message bus platform that offers a single pane of glass for describing, executing, and monitoring interactions when moving data between Oracle Cloud Infrastructure services.

Storage Gateway is a cloud storage gateway that lets you connect your on-premises applications with Oracle Cloud Infrastructure. Applications that can write data to an NFS target can also write data to the Oracle Cloud Infrastructure Object Storage, without requiring application modification to uptake the REST APIs.

Use Streaming to ingest, consume, and process high-volume data streams in real-time.

The Support Management service allows you to create, view, and manage support tickets.

The Tagging service lets you use metadata tags to organize and manage the resources in your tenancy.
Welcome to Oracle Cloud Infrastructure

The **Vault** service helps you centrally manage the encryption keys that protect your data and the secret credentials that you use for access to resources.

Use **Oracle Cloud VMware Solution** to create and manage VMware enabled software-defined data centers (SDDCs) in Oracle Cloud Infrastructure. To get started with the VMware solution, see "Oracle Cloud VMware Solution," in the Oracle Cloud Infrastructure User Guide.

**WAF** helps you make your endpoints more secure by monitoring and filtering out potentially malicious traffic.

### Accessing Oracle Cloud Infrastructure

You can create and manage resources in the following ways:

- **Oracle Cloud Infrastructure Console** The Console is an intuitive, graphical interface that lets you create and manage your instances, cloud networks, and storage volumes, as well as your users and permissions. See Using the Console on page 42.

- **Oracle Cloud Infrastructure APIs** The Oracle Cloud Infrastructure APIs are typical REST APIs that use HTTPS requests and responses. See "Using the API" in the Oracle Cloud Infrastructure User Guide.

- **SDKs** Several Software Development Kits are available for easy integration with the Oracle Cloud Infrastructure APIs, including SDKs for Java, Ruby, and Python. For more information, see "Developer Tools" in the Oracle Cloud Infrastructure User Guide.

- **Command Line Interface (CLI)** You can use a command line interface with some services. For more information, see "Developer Tools" in the Oracle Cloud Infrastructure User Guide.

- **Terraform** Oracle supports Terraform. Terraform is "infrastructure-as-code" software that allows you to define your infrastructure resources in files that you can persist, version, and share. For more information, see Getting Started on page 102.

- **Ansible** Oracle supports the use of Ansible for cloud infrastructure provisioning, orchestration, and configuration management. Ansible allows you to automate configuring and provisioning your cloud infrastructure, deploying and updating software assets, and orchestrating your complex operational processes. For more information, see Getting Started on page 4331.

- **Resource Manager** Resource Manager is an Oracle Cloud Infrastructure service that allows you to automate the process of provisioning your Oracle Cloud Infrastructure resources. Using Terraform, Resource Manager helps you install, configure, and manage resources through the "infrastructure-as-code" model. For more information, see Overview of Resource Manager on page 3534.

For new capabilities, Oracle targets the release of relevant APIs, as well as CLI, SDKs, and Console updates, at the time of general availability (GA). We also target the release of an updated Terraform provider within 30 days of GA.

### How Do I Get Started?

- Sign up for Oracle Cloud Infrastructure
- Understand Oracle Cloud Infrastructure concepts and terminology
- Follow guided tutorials to:
  - Launch your first instance (**Linux** or **Windows**)
  - Add users
  - Put data into object storage
  - Create a load balancer
- Get started with APIs, see "Using the API" in the Oracle Cloud Infrastructure User Guide
- FAQs

### Key Concepts and Terminology

Understand the following concepts and terminology to help you get started with Oracle Cloud Infrastructure.

**BARE METAL HOST**

Oracle Cloud Infrastructure provides you control of the physical host ("bare metal") machine. Bare metal compute instances run directly on bare metal servers without a hypervisor. When you provision a bare metal
compute instance, you maintain sole control of the physical CPU, memory, and network interface card (NIC). You can configure and utilize the full capabilities of each physical machine as if it were hardware running in your own data center. You do not share the physical machine with any other tenants.

REGIONS AND AVAILABILITY DOMAINS

Oracle Cloud Infrastructure is physically hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance.

Availability domains are isolated from each other, fault tolerant, and very unlikely to fail simultaneously or be impacted by the failure of another availability domain. When you configure your cloud services, use multiple availability domains to ensure high availability and to protect against resource failure. Be aware that some resources must be created within the same availability domain, such as an instance and the storage volume attached to it.

For more details see "Regions and Availability domains" in the Oracle Cloud Infrastructure User Guide.

REALM

A realm is a logical collection of regions. Realms are isolated from each other and do not share any data. Your tenancy exists in a single realm and has access to the regions that belong to that realm. Oracle Cloud Infrastructure currently offers a realm for commercial regions and two realms for government cloud regions: FedRAMP authorized and IL5 authorized.

CONSOLE

The simple and intuitive web-based user interface you can use to access and manage Oracle Cloud Infrastructure.

tenancy

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for your company, which is a secure and isolated partition within Oracle Cloud Infrastructure where you can create, organize, and administer your cloud resources.

compartments

Compartments allow you to organize and control access to your cloud resources. A compartment is a collection of related resources (such as instances, virtual cloud networks, block volumes) that can be accessed only by certain groups that have been given permission by an administrator. A compartment should be thought of as a logical group and not a physical container. When you begin working with resources in the Console, the compartment acts as a filter for what you are viewing.

When you sign up for Oracle Cloud Infrastructure, Oracle creates your tenancy, which is the root compartment that holds all your cloud resources. You then create additional compartments within the tenancy (root compartment) and corresponding policies to control access to the resources in each compartment. When you create a cloud resource such as an instance, block volume, or cloud network, you must specify to which compartment you want the resource to belong.

Ultimately, the goal is to ensure that each person has access to only the resources they need.

SECURITY ZONES

A security zone is associated with a compartment. When you create and update cloud resources in a security zone, Oracle Cloud Infrastructure validates these operations against security zone policies. If any policy is violated, then the operation is denied. Security zones let you be confident that your resources comply with Oracle security principles.

VIRTUAL CLOUD NETWORK (VCN)

A virtual cloud network is a virtual version of a traditional network—including subnets, route tables, and gateways—on which your instances run. A cloud network resides within a single region but includes all the region's availability domains. Each subnet you define in the cloud network can either be in a single availability domain or span all the availability domains in the region (recommended). You need to set up
Welcome to Oracle Cloud Infrastructure

at least one cloud network before you can launch instances. You can configure the cloud network with an optional internet gateway to handle public traffic, and an optional IPSec VPN connection or FastConnect to securely extend your on-premises network.

INSTANCE

An instance is a compute host running in the cloud. An Oracle Cloud Infrastructure compute instance allows you to utilize hosted physical hardware, as opposed to the traditional software-based virtual machines, ensuring a high level of security and performance.

IMAGE

The image is a template of a virtual hard drive that defines the operating system and other software for an instance, for example, Oracle Linux. When you launch an instance, you can define its characteristics by choosing its image. Oracle provides a set of images you can use. You can also save an image from an instance that you have already configured to use as a template to launch more instances with the same software and customizations.

SHAPE

In Compute, the shape specifies the number of CPUs and amount of memory allocated to the instance. Oracle Cloud Infrastructure offers shapes to fit various computing requirements. See “Compute Shapes” in the Oracle Cloud Infrastructure User Guide.

In Load Balancing, the shape determines the load balancer's total pre-provisioned maximum capacity (bandwidth) for ingress plus egress traffic. Available shapes include 100 Mbps, 400 Mbps, and 8000 Mbps.

KEY PAIR

A key pair is an authentication mechanism used by Oracle Cloud Infrastructure. A key pair consists of a private key file and a public key file. You upload your public key to Oracle Cloud Infrastructure. You keep the private key securely on your computer. The private key is private to you, like a password.

Key pairs can be generated according to different specifications. Oracle Cloud Infrastructure uses two types of key pairs for specific purposes:

- Instance SSH Key pair: This key pair is used to establish secure shell (SSH) connection to an instance. When you provision an instance, you provide the public key, which is saved to the instance's authorized key file. To log on to the instance, you provide your private key, which is verified with the public key.
- API signing key pair: This key pair is in PEM format and is used to authenticate you when submitting API requests. Only users who will be accessing Oracle Cloud Infrastructure via the API need this key pair.

For details about the syntax of an OCID, see "Security Credentials" in the Oracle Cloud Infrastructure User Guide.

BLOCK VOLUME

A block volume is a virtual disk that provides persistent block storage space for Oracle Cloud Infrastructure instances. Use a block volume just as you would a physical hard drive on your computer, for example, to store data and applications. You can detach a volume from one instance and attach it to another instance without loss of data.

OBJECT STORAGE

Object Storage is a storage architecture that allow you to store and manage data as objects. Data files can be of any type and up to 50 GB in size. Once you upload data to Object Storage it can be accessed from anywhere. Use Object Storage when you want to store a very large amount of data that does not change very frequently. Some typical use cases for Object Storage include data backup, file sharing, and storing unstructured data like logs and sensor-generated data.

BUCKET

A bucket is a logical container used by Object Storage for storing your data and files. A bucket can contain an unlimited number of objects.
ORACLE CLOUD IDENTIFIER (OCID)

Every Oracle Cloud Infrastructure resource has an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). This ID is included as part of the resource's information in both the Console and API.

For details about the syntax of an OCID, see "Resource Identifiers" in the Oracle Cloud Infrastructure User Guide.

Request and Manage Free Oracle Cloud Promotions

You can sign up for a 30-day Oracle Cloud promotion and receive free credits. This promotion applies to eligible Oracle Cloud Infrastructure services.

Estimate Your Monthly Cost on page 32
Sign Up for the Free Oracle Cloud Promotion on page 34
Monitor the Credit Balance for Your Free Oracle Cloud Promotion on page 35
What Happens When the Promotion Expires on page 35
Upgrade Your Free Oracle Cloud Promotion on page 35

Estimate Your Monthly Cost

Oracle provides you with a cost estimator to help you figure out your monthly usage and costs for Oracle’s Infrastructure and Platform Cloud (Oracle IaaS/PaaS) services before you commit to an amount.

The cost estimate is automatically calculated based on your choice of the Oracle Cloud service category, its service configurations, and the usage of each resource in the configuration.

You can start using Oracle Cloud with no up-front cost. Oracle will bill you for the services and resources you use. For the purpose of planning, use the results from the Cost Estimator to estimate how much you are likely to be charged for usage each month.

To use the Cost Estimator:

1. Go to the Cost Estimator page on the Oracle Cloud website.
2. Select a category of cloud services, such as Infrastructure or Data Management, from the list on the left side of the page.
   The cost estimator displays a set of packages, which represent the services and resources that are typically required to support the selected service category. To see all the packages of the selected service category, scroll to the right.
3. Select one of the packages, as a starting point for your estimate. The estimator begins calculating the cost for the selected service and package.
4. In the Configuration Options section, expand each service, use the sliders, or select from the drop-down lists to adjust the values to match your project’s or organization’s needs.
   As soon as you adjust the amount of resources, the cost estimate changes.
   If you have existing software licences for services such as Oracle Database or Oracle Middleware, you can use them to estimate your cost for cloud services. Simply select the BYOL (Bring Your Own License) option from the service packages or under the Configuration Options section. For example, if you have an existing license for Autonomous Data Warehouse, then select the Autonomous Data Warehouse Cloud - BYOL package from the service packages set. If you’ve an Oracle Database Enterprise Edition license, then select the Enterprise Edition Extreme Performance BYOL option from the Edition list under Configuration Options. The cost immediately reflects the BYOL pricing, which is typically lower than the normal cloud service costs.
   You can experiment with different configuration options until you balance the cost with your organization’s needs.
5. Review your estimates, and then click Start for Free to sign up for the Oracle Cloud Free Tier and get free credits. You can upgrade your free promotion to a paid account at any time during the promotion period.
Example: Estimating Your Monthly Cost for Oracle Database Cloud Service

In this example, see how you can estimate your monthly cost for Oracle Database Cloud Service based on your requirements.

To estimate your costs:

1. In the Cost Estimator page, select the Data Management category from the list on the left side of the screen.
2. From the list of configurations displayed, select Oracle Database Cloud Service and click Add.

   The cost estimator displays a set of packages, which represent the services and resources that are typically required to support the selected service category. To see all the packages of the selected service category, scroll to the right.
3. In the Configuration Options section of the page, expand Database.
4. Expand each of the resources under Database, such as Number of Instances, Average Days Usage per Month, or Average Hours Usage per Day. You’ll see some default values as you expand each item.
5. Increase the number of instances to 2: One for development and one for testing.
6. Use the slider to adjust values for Average Days Usage per Month or Average Hours Usage per Day, as needed. By default, they are set to 31 days (in a month) and 24 hours (per day) of usage. If you intend to use the Database service for a lesser period, then adjust the values accordingly.
7. Select Enterprise Edition High Performance - General Purpose from the Edition drop-down menu to see how this affects the monthly estimate.
8. You can also remove certain sections by clicking the trash icon next to them. For example, if you don’t need Database Backup service, you can remove it by clicking the trash icon.
9. When you have estimated all your requirements, select the payment plan, and click Buy Now.

You can also add other configurations in the Data Management category such as Oracle Database Exadata Cloud Service or Oracle Big Data Cloud Service to estimate your total cost. Or, you can add other service categories, such as Infrastructure or Integration and their configurations, as needed, to get your total usage cost estimate.

Save and Share Your Cost Estimator Results

When you are satisfied with your monthly usage estimates, you can save them either by downloading them as a PDF file or exporting them to an .oce file. The .oce file is only used to export and import your saved estimates in the Cost Estimator. This is useful when you want to share and review the quotes with your management, finance, or other departments to get their approval.

Save Your Cost Estimates

To save your cost estimate:

- In the Cost Estimator page, select from the following options:
  - Load/Save: Click this button to save your service configurations in your browser. Provide a name for your configuration and click Save. Note that this action is browser specific. You can’t use a configuration that you saved on Google Chrome in Firefox, or vice versa.
  - Save as PDF: Click this button to save the estimates as a PDF file. This is useful for presenting the estimates to others. The PDF is read-only.
  - Export: Click this button to export the estimates to an .oce file. This is useful if you need to share the estimates with reviewers or might need to make changes to them later. The reviewers can then import the .oce file to their own Cost Estimator pages and make changes as needed.

Import or Load Your Saved Estimates

If you want to make changes to your saved estimates, or if you’re reviewing them, you can import them to the Cost Estimator. You can also load previously saved service configurations on your browser to continue with your estimate.

To import or load your saved cost estimate, use any of the following options:
Welcome to Oracle Cloud Infrastructure

- **Load/Save**: Click this button to load your saved service configurations. Note that this action is browser specific.
  1. Click **Select Saved Configuration**.
  2. Select a saved configuration and then click **Load**.
- **Import**: Click this button to import any previously exported estimates. Ensure that you have exported the estimates to an `.oce` file.
  - Browse for the `.oce` file and click **Open**.

The saved estimates appear in the Cost Estimator page. You can then make changes as required.

### Sign Up for the Free Oracle Cloud Promotion

Signing up for Oracle Cloud Free Tier is easy.

2. Provide information for your Oracle Cloud account.
   - Select your country. For some countries, such as Russia, you must manually accept the Terms of Use by selecting the check boxes when prompted.
   - Enter your name and optionally enter the name of your company.
   - Provide a valid email address. You'll use this email ID later to sign in to your Oracle Cloud account. Instructions about signing in to your new cloud account are sent to this address. Your email ID is also used to check if you are eligible for any special offers. If you are, then you'll be prompted to select a special offer from a list of applicable offers.
   - Oracle permits one cloud account to be created per email address. If your email address is already associated with a cloud account, then you can click the link to get all your accounts associated with your email address.
   - Enter a password based on the password policy specified on the web page. You will use this password later to sign in to your Oracle Cloud account. Password must contain a minimum of 8 characters, 1 lowercase, 1 uppercase, 1 numeric, and 1 special character. Password can't exceed 40-characters, contain the users first name, last name, email address, spaces, or `~ < > \` characters.
   - Re-enter the password to confirm it.
   - Create a cloud account name, which is used to identify your cloud account.
   - Select a **Home Region**, where your services will be hosted.

   **Note:**
   Your home region is the geographic location where your account and identity resources will be created. You can't change this after signing up. If you are not sure which region to select as your home region, contact your sales representative before you create your account.

   - Click **Continue**.
3. Enter your address, and then click **Continue**.
   Provide additional information, such as a PO box number, if you're asked for it. For Brazil, enter your CPF number for tax purposes in the format `xxxxxxxx-xx`. For example, `655156112-18`.
   If you have selected a special offer, then you'll be prompted to enter a phone number. You don't have to provide verification code for certain offers, so in these cases skip to step 8.
4. Enter a valid mobile number, along with country code, and then click **Text me a code**. A verification code will be sent as a text message to your mobile phone. VOIP or internet-only mobile numbers are not accepted as we may need to speak to you if there are questions about your account.
5. Enter the verification code that you received on your phone as a text message, and then click Verify my code. If you already have a verification code, then follow the on-screen instructions to verify your phone number.

You can also click Request another code if you don't receive a verification code soon or if your verification code expires.

6. Click Add payment verification method, and then click Credit Card.

7. Enter your credit card information, and then click Finish. You may see a small, temporary charge on your payment method. This is a verification hold that will be removed automatically. Note that your credit card won't be charged unless you elect to upgrade your cloud account.

8. Accept the terms and conditions, and then click Start my free trial to submit your request for a new Oracle Cloud account.

After the services are provisioned in your tenancy, you'll be redirected to the Oracle Cloud Infrastructure Console. Use the Oracle Cloud Infrastructure Console to create instances of your services.

You'll also receive a welcome (Get Started) email with more information about your account.

For some countries, you may not be able to request a free promotion from the Oracle Cloud website. In these cases, contact Oracle Sales to request a free promotion.

Monitor the Credit Balance for Your Free Oracle Cloud Promotion

After you get free credits, you can monitor and manage your service usage and your credit balance.

In the Console, you can monitor your usage costs from the Account Management page. See Checking Your Expenses and Usage on page 55 for more information.

Oracle sends you a notice when you get close to your credit limit.

What Happens When the Promotion Expires

If you don’t upgrade your free credit promotion to a paid subscription, then it’s important to understand what happens to your cloud account.

All Oracle Cloud Infrastructure accounts (whether free or paid) have a set of resources that are available free of charge for the life of the account. These resources are called Always Free resources. If you have subscribed to a free credit promotion, your account continues to be available to you after the trial period ends (or after you use all of your credits). You can continue to use the Always Free resources in your account for as long as your account remains active. Free accounts remain active and available to you as long as the account has been used within the past 60 days. If you have a paid account, you will not be billed for any Always Free resources you are using. See Oracle Cloud Infrastructure Free Tier on page 140 for more information.

Your Free Credit Promotion expires:

• Thirty (30) days from the day you signed up.

OR

• When you use up the free credits available in your promotion offer.

In both cases, Oracle Cloud sends you warning messages that you are nearing the end of your promotion period or getting close to your free credit limit. Another email will let you know when the promotion actually expires. You will have a grace period of 30 days. You can continue to use paid resources during the grace period. However, you can't create new paid resources during the grace period unless you upgrade your account. If you don't upgrade your account during this period, then your paid resources will be reclaimed. Your Always Free resources will continue to be available.

Upgrade Your Free Oracle Cloud Promotion

You can choose to upgrade your free promotion to a paid account at any time during the promotion period or within 30 days of the promotion expiration.
If you are using the Oracle Cloud Infrastructure Console, then you can upgrade your promotion to a paid account from the Account Management page. For more information, see Changing Your Payment Method on page 56.

Buy an Oracle Cloud Subscription

Use the Oracle Cloud website to estimate your cloud usage and costs for Oracle Cloud Infrastructure services and to sign up for an Oracle Cloud account. You can also contact an Oracle Sales representative to order Oracle Cloud services on your behalf.

To purchase a subscription to Oracle Cloud Applications (SaaS), see Order Oracle Cloud Applications.

About Bring Your Own License Subscriptions

If you already have Oracle software licenses for services such as Oracle Database, Oracle Middleware, or Oracle Analytics, you can reuse them when subscribing to Oracle Platform Cloud Services (Oracle PaaS). This is called Bring Your Own License (BYOL).

With BYOL, you can leverage existing software licenses for Oracle PaaS at a lower cost. For example, if you have purchased a perpetual license for Oracle Database Standard Edition earlier, then you can use the same when you buy Database Standard Package with BYOL pricing. This enables you to get a discounted price for your services. Oracle BYOL to PaaS includes Compute and Compute support along with automation.

You continue to get the same license support (that you had for your existing licenses) and contract when you buy Oracle PaaS with BYOL pricing. This flexible licensing allows you to move between your on-premises and cloud services with ease.

How do You Use Your BYOL for Oracle PaaS?

When you have an existing Oracle software license and you want to use it on Oracle Cloud, you can do so in the following ways:

- Select specific Oracle BYOL options in the Cost Estimator to get your BYOL pricing.
- Apply your BYOL pricing to individual cloud service instances when creating a new instance of your PaaS service. BYOL is the default licensing option during instance creation for all services that support it. For example, when creating a new instance of Oracle Database Cloud Service using the QuickStarts wizard, BYOL option is automatically applied.

For a list of cloud services that support BYOL, search for BYOL in the Universal Credits Service Descriptions Document.

For more information, see BYOL Overview video and Frequently Asked Questions.

About Universal Credits

Oracle Cloud provides a flexible buying and usage model for Oracle Cloud Services, called Universal Credits.

When you sign up for an Oracle Cloud Account, you have unlimited access to all eligible IaaS and PaaS services. You can sign up for a Pay-As-You-Go subscription to pay in arrears based on your actual usage at the end of your monthly billing cycle.

After you sign up, you can start using any of the IaaS or PaaS services at any time. Not all services are available in all the data regions. You can only use services in the data regions that your subscription is enabled in. However, you can always extend your subscription to other data regions to access services available there. See Extending Your Subscription to Another Data Region.

When new eligible services become available as part of the Universal Credits program, you'll receive an email with the details of the newly added services if they are available in one of your enabled data regions.

For new services added to data regions where your subscription is not enabled, see the Service Availability Matrix.
Upgrade Your Free Oracle Cloud Promotion

You can choose to upgrade your free promotion to a paid account at any time during the promotion period or within 30 days of the promotion expiration.

If you are using the Oracle Cloud Infrastructure Console, then you can upgrade your promotion to a paid account from the Account Management page. For more information, see Changing Your Payment Method on page 56.

Activate Your Order from Your Welcome Email

If you ordered Oracle Infrastructure as a Service (Oracle IaaS) and Oracle Platform as a Service (Oracle PaaS) cloud services with Universal Credits through Oracle Sales, then you must activate your services before you start using them.

When an Oracle Sales representative orders Oracle Cloud services on your behalf, you’ll receive a welcome email and you’ll be designated as an activator of the services. To activate your services, you must provide your details and set up your account with Oracle. Review the instructions in the email to create an account and start using your services.

1. Open the email you received from Oracle Cloud.
2. Review the information about your service in the email.
3. Click Activate My Services.
4. Complete the form to sign up for your new Oracle Cloud account.

You will be asked to:

• Provide a new account name, which will be used to identify your Cloud account.
• Provide your email address. You must provide the same email address at which you received your welcome email. Instructions for signing in to your new Oracle Cloud account will be sent to this address. You’ll be prompted for the email ID only if you don’t already have an Oracle Cloud account.
• If prompted, select a Home Region. If you need more information, click the Regions link below the field.

Note:

Your home region contains your account information and identity resources. It is not changeable after your tenancy is provisioned. If you are unsure which region to select as your home region, contact your sales representative before you create your account.

• Provide Oracle Cloud account administrator details. The person you specify here will be a Cloud Account Administrator and a Service Administrator and can create other users in your account. This person will manage and monitor services in the specified Oracle Cloud account.
• After you enter all the required information, click Create Account to submit your request for an Oracle Cloud account.

After successful activation, you’ll receive another email with your sign in credentials. Use this information to sign in to your account and change your password after initial sign in.

Verify That Your Services Are Ready

When you sign up for a Free Oracle Promotion or a paid account, your Oracle Cloud account is created soon after sign up, but the service provisioning takes some time. You’ll receive a Welcome email soon after you sign up.

The email contains information required to access your account and sign in to Infrastructure Classic Console:

• Your user name and temporary password (sign-in credentials)
• The name of your Cloud Account

Sign in to Infrastructure Classic Console to see how many services are provisioned. A message at the top of the Infrastructure Classic Console indicates how many services are active.

1. Click Get Started with Oracle Cloud from your welcome email.
2. Change your password when prompted.
3. Scan the dashboard to check the current status of your service. When the services are provisioned, they might not immediately be displayed on the Infrastructure Classic Console. Services with instances are automatically displayed.
4. Click the gear icon next to Dashboard and set the services to Show. By default, all service tiles are hidden, unless a service has at least one instance. The Customize Dashboard dialog box appears.

When all the services in your order are provisioned, you’ll get a message on the Infrastructure Classic Console. You can then add users, view service details, monitor account usage, and access the service consoles.

Some services in your order may require additional sign-in credentials, which you can find in the Manage Account, My Admin Accounts page. For more information about these services, see Access Traditional Cloud Account Services.

Request and Manage the Oracle Startup Program

You can sign up for the Oracle Startup Program and receive free credits. This promotion applies to eligible Oracle Infrastructure as a Service (Oracle IaaS) and Platform as a Service (Oracle PaaS) services.

After you consume your free credits, you’ll be charged for the services and resources you use. For information about monitoring the usage of your free credits, see Monitor the Credit Balance for Your Free Oracle Cloud Promotion on page 35.

Sign Up for the Oracle Startup Program

Signing up for the Oracle Startup Program is easy. You create an Oracle Cloud account, and then you get a welcome email with the details that you need to sign in.

1. Go to the Oracle for Startups website, and then click Join Oracle for Startups.
2. Fill out the Oracle for Startups form. You are asked to:

   Create Account:
   • Select your country. For some countries such as Russia, you must manually accept the Terms of Use by selecting the check boxes when prompted.
   • Provide a valid email address, and then click Next. Instructions for signing in to your new cloud account are sent to this address. You can sign up for only one Oracle Startup Program even if you have an existing Oracle Cloud account. If your email address is already associated with the Oracle Startup Program, then you’ll be provided information to access your existing account.

   Enter Account Details:
   • Create a cloud account name, which is used to identify your cloud account.
   • Select a Home Region, where your services will be hosted. See Data Regions for Platform and Infrastructure Services for service availability in each region.

   Note: Your home region contains your account information and identity resources. It is not changeable after your tenancy is provisioned. If you
Welcome to Oracle Cloud Infrastructure

If you are unsure which region to select as your home region, contact your sales representative before you create your account.

- Provide your name, company name, and address.
- Provide additional information, such as a PO box number, if you're asked for it. For Brazil, enter your CNPJ number for tax purposes in the format xxxxxxx/xxxx-xx. For example, 12345678/0001-18.
- Enter a valid mobile number, so that Oracle can text you a verification code, and then click Next: Verify Mobile Number. VOIP or internet-only mobile numbers are not accepted.
- Your address is validated and displayed with corrections, if any. Confirm your address if prompted.

Verify Your Mobile Number:

- Enter the SMS code you received on your phone and click Verify Code. If you already have a verification code, then follow the on-screen instructions to verify your phone number.
- You can also request another code if you don't receive a verification code soon.

Payment Information:

- Click Add Credit Card Details. Enter your credit card information. During sign up, you may see an authorization of $100 USD (or local currency equivalent) on your payment card account. Authorizations do not represent charges nor money owed to Oracle. This is a temporary hold on available credit that will be removed automatically.
- Click Finish.

3. Accept the terms and conditions, and then click Complete Sign-Up to submit your request for a new Oracle Cloud account.

Your account is created. After the services in your tenancy are provisioned, you'll be redirected to the sign-in page. You'll also receive a welcome (Get Started) email with your sign-in credentials.

Understanding the Sign-In Options

This topic describes sign in options available to you when you sign up for an Oracle Cloud account.

About the Sign In Options

When you sign up for Oracle Cloud, Oracle creates a user for you in two different identity systems, giving you two options to sign in to Oracle Cloud Infrastructure.
Welcome to Oracle Cloud Infrastructure

When you want to use Oracle Cloud Infrastructure, you can choose which identity provider to sign in through:

**Oracle Identity Cloud Service**

Many Oracle Cloud services, including Oracle Cloud Infrastructure, are integrated with Oracle Identity Cloud Service. When you sign up for an Oracle Cloud account, a user is created for you in Oracle Identity Cloud Service with the username and password you selected at sign up. You can use this single sign-on option to sign in to Oracle Cloud Infrastructure and then navigate to other Oracle Cloud services without reauthenticating. This user has administrator privileges for all the Oracle Cloud services included with your account.

**Oracle Cloud Infrastructure**

Oracle Cloud Infrastructure includes its own identity service, called the Identity and Access Management service, or IAM, for short. When you sign up for an Oracle Cloud account, this service is included. A second, separate user is created for you in the IAM service with the username and password you selected at sign up. You are granted administrator privileges in Oracle Cloud Infrastructure so you can get started right away with all Oracle Cloud Infrastructure services.
Welcome to Oracle Cloud Infrastructure

Important:

Although the credentials are identical in both systems when your account is created, the users are in separate identity management systems, and you manage them separately. If you change your password in the Oracle Cloud Infrastructure IAM, your password in Oracle Identity Cloud Service is not changed, and conversely.

When to Use Each Sign-In Option

If you plan to use Oracle Cloud Infrastructure services exclusively, it makes sense for you to use your direct sign-in credentials to the IAM service.

If you want to use other Oracle Cloud services that are managed through Oracle Identity Cloud Service, then sign in with your single sign-on credentials.

More Information About Managing Users in Oracle Cloud Identity Providers

Managing Users in the IAM Service

Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372

Adding Users on page 57

Signing In to the Console

This topic describes how to sign in to the Oracle Cloud Infrastructure Console.

Supported Browsers

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Signing In for the First Time

To sign in to Oracle Cloud at https://cloud.oracle.com, you need:

- Your cloud account name (also sometimes referred to as your tenancy name)
- User name and password
Welcome to Oracle Cloud Infrastructure

When your tenancy is provisioned, Oracle sends an email to the default administrator at your company with the sign-in credentials and URL. This administrator can then create a user for each person who needs access to Oracle Cloud Infrastructure. Check your email or contact your administrator for your credentials and account name.

1. Open a supported browser and go to https://cloud.oracle.com.
2. Enter your Cloud Account Name and click Next.
3. On the Single Sign-On (SSO) panel, click Continue.
4. Enter your user name and temporary password from your welcome email. You will be prompted to change your temporary password.

After you sign in, the Console Home page is displayed.

Note:
When you're logged in to the Console for one of the commercial realm regions, the browser times out after 60 minutes of inactivity, and you need to sign in again to use the Console.

Next Steps

Get to know the Console. See Using the Console on page 42.

Follow guided tutorials to launch your first instance, add users, or put data into object storage.

Begin setting up your tenancy for other users. See Setting Up Your Tenancy on page 122.

Using the Console

This topic provides basic information about the Oracle Cloud Console. To access the Console, you must use a supported browser.

About the Console Home Page

When you sign in to the Console, you see the home page.

### The Get Started tab
- Provides features helpful for new users.

### The Dashboard tab
- Supports widgets that provide an overview of your resources and billing usage.

### The Help menu
- Provides links to support and documentation.
The home page offers features for both new and experienced users. For new users, the Get Started tab provides features to help you start learning about and working with Oracle Cloud Infrastructure. The Dashboard tab supports widgets to help you quickly access and monitor your resources and billing usage.

Features of the Get Started Tab

The Get Started tab includes features that are particularly helpful for new users or users who want to jump in and quickly create common resources.

Quick Actions

Use the Quick Actions tiles to navigate directly to common tasks, like creating a VM instance, setting up a network with a wizard, and setting up a load balancer. Use these links to set up your environment.

Start Exploring

The Start Exploring section provides links to tutorials, developer tools, and blogs that demonstrate how to use Oracle Cloud Infrastructure to build solutions.

- In the Get Started category, find introductory materials that you can use to learn more about basics, such as information about virtual training classes, key concepts, and introductory demos.
- In the Deploy Websites & Apps category, find tutorials that leverage both basic and more advanced features available to build solutions.
- In the Explore Developer Tools category, explore the developer kits, tools, and plug-ins that you can use to facilitate the development of apps and to simplify the management of infrastructure.
- In the Manage Bills category, learn about the billing and payment tools that to help you manage your service costs.

Features of the Dashboard Tab

The Dashboard tab includes widgets you can use to explore your resources and billing usage.

Get an Overview of All Your Resources with the Resource Explorer

Use the resource explorer to get an overview of the number and types of resources that exist in a selected compartment and region.
To use the resource explorer to find resources:

1. On the Console home page, click the **Dashboard** tab.
2. The resource explorer displays the list of services and count of resources in the selected **compartment** and **region**. By default, the root compartment is selected. To view another compartment, select it from the compartment picker.
3. Expand the entry for a service to see the count for each resource-type within the service.
4. To see more information about a resource-type in the list, click the resource-type to open the detailed list. To navigate directly to a specific resource in the list, click the **Display Name**.

**Monitor Your Usage with the Billing Widget**

Administrators and users with appropriate permissions can view the billing widget. The billing widget lets you quickly view your current charges or usage and the days elapsed in your billing cycle. Your view depends on your account type.

- Pay-as-you-go customers see the current charges and the numbers of days elapsed in the current billing cycle.
- Universal credit customers see the total credits used and number of days elapsed in the credit period.
- Trial customers see the total credits used and number of days elapsed in the trial period.

To get a more detailed view of your spending, click the **Analyze Costs** link to go to the **Cost Analysis tool** where you can generate charts and reports of aggregated cost data for your Oracle Cloud Infrastructure consumption. If your account is a free tier or promotional trial account, you’ll see an option to **Upgrade your account**. If you have a paid account, you’ll see the option to **Manage payment method** to view or change your payment method.

**Navigating to Oracle Cloud Infrastructure Services**

Open the navigation menu in the upper left to work with services and resources. Services and resources are organized by functional group. For example, to work with Compute service instances: Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.

**Navigating to More Oracle Cloud Services from the Console**

For more details about accessing other Oracle Cloud offerings, see **Navigate to Your Cloud Services**.

The Oracle Cloud Console provides navigation to other Oracle Cloud services in addition to Oracle Cloud Infrastructure services.

If your account also has Oracle Cloud Platform services, Oracle Cloud Infrastructure Classic services, or Oracle Cloud Applications, then you can navigate to these services from the Oracle Cloud Console:
Navigating to Platform Services
Open the navigation menu. Under More Oracle Cloud Services, go to Platform Services, and then click the service you want to access.

Navigating to Classic Data Management Services
Open the navigation menu. Under More Oracle Cloud Services, go to Classic Data Management Services, and then click the service you want to access.

Navigating to Classic Infrastructure Services
Open the navigation menu. Under More Oracle Cloud Services, go to Classic Infrastructure Services, and then click the service you want to access.

Navigating to the Applications Console
If your Cloud account also has Cloud Applications services provisioned, then you have access to the Applications Console.
In the Console header, click Applications to switch to the Applications Console.
For more information about the consoles for these Oracle Cloud services, see About the Consoles.

Switching Regions
Your current region is displayed at the top of the Console. If your tenancy is subscribed to multiple regions, you can switch regions by selecting a different region from the Region menu.
Welcome to Oracle Cloud Infrastructure

Working Across Regions

When working within a service, the Console displays resources that are in the currently selected region. So if your tenancy has instances in CompartmentA in US West (Phoenix), and instances in CompartmentA in US East (Ashburn), you can only view the instances in one region at a time, even though the instances are in the same compartment.

Using the following figure as an example, if you select US West (Phoenix) and then select CompartmentA, you see instances 1 and 2 listed. To see instances 3 and 4 in the Console, you must switch to US East (Ashburn) (and then you no longer see instances 1 and 2).

To view resources across regions that are in a specific compartment, you can use the tenancy explorer.

IAM resources (compartments, users, groups, policies, tags, and federation providers) are global, so you can see those resources no matter which region you have selected in the Console.
Switching Languages

The Console automatically detects the language setting in your browser. However, if you want to view the Console in a different language, you can change it by using the language selector in the Console.

The language selector supports the following languages:

Supported Languages

- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Czech
- Danish
- Dutch
- English
- Finnish
- French (Canada)
- French (Europe)
- German
- Greek
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Romanian
- Russian
- Serbian
- Slovak
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish
The language you choose persists between sessions. However, the language setting is specific to the browser. If you change to a different browser, the Console displays text in the language last selected in the language selector. If it’s the first time you’re viewing the Console in a particular browser, the Console displays content according to the browser’s language setting.

**Contact Support**

In the Console, you can create a support request or start a live online chat with an Oracle Support or Sales representative. For more information, see *Getting Help and Contacting Support* on page 125.

**Understanding Compartments**

After you select a service from the navigation menu, the menu on the left includes the compartments list.

Compartments help you organize resources to make it easier to control access to them. Your root compartment is created for you by Oracle when your tenancy is provisioned. An administrator can create more compartments in the root compartment and then add the access rules to control which users can see and take action in them. To manage compartments, see *Managing Compartments* on page 2431.

The list of compartments is filtered to show you only the compartments that you have permission to access. Compartments can be nested, and you might have access to a compartment but not its parent. The names of parent compartments that you don’t have permission to access are dimmed, but you can traverse the hierarchy down to the compartment that you do have access to.

After you select a compartment, the Console displays only the resources that you have permission to view in the compartment for the region that you are in. The compartment selection filters the view of your resources. To see resources in another compartment, you must switch to that compartment. To see resources in another region, you must switch to that region, or use the tenancy explorer.

For more details about compartments, see *Setting Up Your Tenancy* on page 122 and *Managing Compartments* on page 2431.

**Filtering the Displayed List of Resources**

To help you locate a resource, some resources let you filter the list that is displayed.
Filters include:

**State:** You can display only the resources that are in the state you select. Valid values for state can vary by resource. Examples are:

- Any state - includes all lifecycle states for the resource
- Available
- Provisioning
- Terminating
- Terminated

**Availability Domain:** For resources that reside in a single availability domain, you can limit the list to the resources that reside in the availability domains you select. For a list of availability domain-specific resources, see Resource Availability on page 184.

**Tags:** Resources that support tagging let you filter the list by tags.

### To filter a list of resources by a defined tag

1. Next to **Tag Filters**, click **add**.
2. In the **Apply a Tag Filter** dialog, enter the following:
   a. **Namespace:** Select the tag namespace.
   b. **Key:** Select a specific key.
   c. **Value:** Select from the following:
      - **Match Any Value** - returns all resources tagged with the selected namespace and key, regardless of the tag value.
      - **Match Any of the Following** - returns resources with the tag value you enter in the text box. Enter a single value in the text box. To specify multiple values for the same namespace and key, click + to display another text box. Enter one value per text box.
   d. Click **Apply Filter**.

### To filter a list of resources by a free-form tag

1. Next to **Tag Filters**, click **add**.
2. In the **Apply a Tag Filter** dialog, enter the following:
   a. **Key:** Enter the tag key.
   b. **Value:** Select from the following:
      - **Match Any Value** - returns all resources tagged with the selected free-form tag key, regardless of the tag value.
      - **Match Any of the Following** - returns resources with the tag value you enter in the text box. Enter a single value in the text box. To specify multiple values for the same key, click + to display another text box. Enter one value per text box.
   c. Click **Apply Filter**.

### Signing Out

To sign out of the Console, open the **Profile menu (👤)** and then click **Sign Out**.

### Using the Mobile App

The Oracle Cloud Infrastructure Mobile app let you review alerts, notifications, and limits on the go. Quickly access information about infrastructure resources, billing, and usage data from your mobile device. Read more to learn about installing and using the app.
Welcome to Oracle Cloud Infrastructure

Download Now

To download and install the app, click the Google Play Store or Apple App Store badge below and follow the instructions at the link.

Alternately, in the Google Play Store or Apple App Store, search for Oracle Cloud Infrastructure, select the app, and follow the installation steps.

This app is supported on the following operating systems:

- Android 8 and later versions
- iOS 11 and later versions

Signing In

To sign in to the Oracle Cloud Infrastructure Mobile app, use the same credentials and steps that you use to sign in to the Console. For more information, see Understanding the Sign-In Options.

The first time you sign in, you must read and accept the End User License Agreement to access the app.

Enabling Automatic Sign-in

For faster sign-in to the mobile app, you can enable automatic sign-in. Automatic sign-in uses an API key to authenticate you when you access the app, keeping you signed in until you sign out. The private key and the generated fingerprint are encrypted and stored in either the Android Keystore or the iCloud Keychain, depending on your device operating system. This encryption and storage ensures that your information is only accessible through the Oracle Cloud Infrastructure Mobile app. For more information about API keys, see Working with Console Passwords and API Keys on page 2456.

To enable automatic sign-in:

1. In the app, open the Profile menu ( ) and then tap Settings.
2. Under Login Security, for Enable automatic sign-in, toggle the Enabled or Disabled switch. When enabled, automatic sign-in will be used next time you open the app.

Generating the API signing key can take a few minutes. Automatic sign-in is available after the key is generated.

After you enable automatic sign-in, if you want to find the API key used by the app:

1. In the app, open the Profile menu ( ) and then tap Settings.
2. Under Login Security, the API key fingerprint value is the API signing key that the mobile app is using.

Each user has a limit of three API keys. If your account has reached this limit, you can't use this feature in the mobile app until you delete one of the existing API keys. You can use the Console to delete API signing keys.

To delete an API signing key

The following procedure works for a regular user or an administrator. Administrators can delete an API key for either another user or themselves.
Welcome to Oracle Cloud Infrastructure

1. View the user's details:
   • If you're deleting an API key for yourself:
     Open the Profile menu (👤) and click User Settings.
   • If you're an administrator deleting an API key for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. For the API key you want to delete, click Delete.

3. Confirm when prompted.

The API key is no longer valid for sending API requests.

Securing Your Account if Your Device is Compromised

If you have automatic sign-in enabled in the Oracle Cloud Infrastructure Mobile app and your device is stolen, you need to secure your account. To secure your account, in the Console, delete your API signing keys.

Switching Regions

Your current region is displayed at the top of the mobile app. If your tenancy is subscribed to multiple regions, you can switch regions by selecting a different region from the Region picker.

Switching Time Zones

You can set the mobile app to use UTC time or local time. To switch the time zone:

1. In the app, open the Profile menu (👤) and then tap Settings.
2. In the Time zone menu, for Set time zone, select Local or UTC.

Navigating in the Mobile App

When you sign in to the app, you see the Home tab.

Home

• The Alarms section displays information about alarms fired within the last 24 hours. For more details, tap an alarm in the list, or navigate to the Alarms tab.
• Tap the tiles in the Resources menu to see details about that type of resource.
• For trial users, the Billing section displays current information about costs associated with resource usage.

In addition to the Home tab, the app has Alarms, Resources, and Limits tabs.

Alarms

The Alarms tab displays details about alarms fired within the last 24 hours. At the top of the tab, use the Compartment picker to select your compartment. To see details about a specific alarm, tap that alarm in the list. For more information about alarms, see Monitoring Overview.

Resources

The Resources tab displays details about a selection of resources. At the top of the tab, use the Compartment picker to select your compartment.

Currently, you can view details about the following types of resources in the mobile app:

• Compute instances
• Block volumes
• Object Storage
• Load balancers
• Autonomous Transaction Processing
Welcome to Oracle Cloud Infrastructure

- Autonomous Data Warehouse

Tap a section to see a list of resources of that type. At the top of the tab, use the Compartments picker to select your compartment. Use the Filter resources text box to search for resources using a free text search based on keywords. For more information, see Search Overview. The indicator next to the resource name tells you the status of the resource.

To see resource details, tap the resource name in the list. This action takes you to a view that displays information about that resource, including:

- Resource status
- Visualizations with metrics that let you monitor the health, capacity, and performance of your resources
- Metadata for the resource

Limits

The Limits tab displays details about your current service limits and usage. The service limit is the quota or allowance set on a resource. For example, your tenancy is allowed a maximum number of compute instances per availability domain. These limits are usually established with your Oracle sales representative when you purchase Oracle Cloud Infrastructure. For more information about service limits, see Service Limits.

To view limits, at the top of the Limits tab:

1. Filter the list to the limits you want to see:
   - Use the Compartments picker to select your compartment.
   - Use the Resource picker to select a service.
2. After making your selections, tap Search limits to see the list of limits and current usage.

Each item in the resulting list shows a description of the service limit, the current usage for that service, and the total limit available.

Signing Out

To sign out of the Oracle Cloud Infrastructure Mobile app, open the Profile menu (👤) and then tap Sign Out.

Contacting Support

To open a support request for the Oracle Cloud Infrastructure Mobile app, sign in to the Console on a computer and follow the steps to create a support request. When you create the request, in the issue summary, include the prefix OCI_Mobile to specify that the support request is for the mobile app. For more information, see Getting Help and Contacting Support on page 125.

To create a support ticket

1. Open the Help menu (",
   go to Support, and click Create support request.
2. Enter the following:
   - Issue Summary: Enter a title that summarizes your issue. Avoid entering confidential information.
   - Describe Your Issue: Provide a brief overview of your issue.
     - Include all the information that support needs to route and respond to your request. For example, "I am unable to connect to my Compute instance."
     - Include troubleshooting steps taken and any available test results.
   - Select the severity level for this request.
3. Click Create Request.

Changing Your Password

This topic describes how users can change their own passwords.
To Change Your Password
Procedure for Oracle Identity Cloud Service users

1. Open the Profile menu and click User Settings.

Your Oracle Cloud Infrastructure IAM service User Details page is displayed. Notice that your username is prefixed with the name of your IDCS federation, for example: oracleidentitycloudservice/User

2. The information banner at the top of the page tells you that your account is managed in Oracle Identity Cloud Service. Click the here link.
3. Your Identity Cloud Service User Details page is displayed. Notice that on this page, your username is displayed without the prefix.

![User Details Page](image)

4. Click Change Password.
5. Follow the instructions in the dialog to create a new password.

**Procedure for local Oracle Cloud Infrastructure users**

Use this procedure if your sign-in page looks like the following image and you sign in through Oracle Cloud Infrastructure.

![Sign In Page](image)

1. Sign in to the Console using the Oracle Cloud Infrastructure Username and Password.
2. After you sign in, go to the top-right corner of the Console, open the Profile menu and then click Change Password.

3. Enter the current password.

4. Follow the prompts to enter the new password, and then click Save New Password.

Checking Your Expenses and Usage

This topic describes how to analyze the Oracle Cloud Infrastructure costs associated with your account.

You can use the following cost-related tools in the Console, which can help you gain insight into your costs and attribution of Oracle Cloud Infrastructure resources:

- Budgets
- Cost Analysis
- Cost and Usage Reports

See Working with Costs Analysis Tools on page 55, and Billing and Payment Tools Overview on page 273 for more information.

Required IAM Policy

To enable users to monitor the costs associated with this account, you will have to grant them access by writing a policy. If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

See Required IAM Policy on page 281 for more information on the required policy statements. Also see Cost and Usage Reports Overview on page 278 for more information on cost and usage reports.

Working with Costs Analysis Tools

Cost Analysis is a visualization tool that helps you track and optimize your Oracle Cloud Infrastructure spending, allows you to generate charts, and download accurate, reliable tabular reports of aggregated cost data on your Oracle Cloud Infrastructure consumption. Use the tool for spot checks of spending trends and for generating reports.

To filter costs by dates
Welcome to Oracle Cloud Infrastructure

1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Cost Analysis.
2. In Start Date, select a date.
3. In End Date, select a date (within six months of the start date).
4. Click Apply Filters.

To filter costs by tags
1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Cost Analysis.
2. From Tag Key, select a tag.
3. Click Apply Filters.

To filter costs by compartments
1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Cost Analysis.
2. From Compartment, select a compartment.
3. Click Apply Filters.

To remove a compartment or tag filter
• When you filter costs, a label appears with the name of the tag or compartment filter. To clear that filter, click the x.

For more information on Cost Analysis, see Cost Analysis Overview on page 282.

Changing Your Payment Method

This topic describes how to upgrade to a paid account, or change your payment method. This topic also describes how to terminate your paid subscription.

Required IAM Policy

To upgrade to a paid account or change your credit card, you must be a member of the Administrators group. See The Administrators Group and Policy on page 2125.

Upgrade Your Free Account

Most new customers in the United States who create new accounts after January 28, 2019 can use these tools.

Note:

If you created your account prior to January 28, 2019 or from outside the United States, use the following links:
• To upgrade to a paid account, see Upgrade Your Free Oracle Cloud Promotion on page 35.
• To change your credit card, see Updating Your Billing Details.

To upgrade to Pay-as-You-Go
1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Payment Method.
2. Under Account Type, select Pay-as-You-Go.
3. Take one of the following actions:
   • Click Edit to review the current credit card
   • Click Add a Credit Card
4. Type or review your information and click Finish.
5. Read the terms and conditions and select the check box to indicate your agreement.
6. Click Start Paid Account.
To request a sales call
1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Payment Method.
2. Under Account Type, select Request a Sales Call.
3. Type a phone number, an email address, or both.
4. Click Submit.

To change your payment method
You cannot change the payment method for promotional accounts.
1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Payment Method.
2. Click Edit Card.
3. Type your information and click Finish.

Terminating Your Account
You can terminate your account at any time through a support request. From the time that your request has been duly processed, billing is stopped (even if you have running instances), and any running resources are terminated.

Adding Users
This chapter provides a quick hands-on tutorial for adding users and groups and creating simple policies to grant them permissions to work with Oracle Cloud Infrastructure resources.

Use these instructions to quickly add some users to try out features. To fully understand the features of IAM and how to manage access to your cloud resources, see "Overview of IAM" in the Oracle Cloud Infrastructure User Guide.

For an overview of user management for all Oracle Cloud services, see Managing Users, User Accounts, and Roles.

About Users, Groups, and Policies
A user’s permissions to access Oracle Cloud Infrastructure services comes from the groups to which they belong. The permissions for a group are defined by policies. Policies define what actions members of a group can perform, and in which compartments. Users can then access services and perform operations based on the policies set for the groups they are members of.

About Oracle Identity Cloud Service Federated Users
When you sign up for Oracle Cloud Infrastructure, your tenancy is federated with Oracle Identity Cloud Service (IDCS) as the identity provider. You can create users and groups in IDCS that you can use with your Oracle Cloud products. To give these users permissions in Oracle Cloud Infrastructure, you need to perform some steps in IDCS and some steps in Oracle Cloud Infrastructure.

You can create your IDCS users and groups directly in the Console. The examples in the following sections include examples of creating IDCS users who can use Oracle Cloud Infrastructure services.

For more details on managing federated users, see Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372.

You can also choose to use Oracle Cloud Infrastructure’s IAM service as your identity provider to manage users and groups exclusively in the IAM service. These users can have permissions to use Oracle Cloud Infrastructure services only. If you want to manage users in the IAM service, see Managing Users on page 2414.

Sample Users and Groups
To help you understand how to set up users with the access permissions they need, perform the following tasks to set up these two basic types of users:
• An IDCS federated user with full administrator permissions (Cloud Administrator)
• An IDCS federated user with permissions to use one compartment only
Add a User with Oracle Cloud Administrator Permissions

The user you create in this task will have full administrator permissions of the default administrator. This means that the user has full access to all compartments and can create and manage all resources in Oracle Cloud Infrastructure as well as other services managed through Oracle Identity Cloud Service. You must have Cloud Administrator permissions to complete this task.

Create a Cloud Administrator user

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
3. Click Create IDCS User.
4. In the Create IDCS User dialog enter the following:
   - **Username**: Enter a unique name or email address for the new user. The value will be the user's login to the Console and must be unique across all other users in your tenancy.
   - **Email**: Enter an email address for this user. The initial sign-in credentials will be sent to this email address.
   - **First Name**: Enter the user's first name.
   - **Last Name**: Enter the user's last name.
   - **Phone Number**: Optionally, enter a phone number.
   - **Groups**: You can skip this step. You will be granting this user full administrator privileges.
5. Click Create.
6. Click Email Password Instructions to send the password link and instructions to the user. If your email app does not launch, copy the reset instructions and manually email them to the user.
7. Click close to close the dialog. You are returned to the Users list on the Identity Provider Details page.
8. Click the name of the user you just created. The User Details page is displayed.
9. Click Manage Roles.
10. Select the check box next to Add Cloud Account Administrator Role.
11. Click Apply Role Settings.
12. A dialog confirms the entitlements granted to the user. To notify the user of these updates, click Send Email to User. Click Close to close the dialog.

Create a Compartment and Add a User with Access to It

In this example, create a compartment called "Sandbox" and then create a user with access to only that compartment.

Procedure Overview: To provide access to the Sandbox compartment and all the resources in it, you create a group (SandboxGroup), and then create a policy (SandboxPolicy) to define the access rule.

To enable access for users created in Identity Cloud Service, create a group in IDCS (IDCSSandboxGroup), and map it to the SandboxGroup.

Finally, create an IDCS user and add them to the IDCSSandboxGroup.

Create a sandbox compartment

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
2. Click Create Compartment.
3. Enter the following:
   - **Name**: Enter Sandbox.
   - **Description**: Enter a description (required), for example: Sandbox compartment for users to try out OCI.
4. Click **Create Compartment**.
   
   Your compartment is displayed in the list.

**Create an Oracle Cloud Infrastructure group**

Next, create the "SandboxGroup" that you will create the policy for.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Groups**.
2. Click **Create Group**.
3. In the **Create Group** dialog:
   
   • **Name:** Enter a unique name for your group, for example, SandboxGroup.
     
     Note that the name cannot contain spaces.
   
   • **Description:** Enter a description (required).
4. Click **Create**.

**Create a policy**

Create the policy to give the SandboxGroup permissions in the Sandbox compartment.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**.
2. Under **List Scope**, ensure that you are in your root compartment.
3. Click **Create Policy**.
4. Enter a unique **Name** for your policy, for example, SandboxPolicy.
   
   Note that the name cannot contain spaces.
5. Enter a **Description** (required), for example, Grants users full permissions on the Sandbox compartment.
6. Enter the following **Statement**:

   ```plaintext
   Allow group SandboxGroup to manage all-resources in compartment Sandbox
   ```

   This statement grants members of the SandboxGroup group full access to the Sandbox compartment.
7. Click **Create**.

**Create an Oracle Identity Cloud Service group**

Next, create the "IDCS_SandboxGroup" in Oracle Identity Cloud Service.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.
3. Under **Resources**, click **Groups**.
4. Click create **IDCS Group**.
5. In the **Create IDCS Group** dialog enter the following:
   
   • **Name:** Enter a unique name for your group, for example, IDCS_SandboxGroup.
     
     Note that the name cannot contain spaces.
   
   • **Description:** Enter a description (required).
6. Click **Create**.

   The group is created and it is displayed in the identity provider details page. Next, map the group.

**Map the Oracle Identity Cloud Service Group to the Oracle Cloud Infrastructure group**

Next, you need to map the Oracle Identity Cloud Service group to the Oracle Cloud Infrastructure group you created. The mapping gives the members of the IDCS group the permissions you granted to the OCI group.

1. On the identity provider details page, click **Group Mapping**. The group mappings are displayed.
2. Click **Edit Mapping**.
3. Click + Add Mapping.
4. From the **Identity Provider Group** menu list, choose the IDCS_SandboxGroup.

5. From the **OCI Group** menu list, select the SandboxGroup.

6. Click **Submit**.

Users that are members of the Oracle Identity Cloud Service groups mapped to the Oracle Cloud Infrastructure groups are now listed in the Console on the Users page. See **Managing User Capabilities for Federated Users** on page 2408 for more information on assigning these users additional credentials.

**Create a user**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.

2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.

3. Click **Create IDCS User**.

4. In the **Create IDCS User** dialog enter the following:

   - **Username**: Enter a unique name or email address for the new user. The value will be the user's login to the Console and must be unique across all other users in your tenancy.
   - **Email**: Enter an email address for this user. The initial sign-in credentials will be sent to this email address.
   - **First Name**: Enter the user's first name.
   - **Last Name**: Enter the user’s last name.
   - **Phone Number**: Optionally, enter a phone number.
   - **Groups**: Select the group you created in the previous step, for example, IDCS_SandboxGroup.

5. Click **Create**.

   The user is created in Oracle Identity Cloud Service. This user can't access their account until they complete the password reset steps.

6. Click **Email Password Instructions** to send the password link and instructions to the user.

   The password link is good for 24 hours. If the user does not reset their password in time, you can generate a new password link by clicking **Reset Password** for the user.

   When this user signs in they can see the compartments they have access to and they can only view, create, and manage resources in the Sandbox compartment. This user cannot create other users or groups.

**Oracle Cloud Infrastructure Tutorials**

---

After you create your **Free Trial account**, use these tutorials to get started.

- **Autonomous Database Quickstart**

  Create an instance in just a few clicks. Then load data into your database from Object Storage and query it.

- **Oracle APEX**

  Use APEX and Autonomous Database

  Oracle Application Express (APEX) is a low-code development framework that enables you to rapidly build modern, data-driven apps right from your browser - no additional tools required.
<table>
<thead>
<tr>
<th>Migrating To Oracle Cloud Infrastructure</th>
<th>Analyze data with Autonomous Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate MySQL on Amazon RDS to Always Free Autonomous Database. Launch an Always Free Linux instance and transfer your other application files to Object Storage.</td>
<td>Use Oracle Analytics Desktop (OAD) to visualize data in Autonomous Database. Use Oracle Machine Learning (OML) to try your hand at predictive analytics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Launch a Linux or Windows VM.</th>
<th>Launch a VM with the CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create your first virtual cloud network and launch an instance. Optionally, attach block storage to your instance.</td>
<td>Use the command line interface to launch a Linux instance or a Windows instance. This tutorial includes working with a compartment, creating a virtual cloud network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Get started with Object Storage</th>
<th>Launch and test a load balancer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create your first bucket and upload some objects.</td>
<td>Create a VCN and load balancer, then test it out.</td>
</tr>
</tbody>
</table>

**Tutorial - Launching Your First Linux Instance**

In this tutorial, you'll learn the basic features of Oracle Cloud Infrastructure by performing some guided steps to launch and connect to an instance. After your instance is up and running, you can optionally create and attach a block volume to your instance.

In this tutorial, you will:

- Create a cloud network and subnet that enables internet access
- Launch an instance
- Connect to the instance
- Add and attach a block volume
The following figure depicts the components you create in the tutorial.

### Task Flow to Launch an Instance

Linux instances use an SSH key pair instead of a password to authenticate a remote user. If you do not already have a key pair, your first task is to create one using common third-party tools (if you have OpenSSH, you can instead use a key pair that is generated by Oracle Cloud Infrastructure). Next, prepare for your instance by launching a cloud network with subnets. You will then launch your instance into one of the subnets and connect to it. If you want to attach some storage, continue with the tutorial to add a cloud block storage volume. When finished with the tutorial, be sure to terminate the resources that you created.

Prepare:
- Create a key pair.
- Choose a compartment for your resources.
- Create a cloud network.

Launch and connect:
- Launch an instance.
- Connect to your instance.

Add storage and clean up:
- Add a block volume (optional).
- Clean up your resources.
Creating a Key Pair

Linux instances use an SSH key pair instead of a password to authenticate a remote user. A key pair file contains a private key and public key. You keep the private key on your computer and provide the public key when you create an instance. When you connect to the instance using SSH, you provide the path to the private key in the SSH command.

**Caution:**
Anyone who has access to the private key can connect to the instance. Store the private key in a secure location.

If you're connecting to your instance from a computer that has OpenSSH installed, you can use a key pair that is generated by Oracle Cloud Infrastructure instead of creating your own key pair.

**Before You Begin**

- If you will connect to your instance from a Windows system using OpenSSH or from a UNIX-based system, you can use a key pair that is generated by Oracle Cloud Infrastructure and skip this step. OpenSSH should be installed on Windows 10 and Windows Server 2019. Proceed to Choosing a Compartment on page 63.
- If you already have an SSH-2 RSA key pair, you can use your existing key pair and skip this step. Proceed to Choosing a Compartment on page 63.
- If you will connect to your instance from a Windows system that does not have OpenSSH, download and install the PuTTY Key Generator from http://www.putty.org.

**Creating an SSH Key Pair on Windows Using PuTTY Key Generator**

1. Find `puttygen.exe` in the PuTTY folder on your computer, for example, C:\Program Files (x86)\PuTTY. Double-click `puttygen.exe` to open it.
2. Specify a key type of SSH-2 RSA and a key size of 2048 bits:
   - In the Key menu, confirm that the default value of SSH-2 RSA key is selected.
   - For the Type of key to generate, accept the default key type of RSA.
   - Set the Number of bits in a generated key to 2048 if it is not already set.
3. Click Generate.
4. Move your mouse around the blank area in the PuTTY window to generate random data in the key.
   When the key is generated, it appears under Public key for pasting into OpenSSH authorized_keys file.
5. A Key comment is generated for you, including the date and time stamp. You can keep the default comment or replace it with your own more descriptive comment.
6. Leave the Key passphrase field blank.
7. Click Save private key, and then click Yes in the prompt about saving the key without a passphrase.
   The key pair is saved in the PuTTY Private Key (PPK) format, which is a proprietary format that works only with the PuTTY tool set.
   You can name the key anything you want, but use the .ppk file extension. For example, mykey.ppk.
8. Select all of the generated key that appears under Public key for pasting into OpenSSH authorized_keys file, copy it using Ctrl + C, paste it into a text file, and then save the file in the same location as the private key.
   (Do not use Save public key because it does not save the key in the OpenSSH format.)
   You can name the key anything you want, but for consistency, use the same name as the private key and a file extension of pub. For example, mykey.pub.
9. Write down the names and location of your public and private key files. You will need the public key when launching an instance. You will need the private key to access the instance via SSH.

**Choosing a Compartment**

Compartments help you organize and control access to your resources. A compartment is a collection of related resources (such as cloud networks, compute instances, or block volumes) that can be accessed only by those groups
that have been given permission by an administrator in your organization. For example, one compartment could contain all the servers and storage volumes that make up the production version of your company's Human Resources system. Only users with permission to that compartment can manage those servers and volumes.

In this tutorial you use one compartment for all your resources. When you are ready to create a production environment you will most likely separate these resources in different compartments.

**Before You Begin**

Sign in to the Console.

**Choosing a Compartment**

To begin working with a service, you must first select a service, and then select a compartment that you have permissions in.

1. In this tutorial, the first resource you create is the cloud network. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.

2. Select the Sandbox compartment (or the compartment designated by your administrator) from the list on the left, as shown in the image. If the Sandbox compartment does not exist, you can create it as described in Creating a Compartment.

**Creating a Compartment**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Compartments**.

2. Click **Create Compartment**.

3. Enter the following:
   - **Name**: Enter "Sandbox".
   - **Description**: Enter a description (required), for example: "Sandbox compartment for the getting started tutorial".
   - **Parent Compartment**: Select the compartment you want this compartment to reside in. Defaults to the root compartment (or tenancy).

4. Click **Create Compartment**.

Your compartment is displayed in the list.

5. Return to Choosing a Compartment.

When you select the Sandbox compartment, you will only see resources that are in the Sandbox. When you create new resources you will be prompted to choose the compartment to create them in, but your current compartment will be the default. If you change compartments, you must come back to the Sandbox compartment to see the resources that were created there.
Creating a Virtual Cloud Network

Before you can launch an instance, you need to have a virtual cloud network (VCN) and subnet to launch it into. A subnet is a subdivision of your VCN. The subnet directs traffic according to a route table. For this tutorial, you'll access the instance over the internet using its public IP address, so your route table will direct traffic to an internet gateway. The subnet also uses a security list to control traffic in and out of the instance.

For information about VCN features, see “Overview of Networking” in the Oracle Cloud Infrastructure User Guide.

Before You Begin

• You or an administrator has created a compartment for your network. See Choosing a Compartment on page 63.

Create a Cloud Network Plus Related Resources

Tip:
The Console offers two choices when you create a VCN: to create only the VCN, or to create the VCN with several related resources that are necessary if you want to immediately launch an instance. To help you get started quickly, the following procedure creates the VCN plus the related resources.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.

   Ensure that the Sandbox compartment (or the compartment designated for you) is selected in the Compartment list on the left.

2. Click Networking Quickstart.

3. Select VCN with Internet Connectivity, and then click Start Workflow.

4. Enter the following:

   • **VCN Name**: Enter a name for your cloud network. The name is incorporated into the names of all the related resources that are automatically created. Avoid entering confidential information.
   • **Compartment**: This field defaults to your current compartment. Select the compartment you want to create the VCN and related resources in, if not already selected.
   • **VCN CIDR Block**: Enter a valid CIDR block for the VCN. For example 10.0.0.0/16.
   • **Public Subnet CIDR Block**: Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block. For example: 10.0.0.0/24.
   • **Private Subnet CIDR Block**: Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block and not overlap with the public subnet's CIDR block. For example: 10.0.1.0/24.
   • Accept the defaults for any other fields.

5. Click Next.

6. Review the list of resources that the workflow will create for you. Notice that the workflow will set up security list rules and route table rules to enable basic access for the VCN.

7. Click Create to start the short workflow.

8. After the workflow completes, click View Virtual Cloud Network.

The cloud network has the following resources and characteristics:

• Internet gateway.
• NAT gateway.
• Service gateway with access to the Oracle Services Network.
• A regional public subnet with access to the internet gateway. This subnet uses the VCN's default security list and default route table. Instances in this subnet may optionally have public IP addresses.
• A regional private subnet with access to the NAT gateway and service gateway. This subnet uses a custom security list and custom route table that the workflow created. Instances in this subnet cannot have public IP addresses.
• Use of the Internet and VCN Resolver for DNS.
Welcome to Oracle Cloud Infrastructure

Important:
This simple cloud network is designed to make it easy to launch an instance when trying out Oracle Cloud Infrastructure. When you create your production instances, ensure that you create appropriate security lists and route table rules to restrict network traffic to your instances.

What’s Next
Now you can launch an instance. See Launching a Linux Instance on page 66.

Launching a Linux Instance
Now you will launch an instance with the Oracle Linux image and basic shape. More advanced options are available; see "Managing Instances" in the Oracle Cloud Infrastructure User Guide for more information.

Before You Begin
• You have created a virtual cloud network (VCN) and public subnet. See Creating a Virtual Cloud Network on page 65.
• If you will connect to your instance from a Windows system that does not have OpenSSH, you have a created an SSH key pair. See Creating a Key Pair on page 63.

Launching an Instance
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click Create Instance.
3. Enter a name for the instance, for example: <your initials> _Instance. Avoid entering confidential information.
4. In the Placement and hardware section, make the following selections:
   a. Accept the default Availability domain.
   b. In the Image section, accept the default, Oracle Linux 7.x.
   c. In the Shape section, click Change Shape. Then, do the following:
      1. For Instance type, accept the default, Virtual Machine.
      2. For Shape series, select Intel Skylake, and then choose the VM.Standard2.1 shape (1 OCPU, 15 GB RAM).

Tip:
To create an instance using the Always Free-eligible VM.Standard.E2.1.Micro shape, select Specialty and Legacy, and then choose the VM.Standard.E2.1.Micro shape. If the Micro shape
Welcome to Oracle Cloud Infrastructure

is disabled, cancel out of the shape selection page, select a different availability domain, and then try again.

The shape defines the number of CPUs and amount of memory allocated to the instance.

3. Click Select Shape.

5. In the Networking section, configure the network details for the instance:

   • For Network, leave Select existing virtual cloud network selected.
   • Virtual cloud network in <compartment_name>: Select the cloud network that you created. If necessary, click Change compartment to switch to the compartment containing the cloud network that you created.
   • For Subnet, leave Select existing subnet selected.
   • Subnet in <compartment_name>: Select the public subnet that was created with your cloud network. If necessary, click Change compartment to switch to the compartment containing the correct subnet.
   • Leave the Use network security groups to control traffic check box cleared.
   • Select the Assign a public IPv4 address option. This creates a public IP address for the instance, which you need to access the instance. If you have trouble selecting this option, confirm that you selected the public subnet that was created with your VCN, not a private subnet.

6. In the Add SSH keys section, select one of the following options:

   • Generate SSH keys: If you will connect to the instance using OpenSSH, select this option. Click Save Private Key and then save the private key on your computer. Optionally, click Save Public Key and then save the public key.

      Caution:
      Anyone who has access to the private key can connect to the instance.
      Store the private key in a secure location.

   • Choose SSH key files: If you will connect to the instance using PuTTY, select this option. To upload the public key portion of the key pair that you want to use for SSH access to the instance, browse to the key file that you want to upload, or drag and drop the file into the box.

7. In the Boot volume section, leave all the options cleared.

8. Click Create.

The instance is displayed in the Console in a provisioning state. Expect provisioning to take several minutes before the state updates to running. Do not refresh the page. After the instance is running, allow another few minutes for the operating system to boot before you attempt to connect.

Getting the Instance Public IP Address

To connect to the instance in the next step, you'll need its public IP address.

To get the instance public IP address:

1. Click the instance name to see its details.
2. The **Public IP Address** and **Username** are displayed on the details page under **Instance Access**, as shown in the following image:

![Instance Access Image]

3. Make a note of the **Public IP Address** before you continue.

### Connecting to Your Instance

You connect to a running Linux instance using a Secure Shell (SSH) connection. Most Linux distributions include an SSH client by default. Windows 10 and Windows Server 2019 systems should include the **OpenSSH client**, which you’ll need if you created your instance using the SSH keys generated by Oracle Cloud Infrastructure. For other Windows versions, you can download a free SSH client called PuTTY from [http://www.putty.org](http://www.putty.org).

**Before You Begin**

- You know the public IP address of your instance. See Launching a Linux Instance on page 66.
- You know the path to the private key file.

**Connecting to Your Linux Instance Using SSH**

Log in to the instance using SSH.

**To connect to a Linux instance from a Unix-style system**
1. Use the following command to set the file permissions so that only you can read the file:

```
chmod 400 <private_key_file>
```

\(<private_key_file>\) is the full path and name of the file that contains the private key associated with the instance you want to access.

2. Use the following SSH command to access the instance.

```
ssh -i <private_key_file> <username>@<public-ip-address>
```

\(<private_key_file>\) is the full path and name of the file that contains the private key associated with the instance you want to access.

\(<username>\) is the default username for the instance. For Oracle Linux and CentOS images, the default username is opc. For Ubuntu images, the default username is ubuntu.

\(<public-ip-address>\) is your instance IP address that you retrieved from the Console.

**To connect to a Linux instance from a Windows system using OpenSSH**

If the instance uses a key pair that was generated by Oracle Cloud Infrastructure, use the following procedure.

1. If this is the first time you are using this key pair, you must set the file permissions so that only you can read the file. Do the following:
   a. In Windows Explorer, navigate to the private key file, right-click the file, and then click Properties.
   c. Ensure that the Owner is your user account.
   d. Click Disable Inheritance, and then select Convert inherited permissions into explicit permissions on this object.
   e. Select each permission entry that is not your user account and click Remove.
   f. Ensure that the access permission for your user account is Full control.
   g. Save your changes.

2. To connect to the instance, open Windows PowerShell and run the following command:

```
ssh -i <private_key_file> <username>@<public-ip-address>
```

\(<private_key_file>\) is the full path and name of the file that contains the private key associated with the instance you want to access.

\(<username>\) is the default username for the instance. For Oracle Linux and CentOS images, the default username is opc. For Ubuntu images, the default username is ubuntu.

\(<public-ip-address>\) is your instance IP address that you retrieved from the Console.

**To connect to a Linux instance from a Windows system using PuTTY**

SSH private key files generated by Oracle Cloud Infrastructure are not compatible with PuTTY. If you are using a private key file generated during the instance creation process you need to convert the file to a .ppk file before you can use it with PuTTY to connect to the instance.

**Convert a generated .key private key file:**

1. Open PuTTYgen.
2. Click Load, and select the private key generated when you created the instance. The extension for the key file is .key.
3. Click Save private key.
4. Specify a name for the key. The extension for new private key is .ppk.
5. Click Save.

**Connect to the Linux instance using a .ppk private key file:**
If the instance uses a key pair that you created using PuTTY Key Generator, use the following procedure.

1. Open PuTTY.
2. In the Category pane, select Session and enter the following:
   • Host Name (or IP address):
     
     <username>@<public-ip-address>

     <username> is the default username for the instance. For Oracle Linux and CentOS images, the default username is opc. For Ubuntu images, the default username is ubuntu.

     <public-ip-address> is your instance public IP address that you retrieved from the Console
   • Port: 22
   • Connection type: SSH
3. In the Category pane, expand Window, and then select Translation.
4. In the Remote character set drop-down list, select UTF-8. The default locale setting on Linux-based instances is UTF-8, and this configures PuTTY to use the same locale.
5. In the Category pane, expand Connection, expand SSH, and then click Auth.
6. Click Browse, and then select your .ppk private key file.
7. Click Open to start the session.

If this is your first time connecting to the instance, you might see a message that the server’s host key is not cached in the registry. Click Yes to continue the connection.

**Tip:**

If the connection fails, you may need to update your PuTTY proxy configuration.

### Running Administrative Tasks on the Instance

When you’re logged in as the default user, opc, you can use the `sudo` command to run administrative tasks.

### What’s Next

Now that you’ve got an instance and have successfully connected to it, consider the following next steps:

- Install software on the instance.
- Add a block volume. See Adding a Block Volume on page 70.
- Add more users to work with Oracle Cloud Infrastructure. See Adding Users on page 57.
- Allow additional users to connect to your instance. See Adding Users on an Instance on page 737.
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See Cleaning Up Resources from the Tutorial on page 72.

If you’re having trouble connecting, see Troubleshooting the SSH Connection on page 737.

### Adding a Block Volume

Block Volume provides network storage to use with your Oracle Cloud Infrastructure instances. After you create, attach, and mount a volume to your instance, you can use it just as you would a physical hard drive on your computer. A volume can be attached to a single instance at a time, but you can detach it from one instance and attach to another instance, keeping your data intact.

This task shows you how to create a volume, attach it to an instance, and then connect the volume to the instance.

For complete details on Block Volume, see "Overview of Block Volume" in the Oracle Cloud Infrastructure User Guide.

#### Creating a Volume

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. Click Create Block Volume.
3. In the **Create Block Volume** dialog, enter the following:

   - **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the volume in, if not already selected.
   - **Name:** Enter a user-friendly name. Avoid entering confidential information.
   - **availability domain:** Select the same **availability domain** that you selected for your instance. If you followed the tutorial instructions when launching your instance, this is the first AD in the list. The volume and the instance must be in the same availability domain.
   - **Size:** Enter 50 to create a 50 GB block volume.
   - **Backup Policy:** Do not select a backup policy.
   - **Tags:** Leave the tagging fields blank.

4. Click **Create Block Volume**.

   A 50 GB block volume is displayed in the provisioning state. When the volume is no longer in the provisioning state, you can attach it to your instance.

**Attaching the Volume to an Instance**

Next you attach the volume via an **iSCSI** network connection to your instance:

1. Find your instance: Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click your instance name to view its details.
3. In the **Resources** section, click **Attached Block Volumes**.
4. Click **Attach Block Volume**.
5. Enter the following:
   - **Select ISCSI**.
   - **Block Volume Compartment:** Select the compartment where you created the block volume.
   - **Select Volume:** Select this option.
   - **Block Volume:** Select the block volume from the list.
   - **Device Path:** If the instance supports consistent device paths, you will see a list of device paths. Select one from the list.
   - **Require CHAP Credentials:** Leave cleared.

   **Tip:**

   **CHAP** is a security protocol. You can leave this box cleared for the purposes of the tutorial. When you set up your production environment, Oracle recommends requiring CHAP credentials.

6. Click **Attach**.

**Connecting to the Volume**

After your volume is attached, you can configure the iSCSI connection. You connect to the volume using the `iscsiadm` command-line tool. The commands you need to configure, authenticate, and log on are provided by the Console so you can easily copy and paste them into your instance session window. After the connection is configured, you can mount the volume on your instance and use it just as you would a physical hard drive.

To connect to your volume:

1. Log on to your instance as described in **Connecting to Your Instance** on page 68.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click your instance name to view its details.
4. In the **Resources** section, click **Attached Block Volumes**.
5. Click the Actions icon (three dots) next to the volume you just attached and then click **iSCSI Commands and Information**.

   The **iSCSI Commands and Information** dialog is displayed. Notice that the dialog displays specific identifying information about your volume (such as IP address and port) as well as the iSCSI commands you'll need to use. The commands are ready to use with the appropriate information already included in each command.

6. The **Attach Commands** configure the iSCSI connection and log on to iSCSI. Copy and paste each command from the **Attach Commands** list into the instance session window.

   Be sure to paste and run each command individually. There are three attach commands. Each command begins with `sudo iscsiadm`.

7. After entering the final command to log on to iSCSI, you are ready to format (if needed) and mount the volume. To get a list of mountable iSCSI devices on the instance, run the following command:

   ```
   sudo fdisk -l
   ```

   If your disk attached successfully, you'll see it in the returned list as follows:

   ```
   Disk /dev/sdb: 50.0 GB, 50010783744 bytes, 97677312 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 4096 bytes / 1048576 bytes
   ```

   **Important:**

   Connecting to Volumes on Linux Instances

   When connecting to volumes on Linux instances, if you want to automatically mount these volumes on instance boot, you need to use some specific options in the `/etc/fstab` file, or the instance may fail to launch. See Traditional fstab Options on page 528 and fstab Options for Block Volumes Using Consistent Device Paths on page 527 for more information.

**What's Next**

Now that you've got an instance running and attached some storage, consider the following next steps:

- Install your own software on the instance.
- Add more users to work with Oracle Cloud Infrastructure. See Adding Users on page 57.
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See Cleaning Up Resources from the Tutorial on page 72.

**Cleaning Up Resources from the Tutorial**

After you've finished with the resources you created for this tutorial, clean up by terminating the instance and deleting the resources you don't intend to continue working with.

**Detach and Delete the Block Volume**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Find your instance in the Instances list and click its name to display its details.
3. In the Resources section on the Instance Details page, click Attached Block Volumes.
4. Find your volume, click the Actions icon (three dots), and then click Detach.
5. Click Continue Detachment and then click OK.
6. When the Console shows the volume status as Detached, you can delete the volume. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
7. Find your volume, click the Actions icon (three dots), and then click Terminate. Confirm when prompted.
Terminate the Instance
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the list of instances, find the instance you created in the tutorial.
3. Click the Actions icon (three dots), and then click Terminate.
4. Select the Permanently delete the attached boot volume check box, and then click Terminate Instance.

Delete the Virtual Cloud Network
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. In the list of VCNs, find the one you created in the tutorial.
3. Click the Actions icon (three dots), and then click Terminate.
4. Click Terminate All to delete all the underlying resources of your VCN.
   When all the resources are successfully deleted you can close the dialog.

Tutorial - Launching Your First Windows Instance

In this tutorial you'll learn the basic features of Oracle Cloud Infrastructure by performing some guided steps to launch and connect to a Windows instance. After your instance is up and running, you can optionally create and attach a block volume to your instance.

In this tutorial you will:
• Create a cloud network and subnet that enables internet access
• Launch an instance
• Connect to the instance
• Add and attach a block volume

The following figure depicts the components you create in the tutorial.
Welcome to Oracle Cloud Infrastructure

Task Flow to Launch a Windows Instance

You will connect to your instance using Remote Desktop Connection and a one-time password that is created when you launch the instance. Before you can launch the instance, you must create a virtual cloud network (VCN) with subnets. You will then launch your instance into one of the subnets of your VCN and connect to it. If you want to attach some storage, continue with the tutorial to add a cloud block storage volume. When finished with the tutorial, be sure to terminate the resources that you created.

Prepare:
- Choose a compartment for your resources.
- Create a cloud network.

Launch and connect:
- Launch a Windows instance.
- Connect to your Windows instance.

Add storage and clean up:
- Add a block volume (optional).
- Clean up your resources.

Choosing a Compartment

Compartments help you organize and control access to your resources. A compartment is a collection of related resources (such as cloud networks, compute instances, or block volumes) that can be accessed only by those groups that have been given permission by an administrator in your organization. For example, one compartment could contain all the servers and storage volumes that make up the production version of your company's Human Resources system. Only users with permission to that compartment can manage those servers and volumes.
In this tutorial you use one compartment for all your resources. When you are ready to create a production environment you will most likely separate these resources in different compartments.

**Before You Begin**

Sign in to the Console.

**Choosing a Compartment**

To begin working with a service, you must first select a service, and then select a compartment that you have permissions in.

1. In this tutorial, the first resource you create is the cloud network. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Select the Sandbox compartment (or the compartment designated by your administrator) from the list on the left, as shown in the image. If the Sandbox compartment does not exist, you can create it as described in Creating a Compartment.

![Virtual Cloud Networks in Sandbox Compartment](image)

**Creating a Compartment**

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
2. Click Create Compartment.
3. Enter the following:
   - **Name:** Enter "Sandbox".
   - **Description:** Enter a description (required), for example: "Sandbox compartment for the getting started tutorial".
   - **Parent Compartment:** Select the compartment you want this compartment to reside in. Defaults to the root compartment (or tenancy).
4. Click Create Compartment.
   - Your compartment is displayed in the list.
5. Return to Choosing a Compartment.

When you select the Sandbox compartment, you will only see resources that are in the Sandbox. When you create new resources you will be prompted to choose the compartment to create them in, but your current compartment will be the default. If you change compartments, you must come back to the Sandbox compartment to see the resources that were created there.

**Creating a Virtual Cloud Network**

Before you can launch an instance, you need to have a virtual cloud network (VCN) and subnet to launch it into. A subnet is a subdivision of your VCN. The subnet directs traffic according to a route table. For this tutorial, you'll access the instance over the internet using its public IP address, so your route table will direct traffic to an internet gateway. The subnet also uses a security list to control traffic in and out of the instance.
For information about VCN features, see “Overview of Networking” in the *Oracle Cloud Infrastructure User Guide*.

**Before You Begin**

- You or an administrator has created a compartment for your network. See Choosing a Compartment on page 74.

**Create a Cloud Network Plus Related Resources**

**Tip:**

The Console offers two choices when you create a VCN: to create only the VCN, or to create the VCN with several related resources that are necessary if you want to immediately launch an instance. To help you get started quickly, the following procedure creates the VCN plus the related resources.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.

   Ensure that the Sandbox compartment (or the compartment designated for you) is selected in the Compartment list on the left.

2. Click Networking Quickstart.

3. Select VCN with Internet Connectivity, and then click Start Workflow.

4. Enter the following:

   - **VCN Name:** Enter a name for your cloud network. The name is incorporated into the names of all the related resources that are automatically created. Avoid entering confidential information.
   - **Compartment:** This field defaults to your current compartment. Select the compartment you want to create the VCN and related resources in, if not already selected.
   - **VCN CIDR Block:** Enter a valid CIDR block for the VCN. For example 10.0.0.0/16.
   - **Public Subnet CIDR Block:** Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block. For example: 10.0.0.0/24.
   - **Private Subnet CIDR Block:** Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block and not overlap with the public subnet's CIDR block. For example: 10.0.1.0/24.
   - Accept the defaults for any other fields.

5. Click Next.

6. Review the list of resources that the workflow will create for you. Notice that the workflow will set up security list rules and route table rules to enable basic access for the VCN.

7. Click Create to start the short workflow.

8. After the workflow completes, click View Virtual Cloud Network.

The cloud network has the following resources and characteristics:

- Internet gateway.
- NAT gateway.
- Service gateway with access to the Oracle Services Network.
- A regional public subnet with access to the internet gateway. This subnet uses the VCN's default security list and default route table. Instances in this subnet may optionally have public IP addresses.
- A regional private subnet with access to the NAT gateway and service gateway. This subnet uses a custom security list and custom route table that the workflow created. Instances in this subnet cannot have public IP addresses.
- Use of the Internet and VCN Resolver for DNS.

**Important:**

This simple cloud network is designed to make it easy to launch an instance when trying out Oracle Cloud Infrastructure. When you create your production instances, ensure that you create appropriate security lists and route table rules to restrict network traffic to your instances.
Edit the Default Security List to Allow Traffic to Your Windows Instance

To enable network traffic to reach your Windows instance, you need to add a security list rule to enable Remote Desktop Protocol (RDP) access. Specifically, for the default security list (which is used by the public subnet), you need a stateful ingress rule for TCP traffic on destination port 3389 from source 0.0.0.0/0 and any source port.

To edit the VCN’s security list:

1. Click the name of the VCN that you just created. Its details are displayed.
3. Click the default security list for your VCN.
   Its details are displayed.
4. Click Add Ingress Rules.
5. Enter the following for your new rule:
   a. Source Type: CIDR
   b. Source CIDR: 0.0.0.0/0
   c. IP Protocol: RDP (TCP/3389)
   d. Source Port Range: All
   e. Destination Port Range: 3389
6. When done, click Add Ingress Rules.

What’s Next

Now you can launch an instance. See Launching a Windows Instance on page 77.

Launching a Windows Instance

Now you will launch an instance with the Oracle Windows image and basic shape. More advanced options are available, see "Managing Instances" in the Oracle Cloud Infrastructure User Guide for more information.

Before You Begin

• You have created a virtual cloud network (VCN) and public subnet. See Creating a Virtual Cloud Network on page 75.

Launching an Instance

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click Create Instance.
3. Enter a name for the instance, for example: <your initials>_Instance. Avoid entering confidential information.

Important:
Use only these ASCII characters in the instance name: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and hyphens (-). See this known issue for more information.

4. In the Placement and hardware section, make the following selections:
   a. Accept the default Availability domain.
   b. In the Image section, click Change Image. Then, do the following:
      1. In the Image source list, select Platform Images.
      3. Review and accept the terms of use, and then click Select Image.
   c. In the Shape section, click Change Shape. Then, do the following:
      1. For Instance type, accept the default, Virtual Machine.
      2. For Shape series, select Intel Skylake, and then choose the VM.Standard2.1 shape (1 OCPU, 15 GB RAM).

      The shape defines the number of CPUs and amount of memory allocated to the instance.
   3. Click Select Shape.

5. In the Networking section, configure the network details for the instance. Do not accept the defaults.
   • For Network, leave Select existing virtual cloud network selected.
   • Virtual cloud network in <compartment_name>: Select the cloud network that you created. If necessary, click Change compartment to switch to the compartment containing the cloud network that you created.
   • For Subnet, leave Select existing subnet selected.
   • Subnet in <compartment_name>: Select the public subnet that was created with your cloud network. If necessary, click Change compartment to switch to the compartment containing the correct subnet.
   • Leave the Use network security groups to control traffic check box cleared.
   • Select the Assign a public IPv4 address option. This creates a public IP address for the instance, which you need to access the instance. If you have trouble selecting this option, confirm that you selected the public subnet that was created with your VCN, not a private subnet.

6. In the Boot volume section, leave all the options cleared.
7. Click Create.

The instance is displayed in the Console in a provisioning state. Expect provisioning to take several minutes before the state updates to Running. Do not refresh the page. After the instance is running, allow another few minutes for the operating system to boot before you attempt to connect.

Getting the Instance Public IP Address and Initial Windows Password

To connect to the instance in the next step, you'll need its public IP address and initial password.

To get the instance public IP address and initial password:
1. Click the instance name to see its details.
2. The **Public IP Address**, **Username**, and **Initial Password** are displayed on the details page, as shown in the following image:

3. To view the **Initial Password**, click **Show**. Although the Console offers a copy option, the paste option is typically not available when you are prompted to enter the password, so be prepared to enter it manually.

4. When you are ready to connect to the instance, make a note of both the public IP address and the initial password.

### Connecting to Your Windows Instance

You connect to a running Windows instance using Remote Desktop.

#### Before You Begin

- You know the public IP address and initial password of your instance, see [Launching a Windows Instance](#) on page 77.
- You have Remote Desktop installed.

#### Connecting to Your Windows Instance from a Remote Desktop Client

1. Open the Remote Desktop client.
2. In the **Computer** field, enter the public IP address that you retrieved from the Console.
3. The **User name** is opc. Depending on the Remote Desktop client you are using, you might have to connect to the instance before you can enter this credential.
4. Click **Connect** to start the session.
5. Accept the certificate if you are prompted to do so.
6. Enter the initial password that you retrieved from the Console. You will be prompted to change the password as soon as you log in.
   
   Your new password must be at least 12 characters long and must comply with Microsoft's password policy.
7. Press **Enter**.

### Running Administrative Tasks on the Instance

The default user, opc, has administrative privileges.

### What's Next

Now that you've got an instance and have successfully connected to it, consider the following next steps:
Welcome to Oracle Cloud Infrastructure

- Install software on the instance.
- Add a block volume. See Adding a Block Volume to a Windows Instance on page 80.
- Add more users to work with Oracle Cloud Infrastructure. See Adding Users on page 57.
- Allow additional users to connect to your instance. See Adding Users on an Instance on page 737.
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See Cleaning Up Resources from the Tutorial on page 81.

If you're having trouble connecting, see Troubleshooting the SSH Connection on page 737.

Adding a Block Volume to a Windows Instance

Block Volume provides network storage to use with your Oracle Cloud Infrastructure instances. After you create, attach, and mount a volume to your instance, you can use it just as you would a physical hard drive on your computer. A volume can be attached to a single instance at a time, but you can detach it from one instance and attach to another instance, keeping your data intact.

This task shows you how to create a volume, attach it to an instance, and then connect the volume to the instance.

For complete details on Block Volume, see "Managing Volumes" in the Oracle Cloud Infrastructure User Guide.

Creating a Volume

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. Click Create Block Volume.
3. In the Create Block Volume dialog box, enter the following:
   a. Create in Compartment: This field defaults to your current compartment. Select the compartment you want to create the volume in, if not already selected.
   b. Name: Enter a user-friendly name. Avoid entering confidential information.
   c. availability domain: Select the same availability domain that you selected for your instance. If you followed the tutorial instructions when launching your instance, this will be the first availability domain in the list. The volume and the instance must be in the same availability domain.
   d. Size: Enter 256 to create a 256 GB block volume.
4. Click Create Block Volume.

A 256 GB block volume is displayed in the list in the provisioning state. When the volume is no longer in the provisioning state, you can attach it to your instance.

Attaching the Volume to an Instance

Next you attach the volume via an iSCSI network connection to your instance:

1. Find your instance: Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click your instance name to view its details.
3. In the Resources section, click Attached Block Volumes.
4. Click Attach Block Volume.
5. Enter the following:
   a. Block Volume Compartment: Select the compartment where you created the block volume.
   b. Block Volume: Select the block volume from the list.
   c. Require CHAP Credentials: Leave cleared.

Tip:

CHAP is a security protocol. You can leave this box cleared for the purposes of the tutorial. When you set up your production environment, Oracle recommends requiring CHAP credentials.

6. Click Attach.
Connecting to the Volume

After your volume is attached, you can configure the iSCSI connection. After the connection is configured, you can mount the volume on your instance and use it just as you would a physical hard drive.

To connect to your volume:

1. Log on to your instance as described in Connecting to Your Windows Instance on page 79.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click your instance name to view the instance details.
4. In the Resources section, click Attached Block Volumes.
5. Click the Actions icon (three dots) next to the volume you just attached and then click iSCSI Commands and Information.

The iSCSI Commands and Information dialog box opens. Notice that the dialog box displays specific identifying information about your volume (such as IP address and port) as well as the iSCSI commands that you can use.

6. On your Windows instance, open the iSCSI Initiator.
   For example: Open Server Manager, click Tools, and select iSCSI Initiator.
7. In the iSCSI Initiator Properties dialog box, click the Discovery tab.
8. Click Discover Portal.
9. Enter the block volume IP address and port. Click OK.
10. Click the Targets tab.
11. In the Discovered Targets region, select the volume IQN.
12. Click Connect and then click OK to close the dialog.
13. You are now ready to format (if needed) and mount the volume. To get a list of mountable iSCSI devices on the instance, in Server Manager, click File and Storage Services and then click Disks.

   The 256 GB disk is displayed in the list.

What's Next

Now that you've got an instance running and attached some storage, consider the following next steps:

- Install your own software on the instance.
- Add more users to work with Oracle Cloud Infrastructure. See Adding Users on page 57.
- Or, if you are finished with your instance, delete the resources that you created in the tutorial. See Cleaning Up Resources from the Tutorial on page 81.

Cleaning Up Resources from the Tutorial

After you've finished with the resources you created for this tutorial, clean up by terminating the instance and deleting the resources you don't intend to continue working with.

Detach and Delete the Block Volume

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Find your instance in the Instances list and click its name to display its details.
3. In the Resources section on the Instance Details page, click Attached Block Volumes.
4. Find your volume, click the Actions icon (three dots), and then click Detach.
5. Click Continue Detachment and then click OK.
6. When the Console shows the volume status as Detached, you can delete the volume. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
7. Find your volume, click the Actions icon (three dots), and then click Terminate. Confirm when prompted.

Terminate the Instance

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the list of instances, find the instance you created in the tutorial.
3. Click the Actions icon (three dots), and then click **Terminate**.
4. Select the **Permanently delete the attached boot volume** check box, and then click **Terminate Instance**.

**Delete the Virtual Cloud Network**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. In the list of VCNs, find the one you created in the tutorial.
3. Click the Actions icon (three dots), and then click **Terminate**.
4. Click **Terminate All** to delete all the underlying resources of your VCN.

When all the resources are successfully deleted you can close the dialog.

**Putting Data into Object Storage**

Object Storage provides reliable, secure, and scalable object storage. Object storage is a storage architecture that stores and manages data as objects. Some typical use cases include data backup, file sharing, and storing unstructured data like logs and sensor-generated data.

Object Storage uses buckets to organize your files. To use Object Storage, first create a bucket and then begin adding data files.

Use this procedure to quickly get started. For more details, see "Overview of Object Storage" in the *Oracle Cloud Infrastructure User Guide*.

**Creating a Bucket**

To create a bucket to store objects:

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
   
   A list of the buckets in the compartment you're viewing is displayed.

2. Select a compartment from the **Compartment** list on the left side of the page.

   A list of existing buckets is displayed.

3. Click **Create Bucket**.

4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   
   - **Bucket Name**: The system generates a default bucket name that reflects the current year, month, day, and time, for example **bucket-20190306-1359**. If you change this default to any other bucket name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
   
   - **Default Storage Tier**: Select the default tier in which you want to store your data. Once set, you cannot change the default storage tier of a bucket. When you upload objects, this tier will be selected by default. You can, however, select a different tier. Available default tiers include:
     
     - **Standard** is the primary, default storage tier used for Object Storage service data. Use the **Standard** tier for storing frequently accessed data that requires fast and immediate access.
     
     - **Archive** is the default storage tier used for Archive Storage service data. Use the **Archive** tier for storing rarely accessed data that requires long retention periods. Access to data in the **Archive** tier is not immediate. Archived data must be restored before the data is accessible.
   
   - **Object Events**: Select **Emit Object Events** if you want to enable the bucket to emit events for object state changes. For more information about events, see **Overview of Events** on page 1784.
   
   - **Encryption**: Buckets are encrypted with keys managed by Oracle by default, but you can optionally encrypt the data in this bucket using your own Vault encryption key. To use Vault for your encryption needs, select **Encrypt Using Customer-Managed Keys**. Then, select the **Vault Compartment** and **Vault** that contain the master encryption key you want to use. Also select the **Master Encryption Key Compartment** and **Master
Welcome to Oracle Cloud Infrastructure

Encryption Key. For more information about encryption, see Overview of Vault on page 3952. For details on how to create a vault, see Managing Vaults on page 3957.

- Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Create Bucket.

The bucket is created immediately and you can add objects to it. Objects added to archive buckets are immediately archived and must be restored before they are available for download.

Uploading Files to a Bucket

Object Storage supports uploading individual files up to 10 TiB. Because memory capacity and browser capability can impact uploading objects using the Console, use the CLI, SDK, or API for larger files. See "Developer Tools" in the Oracle Cloud Infrastructure User Guide.

To upload files to your bucket using the Console:

1. From the Object Storage Buckets screen, click the bucket name to view its details.
2. Click Upload.
3. In the Object Name Prefix field, optionally specify a file name prefix for the files that you plan to upload.
4. If the Storage Tier field displays Standard, you can optionally change the storage tier to upload objects to.
5. Select the object or objects to upload in one of two ways:
   - Drag files from your computer into the Drop files here ... section.
   - Click the select files link to display a file selection dialog box.

As you select files to upload, they are displayed in a scrolling list. If you decide that you do not want to upload a file that you have selected, click the X icon to the right of the file name.

If selected files to upload and files already stored in the bucket have the same name, messages warning you of an overwrite are displayed.

6. Click Upload.

The selected objects are uploaded. Click Close to return to the bucket.

What's Next

For information on managing and accessing your object files, see "Overview of Object Storage" in the Oracle Cloud Infrastructure User Guide.

Getting Started with the Command Line Interface

This topic provides a walk-through of the commands required to launch a Linux instance and a Windows instance. This tutorial includes working with a compartment, creating a virtual cloud network, and launching instances.

About the Command Line Interface (CLI)

The CLI is a tool that lets you work with most of the available services in Oracle Cloud Infrastructure. The CLI provides the same core functionality as the Console, plus additional commands. The CLI's functionality and command help are based on the service's API.
Getting Help with Commands
You can get inline help using the --help, -h, or -? keywords. For example:

oci --help
oci bv volume -h
oci os bucket create -?

You can also view all the CLI help in your browser.

About the CLI Examples
The examples in this document are grouped as a command and a response, where:
• You are told what the command does, and given the command to use
• The result of the command is returned in a drop-down text box

The next example shows a command and response group.

To get the namespace for your tenancy, run the following command.

oci os ns get

Response

Note:

Understanding Response Output
This response to the oci os ns get command shows the standard output, which is returned in JSON format. JSON objects are written as key/value pairs, with the key and value separated by a colon. For example:

```
{
  "data": "docs"
  "id":
  "ocid1.compartment.oc1..aaaaaaaal3gzijdhqol2pqglie6astxxeyqdqeyg35nz5zx1l2u63i35os1aal2j5j24",
  "is-stateless": null
}
```

A key like "id" isn't very informative. To understand the JSON object reference you have to read the key's value.

```
{
  "data": "docs"
}
```

Most of the command and response groups in this guide aren't as simple as the preceding example. However, as you work through the tasks, they are easier to read and work with.

Before You Begin
Before you start using the command line interface, verify that you meet all the requirements described in "Command Line Interface (CLI)" in the Oracle Cloud Infrastructure User Guide.

As a best practice, complete the tasks in this tutorial in a test environment. This approach ensures that your configurations do not affect other environments in the tenancy. At the end of the tutorial, you can safely delete the test resources.
Welcome to Oracle Cloud Infrastructure

Working in a Compartment

In this tutorial, you use one compartment for all your resources. When you are ready to create a production environment, you will most likely separate these resources in different compartments.

You can either use an existing compartment (recommended), or create a new compartment.

Choose a Compartment

Help: oci iam compartment list -h

To list the compartments in your tenancy, run the following command.

oci iam compartment list -c <tenancy_id>

Command Example and Response

```
oci iam compartment list -c
ocid1.tenancy.oc1..aaaaaaaal1fvgn0h9njji5u6ldrwb416aay2x87qatw2wte30f7141al9oom

{
  "data": [
    {
      "compartment-id": "ocid1.tenancy.oc1..aaaaaaaal1fvgn0h9njji5u6ldrwb416aay2x87qatw2wte30f7141al9oom",
      "description": "For testing CLI features",
      "id": "ocid1.tenancy.oc1..aaaaaaaal1fvgn0h9njji5u6ldrwb416aay2x87qatw2wte30f7141al9oom",
      "inactive-status": null,
      "lifecycle-state": "ACTIVE",
      "name": "CLIsandbox",
      "time-created": "2017-06-27T18:52:52.214000+00:00"
    },
    {
      "compartment-id": "ocid1.compartment.oc1..aaaaaaaasqn3hj6e6tq6s1j4rdqqja7qsyuqipmu4sv5ucmyp3rkmrhuv2q",
      "description": "for testing",
      "id": "ocid1.compartment.oc1..aaaaaaaasqn3hj6e6tq6s1j4rdqqja7qsyuqipmu4sv5ucmyp3rkmrhuv2q",
      "inactive-status": null,
      "lifecycle-state": "ACTIVE",
      "name": "CLISandbox",
      "time-created": "2017-05-12T21:31:27.709000+00:00"
    }
  ],
  "opc-next-page": "AAAAAAALGB28zJTjpUeNvgmLxg9QuJdAAAzr110FfKymIMh4y1XItQkO_Xk6RXbGxChkgkYm_pRpf1v6hVoXPTB53F2T231dRelsbxza31jbjwqGwzQsUPYROLXA4OEIjFdr2oYp67AozxSW8jt8MWFC8y19PsHEEEBH1jw8TT7VgP3ZFu6Y-Rab-gPnjs4plh91bkDkwzybHr0OmH4W1rhTJ5HFZ8YGpa0Ntm7_rOyNbd06qeBU496A9Hk24-U_19p4NvAvHuJ_fR-Z6ahgVWP1Qc1icCTR1j6elM7Ed3JnehIV0onOVQvGquJpF2WeEWFPCioQaqF4iScqHEchv--3Mn2klyP_-b4AsVtSPRFYGB8UiRACPzg6ENVFjyeGOk3rrHjLR3j7s61pdgqtMKZ1WtbOv8AcNON8ac1xJPN70Ymj03D0H4JjIt"
}
```

Create a Compartment

Help: oci iam compartment create -h

Before you create a compartment, review "Working with Compartments" in the Oracle Cloud Infrastructure User Guide to understand compartment design, resource management, and compartment constraints.
To create a compartment, run the following command.

```bash
oci iam compartment create --name <compartment_name> -c <root_compartment_id> --description "<friendly_description>"
```

**Command Example and Response**

```bash
oci iam compartment create --name CLIsandbox -c ocid1.tenancy.oc1..aaaaaaaal1fvgn0h9njjj5u61drwb416aay2x87qatw2wte30f7141a19oom --description "For testing CLI features"
```

```json
{
  "data": {
    "compartment-id": "ocid1.tenancy.oc1..aaaaaaaawuu4tdkysd2ups5fsc1gm5ksfjwmx6mwem5sbjyw5ob5ojq2vxxa",
    "description": "For testing CLI features",
    "id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfxyrc11",
    "inactive-status": null,
    "lifecycle-state": "ACTIVE",
    "name": "CLIsandbox",
    "time-created": "2017-06-27T18:52:52.214000+00:00"
  },
  "etag": "24a4737ede9d34eae934c93e9549ee684a15efc8"
}
```

**Tip:**
Keep track of the information that's returned when you run commands. In several cases, you need this information as you work through this document. For example, the preceding command returns the OCID for the tenancy, which is also the root compartment.

```
"compartment-id": "ocid1.tenancy.oc1..aaaaaaaawuu4tdkysd2ups5fsc1gm5ksfjwmx6mwem5sbjyw5ob5ojq2vxxa"
```

## Creating a Virtual Cloud Network

Before you can launch any instances, you have to create a virtual cloud network (VCN) and related resources. The following tasks are used to prepare the network environment:

1. **Create the Virtual Cloud Network**

   **Help:** `oci network vcn create -h`

   Create the VCN, specifying a DNS name and a CIDR block range.

   To create the VCN, run the following command.

   ```bash
   oci network vcn create --compartment-id <compartment_id> --display-name "<friendly_name>" --dns-label <dns_name> --cidr-block "<0.0.0.0/0>"
   ```

   **Command Example and Response**

   ```bash
   oci network vcn create --compartment-id ocid1.compartment.oc1..aaaaaaaal1kqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel6vfxyrc11 --display-name "cli_vcn" --dns-label sandboxvcn1 --cidr-block "10.0.0.0/16"
   ```

   ```json
   {
   }
   ```
Welcome to Oracle Cloud Infrastructure

You can get information about any of your configurations by sending queries to your tenancy.

For example, to get network information, run the following command.

```bash
oci network vcn list -c <compartment_id>
```

### Command Example and Response

```json
{
    "data": [
        {
            "cidr-block": "10.0.0.0/16",
            "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pf92rdrwo5fm6fcouf0ih1vd4ls4j9jjjopee16vfyxc11",
            "default-dhcp-options-id": "ocid1.dhcpoptions.oc1.phx.aaaaaaaaexnsdswjmxmmt4tpzkcyengrnfpgnznklkzz77f6faeqfbd",
            "default-route-table-id": "ocid1.routeable.oc1.phx.aaaaaaaaexnsdswjmxmmt4tpzkcyengrnfpgnznklkzz77f6faeqfbd",
            "default-security-list-id": "ocid1.securitylist.oc1.phx.aaaaaaaaexnsdswjmxmmt4tpzkcyengrnfpgnznklkzz77f6faeqfbd",
            "display-name": "cli_vcn",
            "dns-label": "sandboxvcn1",
            "id": "ocid1.vcn.oc1.phx.aaaaaaaaexnsdswjmxmmt4tpzkcyengrnfpgnznklkzz77f6faeqfbd",
            "lifecycle-state": "AVAILABLE",
            "time-created": "2017-06-27T22:14:15.683000+00:00",
            "vcn-domain-name": "sandboxvcn1.oraclevcn.com"
        }
    ]
}
```

2. Configure a Security List Ingress Rule

   Help: `oci network security-list create -h`

   When you create a VCN, a default security list is created for you. However, the Windows instance also requires inbound traffic enabled for port 3389. The preferred approach is creating a second list that addresses the Windows
Welcome to Oracle Cloud Infrastructure

port requirement. You use the `--security-list-ids` option to associate both security lists with the subnet when you create it.

**Note:**

**Passing JSON Strings in the CLI**

The next command passes complex input as a JSON text string. For help with formatting JSON input, especially when working in a Windows environment, see "Passing Complex Input" in the Oracle Cloud Infrastructure User Guide.

To create a new security list and configure the ingress rule for port 3389, run the following command.

```
oci network security-list create -c <compartment_id> --egress-security-rules 
"{"destination": "<0.0.0.0/0>" , "protocol": "<6>",
"isStateless": <true> , "tcpOptions": {"destinationPortRange": 
"<null>"}}"
--ingress-security-rules 
"{"source": 
"<0.0.0.0/0>" , "protocol": "<6>",
"isStateless": <false> ,
"tcpOptions": {"destinationPortRange": 
"<null>"}}"
--vcn-id <vcn_id> --display-name <rule_name>
```

**Command Example and Response**

```json
{
"data": {
"compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pf92rdrwo5f6mfcouf0ih1vd4ls4j9jjpge16vfylxc1",
"egress-security-rules": 
"{"destination": "<0.0.0.0/0>" , "protocol": 
"6" ,
"isStateless": true , "tcpOptions": {"destinationPortRange": 
null , "sourcePortRange": null}}",
"ingress-security-rules": 
"{"source": "<0.0.0.0/0>" , "protocol": "6" ,
"isStateless": false ,
"tcpOptions": {"destinationPortRange": 
{"max": 3389 , "min": 3389} ,
"sourcePortRange": null}}"
"vcn-id":
"ocid1.vcn.oc1.phx.aaaaaaaa6va8fkr1m4hvzj3k3nzo8x290qymdrwiblxw5qppz1m64rdd7vcr",
"display-name": "port3389rule"
}
```

Oracle Cloud Infrastructure User Guide 88
3. Create a Subnet

Help: oci iam availability-domain list -h, oci network subnet create -h

In this next step, you have to provide the OCIDs for the default security list and the new security list. If you didn't record these OCIDs, use the oci network security-list list command to get a list of the security lists in the virtual cloud network.

Before you create a subnet, you have to find out which availability domains are available to create the subnet in.

To get the availability domain list for your compartment, run the following command.

oci iam availability-domain list -c <compartment_id>

**Command Example and Response**

```bash
oci iam availability-domain list -c
oci iam compartment ocl..aaaaaaaalkqnr7pf92d9rwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l
```

```json
{
   "data": [
      {
         "compartment-id": "oci1.compartment.o1..aaaaaaaalkqnr7pf92d9rwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l",
         "name": "EMIR:PHX-AD-1"
      },
      {
         "compartment-id": "oci1.compartment.o1..aaaaaaaalkqnr7pf92d9rwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l",
         "name": "EMIR:PHX-AD-2"
      },
      {
         "compartment-id": "oci1.compartment.o1..aaaaaaaalkqnr7pf92d9rwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l",
         "name": "EMIR:PHX-AD-3"
      }
   ]
}
```
To create a subnet in AD-1, run the following command.

```bash
oci network subnet create --vcn-id <vcn_id> -c <compartment_id>
--availability-domain "<availability_domain_name>" --display-name "<display_name>" --dns-label "<dns_label>" --cidr-block "<10.0.0.0/16>" --security-list-ids ["<default_security_list_id>", "<new_security_list_id>"]
```

**Command Example and Response**

```bash
oci network subnet create --vcn-id ocid1.vcn.oc1.phx.aaaaaaaaah2ast7desae6ok3amu64wozj3kskox75awyr5j2nd7tkocplaajq -c ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jppge16vfyxrcll --availability-domain "EMIr:PHX-AD-1" --display-name CLISUB --dns-label "vminstances" --cidr-block "10.0.0.0/16" --security-list-ids ["ocid1.securitylist.oc1.phx.aaaaaaaaw7c62ybv4f5drwv2mup3f75aiquhbkbh4s676muq5t7j5t"]
```

```json
{
  "data": {
    "availability-domain": "EMIr:PHX-AD-1",
    "cidr-block": "10.0.0.0/16",
    "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jppge16vfyxrcll",
    "dhcp-options-id": "ocid1.dhcpoptions.oc1.phx.aaaaaaaaexnsdjmnnmnt4tpzkengrnfwspgnqz1drw7qfx6cbfaeqfbd",
    "display-name": "CLISUB",
    "dns-label": "vminstances",
    "id": "ocid1.subnet.oc1.phx.aaaaaaaaahvx05fhw7p320cxmdrwo5wlfl50e9i9cmdzs1plb1x16c5wvb5s2",
    "lifecycle-state": "PROVISIONING",
    "prohibit-public-ip-on-vnic": false,
    "route-table-id": "ocid1.routetable.oc1.phx.aaaaaaaagdjqga3i6grxvf23stedpre4rmkdrw6qeqkftjtzyn7vctmujo",
    "security-list-ids": [
      "ocid1.securitylist.oc1.phx.aaaaaaaaw7c62ybv4f5drwv2mup3f75aiquhbkbh4s676muq5t7j5t",
      "ocid1.securitylist.oc1.phx.aaaaaaaaw7c62ybv4f5drwv2mup3f75aiquhbkbh4s676muq5t7j5t",
      "ocid1.securitylist.oc1.phx.aaaaaaaaw7c62ybv4f5drwv2mup3f75aiquhbkbh4s676muq5t7j5t",
      "ocid1.securitylist.oc1.phx.aaaaaaa7snx4jffons602h33drwdh5hev6elir55hnrhi2yqwfnd5rc",
      "subnet-domain-name": "vminstances.sandboxvcn1.oraclevcn.com",
      "time-created": "2017-08-24T00:51:30.462000+00:00",
      "vcn-id": "ocid1.vcn.oc1.phx.aaaaaaaa6va8fkr1m4hvzjk3nzo8x290qymdrwiblxw5qpz1m64rdd74vchr",
      "virtual-router-ip": "10.0.0.1",
      "virtual-router-mac": "00:00:17:7F:8A:D7"
    ],
    "etag": "92d20c35"
  }
}
```
4. Create an Internet Gateway

Help: `oci network internet-gateway create -h`

To create an Internet Gateway, run the following command.

```
oci network internet-gateway create -c <compartment_id> --is-enabled <true> --vcn-id <vcn_id> --display-name <gateway_display_name>
```

**Command Example and Response**

```
oci network internet-gateway create -c ocid1.compartment.oc1..aaaaaaaalkqnr7pfdrwo5f6m6fcooufoih1vd4ls49jgjgei6vfxycFormsModule --is-enabled true --vcn-id ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvjzjk3nzo8x290qymdrwbilw5qplm64rdd74vchr --display-name sbgateway
```

```
{
    "data": {
        "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfdrwo5f6m6fcooufoih1vd4ls49jgjgei6vfxycFormsModule",
        "display-name": "sbgateway",
        "id": "ocid1.internetgateway.oc1.phx.aaaaaaa3vcd7gmgqah4p06wsmjhc4dxdldfieqnmhbanzz2wsh5gdr",
        "is-enabled": true,
        "lifecycle-state": "AVAILABLE",
        "time-created": "2017-08-25T20:03:48.482000+00:00",
        "vcn-id": "ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvjzjk3nzo8x290qymdrwbilw5qplm64rdd74vchr"
    },
    "etag": "d13fb7e3"
}
```

5. Add a Rule to the Route Table

Help: `oci network route-table list -h, oci network route-table update -h`

When you create a VCN, a route table is created automatically. Before you add a rule to the route table, you need the OCID for the table.

To get the route table OCID, run the following command.

```
oci network route-table list -c <compartment_id> --vcn-id <vcn_id>
```

**Command Example and Response**

```
oci network route-table list -c ocid1.compartment.oc1..aaaaaaaalkqnr7pfdrwo5f6m6fcooufoih1vd4ls49jgjgei6vfxycFormsModule --vcn-id ocid1.vcn.oc1.phx.aaaaaaa6va8fxr1m4hvjzjk3nzo8x290qymdrwbilw5qplm64rdd74vchr
```

```
{
    "data": [
        {
            "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfdrwo5f6m6fcooufoih1vd4ls49jgjgei6vfxycFormsModule",
            "display-name": "Default Route Table for cli_vcn",
            "id": "ocid1.routetable.oc1.phx.aaaaaaaagdjqga3i6qrxvf3stedpre4rmkdrw6qeqkftjtzyn7vctmujo",
            "lifecycle-state": "AVAILABLE",
            "route-rules": [],
            "time-created": "2017-08-25T21:46:04.324000+00:00",
        }
    ],
    "etag": "d13fb7e3"
}
```
Welcome to Oracle Cloud Infrastructure

The information in the previous response shows that there is a route table without any rules: "route rules": 
[]. Because the table exists, you create a rule by updating the table. When you run the next command, you get a warning about updates to route rules. Any update to the route rules replaces all the existing rules. If you want to continue and process the update, Enter "y".

To update the route rules, run the following command.

```bash
oci network route-table update --rt-id <route_table_id> --route-rules 
"[{"cidrBlock":"<0.0.0.0/0","networkEntityId":"<internet_gateway_id>"}]
```

WARNING: Updates to route-rules will replace any existing values. Are you sure you want to continue? [y/N]: y

Command Example and Response

```bash
oci network route-table update --rt-id ocid1.routetable.oc1.phx.aaaaaaaagdjqga3i6qrxvf23stedpre4rmkdwr6geqkftjtzy7vctmujo2 --route-rules "[{"cidrBlock":"0.0.0.0/0","networkEntityId":"ocid1.internetgateway.oc1.phx.aaaaaaaa3vcd7gmqqh4po6wnsjhcdxddeqinmnbanzz2wsh5gdr"}]
```

WARNING: Updates to route-rules will replace any existing values. Are you sure you want to continue? [y/N]: y

```json
{
"data": {
"compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jppge16vfyxrc1ll",
"display-name": "Default Route Table for cli_vcn",
"id": "ocid1.routetable.oc1.phx.aaaaaaaa4kujevzdsnd7bh6aetvrhwzdrwcxmblspmyj3pqwckchajvz6",
"lifecycle-state": "AVAILABLE",
"route-rules": [
{"cidr-block": "0.0.0.0/0",
 "network-entity-id": "ocid1.internetgateway.oc1.phx.aaaaaaaa3vcd7gmqqh4po6wnsjhcdxddeqinmnbanzz2wsh5gdr"},
],
"time-created": "2017-08-25T23:46:04.324000+00:00","vcn-id": "ocid1.vcn.oc1.phx.aaaaaaaa6va8fzr1m4hvzjk3nzo8x290qymdrwiblxw5qpzl64rdd74vchr" },
"etag": "3fc998d8"
}
```

Preparing to Launch an Instance

When you launch an instance you have to provide the following information, some of which you've already obtained:

- compartment-id
- availability-domain
- subnet-id
- image-id
- shape
1. Get Information About the Available Images

   Help: oci compute image list -h

   The image-id identifies the operating system that you want to install. For more information, see "Oracle-
   Provided Images" in the Oracle Cloud Infrastructure User Guide.

   To get a list of images, run the following command.

   ```
   oci compute image list -c <compartment_id>
   ```

   **Command Example and Response**

   Images are available for: Oracle Linux, CentOS, Ubuntu, and Windows Server. This response example only
   shows the information for Oracle Linux 7.3.

   ```
   oci compute image list -c
   ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11
   ```

   ```
   {"base-image-id": null,
    "compartment-id": null,
    "create-image-allowed": true,
    "display-name": "Oracle-Linux-7.3-2017.03.03-0",
    "id": "ocid1.image.oc1.phx.aaaaaaaaevkccomzepja4yahz6rguhbuomuto7gdrw5hjimqsig6syeqda",
    "lifecycle-state": "AVAILABLE",
    "operating-system": "Oracle Linux",
    "operating-system-version": "7.3",
    "time-created": "2017-03-03T19:04:30.824000+00:00"
   }
   ```

2. Get Information About the Available Shapes

   Help: oci compute shape list -h

   The shape identifies the configuration of the virtual machine or bare metal host that you want to use. "Overview of
   the Compute Service" in the Oracle Cloud Infrastructure User Guide contains up-to-date information about the
   available shapes.

   For the purposes of this walk-through, use this virtual machine shape for testing: --shape
   "VM.Standard1.1". This shape is configured with 1 CPU and 7 GB of memory.

   **Note:**

   Shape and Block Volume Sizing
   Sizing for compute instance shapes and block volumes are not part of this
   walk-through. The examples use the minimum sizes that are available.

   To get a list of all the available bare metal and virtual machine shapes, run the following command.

   ```
   oci compute shape list -c <compartment_id> --availability-domain
   "<availability_domain_name>"
   ```

   **Command Example and Response**

   ```
   oci compute shape list -c
   ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc11
   --availability-domain "EMIr:PHX-AD-1"
   ```

   ```
   { "data": [ ...
   ```
Welcome to Oracle Cloud Infrastructure

Launching a Linux Instance

Now you're ready to launch a Linux instance based on the configurations you prepared.

1. Use a Public/Private Key Pair to Connect to the Instance
   When you launch an instance using the CLI, you need an existing key pair to access the instance. (This key pair is not the same as an API signing key.)

2. Launch the Instance
   Help: oci compute instance launch -h

   **Caution:**
   In this example, the --ssh-authorized-keys-file parameter references a file that contains the public key required to access the compute instance. If you don't provide this key when you launch the instance you can't connect to the instance after it's launched.

To launch the Linux instance, run the following command.

```
oci compute instance launch --availability-domain "<availability_domain_name>" -c <compartment_id> --shape "<shape_name>"
--display-name "<instance_display_name>" --image-id <image_id> --ssh-authorized-keys-file "<path_toAuthorized_keys_file>" --subnet-id <subnet_id>
```

**Command Example and Response**

```
oci compute instance launch --availability-domain "EMIr:PHX-AD-1" -c ocid1.compartment.oc1..aaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l --shape "VM.Standard1.1" --display-name "Linux Instance" --image-id ocid1.image.oc1.phx.aaaaaaaa5yu6pw3riqtuhxzov7fndqi4tsteganmao54nq3pyxu3hxcuzmoa --ssh-authorized-keys-file "C:\Users\testuser\.oci\linux_key.pem" --subnet-id ocid1.subnet.oc1.phx.aaaaaaaaahvx05fhw7p320cxdwro5wlf50egig9cmdzs1plb1xl6c5wvb5s2
```

{
3. Get VNIC Information for the Instance

Help: oci compute instance list-vnics -h

You need the public IP address of the instance in order to connect to the instance. The VNIC for the instance has this information.

To get a list of VNICs for the instance, run the following command.

```
oci compute instance list-vnics --instance-id <instance_id>
```

**Command Example and Response**

```
oci compute instance list-vnics --instance-id ocid1.instance.oc1.phx.abcdefgh6kykdowc8ozzvr4421kwp7apdrwk6wrj17su82d60c6sp4nap88d
```
4. Create a Block Volume for the Instance

Help: `oci bv volume create -h`

Create a block volume, using the minimum available size.

**Caution:**

Block volume sizes are expressed as increments of 1024 MB. The next command example uses the minimum size, `--size-in-mbs 51200`, or 50 GB.

To create a block volume, run the following command.

```
oci bv volume create --availability-domain "<availability_domain_name>"
-c <compartment_id> --size-in-mbs <51200> --display-name <volume_display_name>
```

**Command Example and Response**

```
oci bv volume create --availability-domain "EMIr:PHX-AD-1" -c
ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel16vfyrcl
--size-in-mbs 51200 --display-name LinuxVol
```

```
{
  "data": {
    "availability-domain": "EMIr:PHX-AD-1",
    "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpgel16vfyrcl",
    "display-name": "LinuxVol",
    "id": "ocid1.volume.oc1.phx.abyhqlsktp2ec7pdazl1y324drw51xruh5nxjrgbgqq7zn5s5004t25nvcta",
    "lifecycle-state": "PROVISIONING",
    "size-in-mbs": 51200,
    "time-created": "2017-08-26T00:51:30.462000+00:00"
  },
  "etag": "720652578"
}
```

After the lifecycle state changes from "PROVISIONING" to "AVAILABLE" you can attach the volume to the Linux instance.

**Tip:**

Finding out the Lifecycle State

You can find out the lifecycle state for the block volume using the `oci bv volume get` command for the volume you created. You can also query other resources such as compute instances and VNICs, to find out their lifecycle state.

5. Attach the Block Volume to the Instance

Help: `oci compute volume-attachment attach -h`

To attach the block volume to the Linux instance, run the following command.

```
oci compute volume-attachment attach --instance-id <instance_id> --type <iscsi> --volume-id <volume_id>
```

**Command Example and Response**

```
oci compute volume-attachment attach --instance-id
ocid1.instance.oc1.phx.abcdefgh6kykdcw58ozzvr4421kwp7apdrkw6wrj17su82d60c6sp4nap88d
```
Launching a Windows Instance

Launching a Windows instance follows the same pattern and requires the same information as launching a Linux instance. The only significant differences are the operating system and shape, as shown in the following commands.

1. Launch the Instance

   Help: oci compute instance launch -h

   To launch the Windows instance, run the following command.

   ```bash
   oci compute instance launch --availability-domain "EMIr:PHX-AD-1" -c ocid1.compartment.oc1..aaaaaaaalkqnr7pfdf92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc1ll
   --shape "VM.Standard1.2" --display-name "Windows Instance" --image-id ocid1.image.oc1.phx.aaaaaaaa53cliasgvmueus5byytfdwafbro2y4ywjebc15szc42e2b7ua
   --subnet-id ocid1.subnet.oc1.phx.aaaaaaaaypsr25bzjmx3drwiha61odzus3yn6xwgcrgxgafscirb5hj0bpa
   ```

   ```json
   {   "data": {   "availability-domain": "EMIr:PHX-AD-1",   "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfdf92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vfyxrc1ll",   "display-name": "Windows Instance",   "extended-metadata": {},   "id": "ocid1.instance.oc1.phx.zsutzirph7cbrbx6ruz91stavdrw58puq3iskn1r07zfc6dq6p9",  }
   }
   ```
2. Get VNIC Information for the Instance
   To get the VNIC information, run the following command.
   
   ```bash
   oci compute instance list-vnics --instance-id <instance_id>
   ```

3. Create a Block Volume for the Instance
   To create a block volume, run the following command.
   
   ```bash
   oci bv volume create --availability-domain "<availability_domain_name>" -c <compartment_id> --size-in-mbs <51200> --display-name <display_name>
   ```

4. Attach the Block Volume to the Instance
   To attach the Block Volume to the Windows instance, run the following command.
   
   ```bash
   oci compute volume-attachment attach --instance-id <instance_id> --type <iscsi> --volume-id <volume_id>
   ```

### Connecting to Your Instances

Although the Public IP address is required for connecting to Linux and Windows instances, that is the only thing 
the two have in common. Some of these differences include: authentication, port configuration, and desktop client 
programs.

1. Connect to Your Linux Instance
   
   **Connecting to Your Instance** describes how to connect to a Linux instance from a Unix-style or Windows-style 
system.

2. Connect to Your Windows Instance
   
   **Help:** `oci compute instance list-vnics -h` and `oci compute instance get-windows-initial-creds -h`
   
   To connect to the instance using Remote Desktop Client (RDC), you need:
   
   - The public IP address for the instance
   - The initial Windows credentials
   
   To get the public IP address of the Windows instance, run the following command.
   
   ```bash
   oci compute instance list-vnics --instance-id <instance_id>
   ```

### Command Example and Response

```bash
oci compute instance list-vnics --instance-id
ocid1.instance.oc1.phx.zsutzirph7cbrbx6ruz91stavdrw58puq3iskn1r07zfd6rq6p9

{
```
To get the initial Windows credentials, run the following command.

```
oci compute instance get-windows-initial-creds --instance-id <instance_id>
```

### Command Example and Response

```
oci compute instance get-windows-initial-creds --instance-id ocid1.instance.oc1.phx.zsutzirph7cbrbx6ru91stavdrw58puq3iskn1r07zfcx6rq6p9
```

```json
{
   "data": {
      "password": "Cz{73~~vf@dnK7A",
      "username": "opc"
   }
}
```

Connecting to Your Windows Instance describes how to connect to your instance using RDC.

### Cleaning Up the Test Environment

When you've finished setting up the test environments described in this tutorial, clean up the test environment by removing resources you aren't using.

#### Detach and Delete the Block Volumes

Help: `oci compute volume-attachment list -h`, `oci compute volume-attachment detach -h` and `oci bv volume delete -h`

Removing a block volume from an instance is a 3-step process. Use the following steps to detach and delete the block volume for the Linux instance.
1. Get the volume-attachment-id

   The volume attachment ID is created when you create a block volume.

   To get the volume attachment ID, run the following command.

   `oci compute volume-attachment list -c <compartment_id>`

   **Command Example and Response**

   ```
   oci compute volume-attachment list -c
   ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l
   {
     "data": [
     {
       "attachment-type": "iscsi",
       "availability-domain": "EMIr:PHX-AD-1",
       "chap-secret": null,
       "chap-username": null,
       "compartment-id": "ocid1.compartment.oc1..aaaaaaaalkqnr7pfd92rdrwo5fm6fcoufoih1vd4ls4j9jjpge16vyxrc1l",
       "display-name": null,
       "id": "ocid1.volumeattachment.oc1.phx.abyhqlyto1vg6eaybdwb7mqqms6utjrefofrplyip7f1lf3vtpk",
       "instance-id": "ocid1.instance.oc1.phx.abcdefgh6kykdowc8ozzvr4421kwp7apdrwk6wrjl7su82d60c6sp4nap88d",
       "ipv4": "169.254.2.2",
       "iqn": "iqn.2015-12.com.oracleiaas:e3fd73db-b164-4d76-bc3f-f58b093989d0",
       "lifecycle-state": "ATTACHED",
       "port": 3260,
       "time-created": "2017-08-26T00:51:30.462000+00:00",
       "volume-id": "ocid1.volume.oc1.phx.abyhqpa3ati7ggfjvba7y6dcg7imdrwskgq4bd1jroo2cbwchrebuprxddvca"
     }
     ]
   }
   ```

2. Detach the volume-attachment-id

   To detach the volume attachment-id, run the following command.

   `oci compute volume-attachment detach --volume-attachment-id <volume_attachment_id>`

   **Command Example and Response**

   ```
   oci compute volume-attachment detach --volume-attachment-id
   ocid1.volumeattachment.oc1.phx.abyhqlyto1vg6eaybdwb7mqqms6utjrefofrplyip7f1lf3vtpk5
   Are you sure you want to delete this resource? [y/N]:
   ```

   All destructive actions, such as detaching and deleting resources allow you to use the `--force` parameter, and the resource is removed without requiring confirmation. As a best practice, use the y/N option instead of --force.

   Confirm the deletion. No response is returned after the resource is deleted.
3. **Delete the Block Volume**

To delete the block volume, run the following command.

```bash
oci bv volume delete --volume-id <volume_id> --force
```

**Command Example and Response**

```bash
oci bv volume delete --volume-id
ocid1.volume.oc1.phx.abyhqljroo2cbwchrpa3ati7ggfjvba7y6dcg7imnleskq4bdebuprxddvca
--force
```

There is no response to this action. To verify that the block volume was deleted, run the following command.

```bash
oci bv volume list -c <compartment_id>
```

The response to this query returns "lifecycle-state": "TERMINATED", showing that the volume doesn't exist.

To delete the block volume attached to the Windows instance, use the preceding steps (1-3) as a guide.

**Terminate the Instances**

**Help:** `oci compute instance terminate -h`

To delete the Linux instance, run the following command.

```bash
oci compute instance terminate --instance-id <instance_id>
```

**Command Example and Response**

```bash
oci compute instance terminate --instance-id
ocid1.instance.oc1.phx.abcdefgh6kykdowc8ozzvr4421kwp7apdrwk6wrj17su82d60c6sp4nap88d
```

Are you sure you want to delete this resource? [y/N]:

Confirm the deletion. No response is returned after the instance is deleted.

To delete the Windows instance, run the following command.

```bash
oci compute instance terminate --instance-id <instance_id>
```

**Command Example and Response**

```bash
oci compute instance terminate --instance-id
ocid1.instance.oc1.phx.zsutzirph7cbrbx6ru91stavdrw58puq3iskn1r07zfcd6rg6p9
```

Are you sure you want to delete this resource? [y/N]:

Confirm the deletion. No response is returned after the instance is deleted.

**Delete the Virtual Cloud Network**

**Help:** `oci network subnet delete -h, oci network vcn delete -h`

It takes the following 2 steps to delete the VCN.
1. Delete the subnet

To delete the subnet, run the following command.

```
oci network subnet delete --subnet-id <subnet_id> --force
```

**Command Example and Response**

```
oci network subnet delete --subnet-id
ocid1.subnet.oc1.phx.aaaaaaaaahvx05fhw7p320cxmdrwo5wlf50egig9cmdzs1plblx16c5wvb5s2
--force
```

None

2. Delete the virtual cloud network

To delete the VCN, run the following command.

```
oci network vcn delete --vcn-id <vcn_id> --force
```

**Command Example and Response**

```
oci network vcn delete --vcn-id
ocid1.vcn.oc1.phx.aaaaaaaa6va8fxr1m4hvzjk3nzo8x290qymdrwiblxw5qz1m64rdd74vchr
--force
```

None

**Getting Started**

Terraform is "infrastructure-as-code" software that allows you to define your Oracle Cloud Infrastructure (OCI) resources in files that you can persist, version, and share. These files describe the steps required to provision your infrastructure and maintain its desired state:

*Resources* can create OCI infrastructure objects such as virtual cloud networks or compute instances. Your first application of the configuration creates the objects, and subsequent applications can update or delete them.

*Data sources* represent read-only views of your existing OCI infrastructure.

*Variables* represent parameters for Terraform.

Terraform then executes these steps and builds out the described infrastructure. Using the OCI Terraform provider requires you to:

- Install or access a distribution of Terraform.
- Download and install the OCI Terraform provider.
- Configure the OCI Terraform provider.
- Describe your infrastructure as code.

**Installing the Provider**

To use the Oracle Cloud Infrastructure (OCI) Terraform provider, you must install both Terraform and the OCI Terraform provider. You can install both Terraform and the OCI Terraform provider with *yum*, or directly download them from HashiCorp.

Government Cloud customers should follow the installation and configuration steps in Enabling FIPS Compatibility on page 4284.

**Tip:**

You can use Resource Manager to reinstall the Oracle Cloud Development Kit on a Compute instance in your compartment. The Oracle Cloud
After downloading and installing, you must configure the Terraform provider so that Terraform can interact with OCI resources.

**Prerequisites for Installing and Using the Provider**

- An Oracle Cloud Infrastructure (OCI) account that has user credentials sufficient to execute a Terraform plan.
- A user in that account.
- Required keys and OCI IDs (OCIDs). For guidance, see "Required Keys and OCIDs" in the Oracle Cloud Infrastructure User Guide.
- The correct Terraform binary file for your operating system. We recommend using Terraform version 0.12.20 or greater.

**Installing with Yum**

If you're running Oracle Linux 7, you can use yum to install Terraform and the OCI Terraform provider.

To use yum to install Terraform:

```bash
sudo yum install terraform
```

To use yum to install the Terraform provider:

```bash
sudo yum install terraform-provider-oci
```

**Download and Install Terraform**

Terraform is available for direct download from the HashiCorp download page. Ensure that you download the correct binary file for your system.

**Download and Install the Provider**

To use the latest version of the OCI Terraform provider, run `terraform init` from the directory that contains a configuration file with the provider `"oci" { ... configuration block. The provider is automatically downloaded. Terraform configurations also allow you to specify a particular version of the OCI Terraform provider.

You can also download the Terraform provider directly to a location of your choice.

**Test the Terraform Installation**

Open a terminal window and run the following command to test your installation:

```bash
terraform -v
```

**Getting Started with Load Balancing**

This chapter provides a hands-on tutorial to introduce you to the components of Load Balancing.

The Load Balancing service allows you to create highly available load balancers within your VCN. All load balancers come with provisioned bandwidth. You can choose to create a load balancer with either a public or a private IP address. Load balancers support SSL handling for both incoming traffic and traffic with your application servers.

When you create a load balancer with a public IP address you specify two subnets, each in a different availability domain, on which the load balancer can run. The two subnets ensure the high availability of the load balancer. A private load balancer requires only one subnet.
Welcome to Oracle Cloud Infrastructure

This tutorial is an introduction to Load Balancing. You can follow the steps here to create a public load balancer and verify it with a basic web server application. For complete details about the service and its components, see Overview of Load Balancing in the Oracle Cloud Infrastructure User Guide.

Before You Begin

To try out the Load Balancing service for this tutorial, you must have these things set up first:

- A virtual cloud network (VCN) with two subnets (each in a different availability domain) and an internet gateway
- Two instances running (in different subnets)
- A web application (such as Apache HTTP Server) running on each instance

If you don't have these items set up yet, you can follow the steps shown here.

Tip:

If you need an introduction to VCNs and instances, try the Tutorial - Launching Your First Linux Instance on page 61 first.

VCN and Instance Setup

The following diagram shows the prerequisite VCN and instances:
Create a VCN

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks. Ensure that the Sandbox compartment (or the compartment designated for you) is selected in the Compartment list on the left.

2. Click Networking Quickstart.

3. Select VCN with Internet Connectivity, and then click Start Workflow.

4. Enter the following:
   - VCN Name: Enter a name for your cloud network. The name is incorporated into the names of all the related resources that are automatically created. Avoid entering confidential information.
   - Compartment: This field defaults to your current compartment. Select the compartment you want to create the VCN and related resources in, if not already selected.
   - VCN CIDR Block: Enter a valid CIDR block for the VCN. For example 10.0.0.0/16.
   - Public Subnet CIDR Block: Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block. For example: 10.0.0.0/24.
   - Private Subnet CIDR Block: Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block and not overlap with the public subnet's CIDR block. For example: 10.0.1.0/24.
   - Accept the defaults for any other fields.

5. Click Next.

6. Review the list of resources that the workflow will create for you. Notice that the workflow will set up security list rules and route table rules to enable basic access for the VCN.

7. Click Create to start the short workflow.

8. After the workflow completes, click View Virtual Cloud Network.

The cloud network has the following resources and characteristics:
- Internet gateway.
- NAT gateway.
- Service gateway with access to the Oracle Services Network.
- A regional public subnet with access to the internet gateway. This subnet uses the VCN's default security list and default route table. Instances in this subnet may optionally have public IP addresses.
- A regional private subnet with access to the NAT gateway and service gateway. This subnet uses a custom security list and custom route table that the workflow created. Instances in this subnet cannot have public IP addresses.
- Use of the Internet and VCN Resolver for DNS.

Launch two instances

This example uses the VM.Standard2.1 shape. If you prefer, you can choose a larger shape.

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.

2. Click Create Instance.

3. On the Create Compute Instance page, for Name, enter a name, for example: Webserver1. Avoid entering confidential information.

4. In the Placement and hardware section, enter the following:
   - Availability domain: Select the first availability domain in the list (AD-1).
   - Image: Select the Oracle Linux 7.x image.
   - Shape: Click Change Shape, and then make the following selections:
     1. For Instance type, select Virtual Machine.
     2. For Shape series, select Intel Skylake, and then select the VM Standard2.1 shape (1 OCPU, 15 GB RAM).
     3. Click Select Shape.
5. In the **Configure networking** section, configure the network details for the instance. Do not accept the defaults.
   
   a. For **Network**, leave **Select existing virtual cloud network** selected.
   
   b. **Virtual cloud network in `<compartment_name>`**: Select the cloud network that you created. If necessary, click **Change compartment** to switch to the compartment containing the cloud network that you created.
   
   c. For **Subnet**, leave **Select existing subnet** selected.
   
   d. **Subnet in `<compartment_name>`**: Select the public subnet in availability domain 1. If necessary, click **Change compartment** to switch to the compartment that contains the correct subnet.
   
   e. Leave the **Use network security groups to control traffic** check box cleared.
   
   f. Select the **Assign a public IPv4 address** option. This creates a public IP address for the instance, which you need to access the instance. If you have trouble selecting this option, confirm that you selected the public subnet that was created with your VCN, not a private subnet.

6. In the **Add SSH keys** section, upload the public key portion of the key pair that you want to use for SSH access to the instance. Browse to the key file that you want to upload, or drag and drop the file into the box.

   If you do not have an SSH key pair, see Creating a Key Pair on page 63.

7. In the **Boot volume** section, leave all the options cleared.

8. Click **Show Advanced Options**. On the **Networking** tab, ensure that the **Hostname** field is blank.

9. Click **Create**.

10. Repeat the previous steps. This time, enter the name **Webserver2** and select the subnet in availability domain 2.

**Start a web application on each instance**

This example uses Apache HTTP Server.

1. Connect to your instance. If you need help, see Connecting to Your Instance on page 68.

2. Run yum update:

   ```bash
   sudo yum -y update
   ```

3. Install the Apache HTTP Server:

   ```bash
   sudo yum -y install httpd
   ```

4. Allow Apache (HTTP and HTTPS) through the firewall:

   ```bash
   sudo firewall-cmd --permanent --add-port=80/tcp
   
sudo firewall-cmd --permanent --add-port=443/tcp
   ```

   **Note:**

   Open the Firewall

   If you choose to run a different application than Apache, ensure that you run the preceding command to open the firewall for your application's port.

5. Reload the firewall:

   ```bash
   sudo firewall-cmd --reload
   ```

6. Start the web server:

   ```bash
   sudo systemctl start httpd
   ```
7. Add an index.htm file on each server that indicates which server it is, for example:
   a. On Webserver 1:
      ```
sudo su

    echo 'WebServer1' >/var/www/html/index.html
      ```
   b. On Webserver 2:
      ```
sudo su

    echo 'WebServer2' >/var/www/html/index.html
      ```

**Tutorial Overview**

In this tutorial, you create a public load balancer and verify it. A load balancer requires configuration of several components to be functional, and this tutorial walks you through each step to help you understand these components.

To create and test the load balancer, complete the following steps:

1. Add two subnets to your VCN to host your load balancer.
2. Create a load balancer.
3. Create a backend set with health check.
4. Add backend servers to your backend set.
5. Create a listener.
6. Update the load balancer subnet security list and allow internet traffic to the listener.
7. Verify your load balancer.
8. Update rules to protect your backend servers.
9. Delete your load balancer.

**Add Two Subnets to Your VCN to Host Your Load Balancer**

Your load balancer must reside in different subnets from your application instances. This configuration allows you to keep your application instances secured in subnets with stricter access rules, while allowing public internet traffic to the load balancer in the public subnets.

To add the public subnets to your VCN:

**Add a Security List**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.

    The list of VCNs in the current compartment is displayed.

2. Click the name of the VCN that includes your application instances.


4. Click Create Security List.

   a. **Create in Compartment**: This field defaults to your current compartment. Select the compartment you want to create the security list in, if not already selected.
   b. Enter a **Name**, for example, "LB Security List". Avoid entering confidential information.
   c. Delete the entry for the ingress rule and the entry for the egress rule. The security list must have no rules. The correct rules are added automatically during the load balancer workflow.
   d. **Tags**: Leave as is (you can add tags later if you like).
   e. Click **Create Security List**.
   f. Return to your Virtual Cloud Network Details page.
Add a Route Table

1. Under Resources, click Route Tables.
2. Click Create Route Table. Enter the following:
   a. Create in Compartment: This field defaults to your current compartment. Select the compartment you want to create the route table in, if not already selected.
   b. Name: Enter a name, for example, "LB Route Table". Avoid entering confidential information.
   c. Target Type: Select Internet Gateway.
   d. Destination CIDR Block: Enter 0.0.0.0/0.
   e. Compartment: Select the compartment that contains your VCN's internet gateway.
   f. Target: Select your VCN's internet gateway.
   g. Tags: Leave as is (you can add tags later if you like).
   h. Click Create Route Table.

Create the first subnet

1. Under Resources, click Subnets.
2. Click Create Subnet.
3. Enter or select the following:
   a. Name: Enter a name, for example, "LB Subnet 1". Avoid entering confidential information.
   b. availability domain: Choose the first availability domain (AD-1).
   c. CIDR Block: Enter 10.0.4.0/24.
   d. Route Table: Select the LB Route Table you created.
   e. Subnet Access: Select Public Subnet.
   f. DNS Resolution: Select Use DNS Hostnames in this Subnet.
   g. DHCP Options: Select Default DHCP Options for LB_Network.
   h. Security Lists: Select the LB Security List you created.
   i. Tags: Leave as is (you can add tags later if you like).
4. Click Create.

Create the second subnet

Create a second load balancer subnet in a different availability domain.

1. In the details page of your VCN, click Create Subnet.
2. Enter the following:
   a. Name: Enter a name, for example, "LB Subnet 2". Avoid entering confidential information.
   b. availability domain: Choose the second availability domain (AD-2).
   c. CIDR Block: Enter 10.0.5.0/24.
   d. Route Table: Select the LB Route Table you created.
   e. Subnet Access: Select Public Subnet.
   f. DNS Resolution: Select Use DNS Hostnames in this Subnet.
   g. DHCP Options: Select Default DHCP Options for LB_Network.
   h. Security Lists: Select the LB Security List you created.
   i. Tags: Leave as is (you can add tags later if you like).
3. Click Create.

The following figure shows the new components added to the VCN:
Create the Load Balancer

When you create a public load balancer, you choose its shape (size) and you select two subnets, each in a different availability domain. This configuration ensures that the load balancer is highly available. It is active in only one subnet at a time. This load balancer comes with a public IP address and provisioned bandwidth corresponding to the shape you chose.

**Tip:**

Although the load balancer resides in a subnet, it can direct traffic to backend sets that reside in any of the subnets within the VCN.

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.

   Ensure that the Sandbox compartment (or the compartment designated for you) is selected on the left.

2. Click **Create Load Balancer**.

3. Enter the following:

   - **Name**: Enter a name for your load balancer. Avoid entering confidential information.
   - **Shape**: Select 100 Mbps. The shape specifies the bandwidth of the load balancer. For the tutorial, use the smallest shape. The shape cannot be changed later.
   - **Virtual Cloud Network**: Select the virtual cloud network for your load balancer.
   - **Visibility**: Choose **Create Public Load Balancer**.
   - **Subnet (1 of 2)**: Select LB Subnet 1.
   - **Subnet (2 of 2)**: Select LB Subnet 2. The second subnet must be in a different availability domain than the first subnet you chose.

4. Click **Create**.
Welcome to Oracle Cloud Infrastructure

When the load balancer is created, you get a public IP address. You route all your incoming traffic to this IP address. The IP address is available from both subnets that you specified, but it is active in only one subnet at a time.

Create a Backend Set

A backend set is a collection of backend servers to which your load balancer directs traffic. A list of backend servers, a load balancing policy, and a health check script define each backend set. A load balancer can have multiple backend sets, but for this tutorial, you create only one backend set that includes both of your web servers.

In this step, you define the backend set policy and health check. You add your servers in a separate step.

To create the backend set:

1. Click the name of your load balancer and view its details.
2. Click Create Backend Set.
3. In the dialog box, enter:
   a. Name: Give your load balancer backend set a name. The name cannot contain spaces. Avoid entering confidential information.
   b. Policy: Choose Weighted Round Robin.
4. Enter the Health Check details.

   Load Balancing automatically checks the health of the instances for your load balancer. If it detects an unhealthy instance, it stops sending traffic to the instance and reroutes traffic to healthy instances. In this step, you provide the information required to check the health of servers in the backend set and ensure that they can receive data traffic.

   • Protocol: Select HTTP.
   • Port: Enter 80
   • URL Path (URI): Enter /

   The rest of the fields are optional and can be left blank for this tutorial.
5. Click Create.

When the Backend Set is created, the Work Request shows a status of Succeeded. Close the Work Request dialog box.

What is a policy?
The policy determines how traffic is distributed to your backend servers.

- Round Robin - This policy distributes incoming traffic sequentially to each server in a backend set list. When each server has received a connection, the load balancer repeats the list in the same order.
- IP Hash - This policy uses an incoming request's source IP address as a hashing key to route non-sticky traffic to the same backend server. The load balancer routes requests from the same client to the same backend server as long as that server is available.
- Least Connections - This policy routes incoming non-sticky request traffic to the backend server with the fewest active connections.

Add Backends (Servers) to Your Backend Set
After the backend set is created, you can add compute instances (backend servers) to it. To add a backend server, you can enter the OCID for each instance and your application port. The OCID enables the Console to create the security list rules required to enable traffic between the load balancer subnets and the instance subnets.

Tip:

Security lists are virtual firewall rules for your VCN that provide ingress and egress rules to specify the types of traffic allowed in and out of a subnet. Update your VCN's security list rules to allow traffic flow between the load balancer subnets and the backend server subnets. In this step, you can have the security lists automatically updated by providing the instance OCIDs.

To add a server to your backend set:
1. On the details page of your load balancer, click Backend Sets. The backend set you just created is displayed.
2. Click the name of the backend set and view its details.
3. Click Edit Backends.

In the dialog:

1. Ensure that Help me create proper security list rules is checked.
2. OCID: Paste the OCID of the first instance (Webserver1).
3. Port: Enter 80.
4. Weight: Leave blank to weight the servers evenly.
5. Repeat Steps 2 through 4, pasting in the OCID for the second instance (Webserver2).
6. Click Create Rules.

The following figure shows the components created in this task:
What rules are added to my security lists?

The system updates the security list used by your load balancer subnets to allow egress traffic from the load balancer to each backend server's subnet:

- Updates to the security list for your load balancer subnets:
  - Allow egress traffic to the backend server 1 subnet (for example, Public-Subnet-AD1)
  - Allow egress traffic to the backend server 2 subnet (for example, Public-Subnet-AD2)

![Egress Rules for LB Security List](image)

The system updates the security list used by your backend server subnets to allow ingress traffic from the load balancer subnets:
Welcome to Oracle Cloud Infrastructure

- Updates to the security list for your backend server subnets:
  - Allow ingress traffic from load balancer subnet 1
  - Allow ingress traffic from load balancer subnet 2

![Ingress Rules for Default Security List](image1)

**How do I get the OCID of an instance?**

The OCID (Oracle Cloud Identifier) is displayed when you view the instance, on the instance details page.

1. In the dialog, right-click **View Instances** and select a browser option to open the link in a new tab.

![Edit Backends](image2)

A new Console browser tab launches, displaying the instances in the current compartment.

2. In the tab that just opened, if your instances are not in the current compartment, select the compartment to which the instance belongs. (Select from the list on the left side of the page.)

A shortened version of the OCID is displayed next to each instance.

3. Click the instance that you're interested in.

A shortened version of the OCID is displayed on the instance details page.

4. Click **Copy** to copy the OCID. You can then paste it into the Instance ID field.
Create the Listener for Your Load Balancer

A listener is an entity that checks for connection requests. The load balancer listener listens for ingress client traffic using the port you specify within the listener and the load balancer's public IP.

In this tutorial, you define a listener that accepts HTTP requests on port 80.

Note:

Listening on Multiple Ports
A listener can listen on one port. To listen on more ports (such as 443 for SSL), create another listener. For information on enabling SSL for your load balancer, see "Managing SSL Certificates" in the Oracle Cloud Infrastructure User Guide.

To create a listener:

1. On your Load Balancer Details page, click Listeners.
2. Click Create Listener.
3. Enter the following:
   - Name: Enter a friendly name. Avoid entering confidential information.
   - Protocol: Select HTTP.
   - Port: Enter 80 as the port on which to listen for incoming traffic.
   - Backend Set: Select the backend set you created.
4. Click Create.

Update Load Balancer Security Lists and Allow Internet Traffic to the Listener

When you create a listener, you must also update your VCN's security list to allow traffic to that listener.

Allow the Listener to Accept Traffic

The subnets where the load balancer resides must allow the listener to accept traffic. To enable the traffic to get to the listener, update the load balancer subnet's security list.

To update the security list to allow the listener to accept traffic:

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   - The list of VCNs in the current compartment is displayed.
2. Click Security Lists. A list of the security lists in the cloud network is displayed.
3. Click the LB Security List. The details are displayed.
4. Click Edit All Rules.
5. Under Allow Rules for Ingress, click Add Rule.
6. Enter the following ingress rule:
   - Source Type: Select CIDR
   - Source CIDR: Enter 0.0.0.0/0
   - IP Protocol: Select TCP
   - Destination Port Range: Enter 80 (the listener port).

If you created other listeners, add an ingress rule for each listener port to allow traffic to the listener. For example, if you created a listener on port 443, repeat the previous steps using Destination Port Range: 443.

The following figure shows the component created in this task:
Verify Your Load Balancer

To test your load balancer's functionality, you can open a web browser and navigate to its public IP address (listed on the load balancer's detail page). If the load balancer is properly configured, you can see the name of one of the web server instances:

1. Open a web browser.
2. Enter the load balancer public IP address.
   
The index.htm page of one of your web servers appears.

3. Refresh the web page.
   
The index.htm page of the other web server now appears.
Because you configured the load balancer backend set policy as Round Robin, refreshing the page alternates between the two web servers.

**Update Rules to Limit Traffic to Backend Servers**

Update the default security list and the default route table to limit traffic to your backend servers. If you used the *Create Virtual Cloud Network Plus Related Resources* option to create your VCN and you are not going to terminate this load balancer immediately, these actions are important.

**To delete the default route table rule:**

1. Open the navigation menu. Under *Core Infrastructure*, go to *Networking* and click *Virtual Cloud Networks*.
2. Click the name of your VCN and review its details.
3. Under *Resources*, click *Route Tables*.
4. Click the Default Route Table for the VCN.
5. Click *Edit Route Rules*.
6. Click the X next to the route rule, and then click *Save*.

There are now no Route Rules for the default route table.

**To edit the default security list rules:**

1. Go to your *Virtual Cloud Network Details* page.
3. Click the Default Security List for the VCN.
4. Click *Edit All Rules*.
5. Under *Allow Rules for Ingress*, delete the following rules:

<table>
<thead>
<tr>
<th>Action</th>
<th>Source CIDR</th>
<th>IP Protocol</th>
<th>Destination Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>22</td>
</tr>
<tr>
<td>Delete</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>3,4</td>
</tr>
<tr>
<td>Delete</td>
<td>10.0.0.0/16</td>
<td>ICMP</td>
<td>3</td>
</tr>
</tbody>
</table>

6. Under *Allow Rules for Egress*, delete the rule. There can be no Egress Rules.

Now your instances can receive data traffic from, and direct traffic to, only the load balancer subnets. You no longer can connect directly to your instance's public IP address.

**Delete Your Load Balancer**

When your load balancer becomes available, you are billed for each hour that you keep it running. Once you no longer need a load balancer, you can delete it. When the load balancer is deleted, you stop incurring charges for it. Deleting a load balancer does not affect the backend servers or subnets used by the load balancer.

To delete your load balancer:

1. Open the navigation menu. Under the *Core Infrastructure* group, go to *Networking* and click *Load Balancers*.
2. Choose the *Compartment* that contains your load balancer.
3. Next to your load balancer, click the Actions icon (three dots), and then click *Terminate*.
4. Confirm when prompted.

If you want to delete the instances and VCN you created for this tutorial, follow the instructions in *Cleaning Up Resources from the Tutorial* on page 72.

**Getting Started with Audit**

This chapter provides a hands-on tutorial to introduce you to the components of the Oracle Cloud Infrastructure Audit service.
Welcome to Oracle Cloud Infrastructure

The Oracle Cloud Infrastructure Audit service is included with your Oracle Cloud Infrastructure tenancy. The Audit service automatically records calls to the public application programming interface (API) endpoints for your Oracle Cloud Infrastructure tenancy. The service records events relating to the actions taken on the Oracle Cloud Infrastructure resources. Events recorded in the log can be viewed, retrieved, stored, and analyzed. These log events include information such as:

- ID of the caller
- target resource
- time of the recorded event
- request parameters
- response parameters

This task helps you get started with the Audit service by showing you how to find and view a specific event.

For complete details on Audit, see "Overview of the Audit in the Oracle Cloud Infrastructure User Guide."

**Prerequisite**

To create an event to view, create and delete a VCN in the Networking service.

**Create and Delete a VCN**

1. Select the *compartment* (from the list on the left) in which you want to create the VCN.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
3. Click Create Virtual Cloud Network.
4. Enter the following:
   a. Name: Enter "Audit_Test".
   b. CIDR Block: Enter "10.0.0.0/16".
   c. Leave all other fields with their default settings. Click Create Virtual Cloud Network.

The VCN is displayed in the list.

5. Next to your VCN name, click the **OCID: Copy** link. You will use the **OCID** to help you find the event.
6. Terminate the VCN: Click the Actions icon (three dots), and then click **Terminate**. Confirm when prompted.

**Using Audit to View Events**

In this task, you will use Audit to find the delete VCN event.

**Tip:**

Audit time stamps events according to Greenwich Mean Time (GMT). Before you get started, be aware of your local time zone offset.

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Audit.

The list of events that occurred in the current compartment is displayed. Audit logs are organized by compartment, so if you are looking for a particular event, you must know which compartment the event occurred in.

2. From the **Compartments** list, select the compartment in which you created the VCN.

The list of events for the compartment is displayed.
3. To find the delete VCN event, you can try the following filters:

**Filter by time**

- **a.** Click in the **Start Date** box to display the date and time editor.
- **b.** Select the current date from the calendar. Type or select values for hour and minute to approximate the preceding hour. Enter the time as Greenwich Mean Time (GMT) using 24-hour clock notation.
- **c.** Repeat the above steps to enter an end date for the current date and time, so that you filter results for the preceding hour.

**Example**

If you are in located in the America/Los Angeles time zone and you are looking for an event that occurred between 1:15 PM and 2:15 PM local time on October 25, enter 21:15 and 22:15 to account for the GMT offset.

d. Click **Search**.

**Filter events by keywords**

You can further filter the results list to display only log entries that include a specific text string. Try the following entries to help you find the delete VCN event:

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you filter by keywords, use quotes to avoid results that have a similar string embedded in a longer string. For example, the quotes around ...</td>
</tr>
</tbody>
</table>
Welcome to Oracle Cloud Infrastructure

the responseStatus "204" prevent matches of 204 embedded in a longer string somewhere else in the audit event.

- Filter by the responseStatus value
  In the Keywords box, type "204" and click Search to display only events that returned the 204 (i.e., deleting resource) response status.
- Filter by requestResource value
  In the Keywords box, paste the VCN OCID that you copied to your clipboard in the prerequisite step and click Search.

Review the events to find the DELETE event.

Filter events by request action types

- Filter by the request action types
  In Request Actions Types, select "DELETE" and click Search.

The list filters to show only DELETE events. Scan the list to find your VCN termination event.

4. View the details of your event:
   - To see only the top-level details, click the down arrow to the right of an event.
   - To see lower-level details, click { . . . } to the right of the collapsed parameter.

Getting Started with Oracle Platform Services

This chapter helps you get started with Oracle Platform Services on Oracle Cloud Infrastructure.

Note:
Oracle Platform Services are not available in Oracle Cloud Infrastructure Government Cloud tenancies.

Supported Platform Services

The following platform services are supported on Oracle Cloud Infrastructure:

- Analytics Cloud
- API Platform Cloud Service
- Autonomous Data Warehouse
- Integration
- Autonomous Mobile Cloud Enterprise
- NoSQL Database Cloud Service
- Oracle Visual Builder
- Content and Experience Cloud
- Data Hub Cloud Service
- Data Integration Platform Cloud
- Database Cloud Service
- Developer Cloud Service
- Event Hub Cloud Service
- Java Cloud Service
- Oracle SOA Cloud Service

For services that are supported on both Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic, you can choose Oracle Cloud Infrastructure during instance creation by selecting an appropriate region.
Welcome to Oracle Cloud Infrastructure

Understand the Infrastructure Prerequisites

Before creating instances of your service on Oracle Cloud Infrastructure, you must create certain resources in Oracle Cloud Infrastructure for use by your platform service instances.

See "Prerequisites for Oracle Platform Services on Oracle Cloud Infrastructure" in the Oracle Cloud Infrastructure User Guide.

Learn About Service-Specific Differences and Workflows

Broadly, the service features are the same regardless of the infrastructure you choose (Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic), but differences may exist in some services. And the workflows for creating instances on Oracle Cloud Infrastructure may vary across services.

See the following documentation:

<table>
<thead>
<tr>
<th>Service</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Hub Cloud Service</td>
<td>About Oracle Data Hub Cloud Service Clusters in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Database Cloud Service</td>
<td>About Database Deployments in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Event Hub Cloud Service</td>
<td>About Instances in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Java Cloud Service</td>
<td>About Java Cloud Service Instances in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Oracle SOA Cloud Service</td>
<td>About SOA Cloud Service Instances in Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure</td>
</tr>
</tbody>
</table>

REST API Endpoints for Platform Services

You can use the following URL structure to access the REST API endpoints for a Platform Service:

https://<rest_server>/<endpoint_path>

where:

- `<endpoint_path>` is the relative path that defines the REST resource. For a list of available paths, refer to the REST API documentation for the specific service.
- `<rest_server>` is the REST server. Choose the REST server based on the region in which your platform service was created. Refer to the following table.

<table>
<thead>
<tr>
<th>REST Server</th>
<th>Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>psm.us.oraclecloud.com</td>
<td>• US East (Ashburn)</td>
</tr>
<tr>
<td></td>
<td>• US West (Phoenix)</td>
</tr>
<tr>
<td></td>
<td>• US West (San Jose)</td>
</tr>
<tr>
<td></td>
<td>• Canada Southeast (Montreal)</td>
</tr>
<tr>
<td></td>
<td>• Canada Southeast (Toronto)</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 120
Welcome to Oracle Cloud Infrastructure

<table>
<thead>
<tr>
<th>REST Server</th>
<th>Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>psm.europe.oraclecloud.com</td>
<td>• Germany Central (Frankfurt)</td>
</tr>
<tr>
<td></td>
<td>• Netherlands Northwest (Amsterdam)</td>
</tr>
<tr>
<td></td>
<td>• Saudi Arabia West (Jeddah)</td>
</tr>
<tr>
<td></td>
<td>• Switzerland North (Zurich)</td>
</tr>
<tr>
<td></td>
<td>• UAE East (Dubai)</td>
</tr>
<tr>
<td></td>
<td>• UK South (London)</td>
</tr>
<tr>
<td></td>
<td>• UK West (Newport)</td>
</tr>
<tr>
<td>psm.aucom.oraclecloud.com</td>
<td>• Australia East (Sydney)</td>
</tr>
<tr>
<td></td>
<td>• Australia Southeast (Melbourne)</td>
</tr>
<tr>
<td></td>
<td>• India West (Mumbai)</td>
</tr>
<tr>
<td></td>
<td>• India South (Hyderabad)</td>
</tr>
<tr>
<td></td>
<td>• Japan Central (Osaka)</td>
</tr>
<tr>
<td></td>
<td>• Japan East (Tokyo)</td>
</tr>
<tr>
<td></td>
<td>• South Korea Central (Seoul)</td>
</tr>
<tr>
<td></td>
<td>• South Korea North (Chuncheon)</td>
</tr>
<tr>
<td>psm.brcom-central-1.oraclecloud.com</td>
<td>• Brazil East (Sao Paulo)</td>
</tr>
<tr>
<td></td>
<td>• Chile (Santiago)</td>
</tr>
<tr>
<td>psm-&lt;account_name&gt;.console.oraclecloud.com</td>
<td>All regions</td>
</tr>
<tr>
<td></td>
<td>&lt;account_name&gt; is your tenant name or cloud account name</td>
</tr>
<tr>
<td>psm-cacct-&lt;account_id&gt;.console.oraclecloud.com</td>
<td>All regions</td>
</tr>
<tr>
<td></td>
<td>&lt;account_id&gt; is the alphanumeric ID of your tenant name or cloud account</td>
</tr>
</tbody>
</table>

You can find `<account_name>` or `<account_id>` in either:
- The welcome email sent to your cloud account administrator
- The URL used to access the console for the Platform Service

### Getting Started with Oracle Applications

This chapter helps you get started with Oracle Applications on Oracle Cloud Infrastructure.

### Support for Oracle Applications

Oracle Cloud Infrastructure is an ideal place to host your Oracle Applications. You can deploy and manage Oracle applications on Oracle Cloud Infrastructure using the standard procedures found in the application product documentation, or using Oracle-provided automation solutions (available for some applications).

Oracle applications that meet the following criteria are supported:

- The application version is under Premier, Extended, or Sustained support.
- You plan to run the application on an operating system and database version that is supported on Oracle Cloud Infrastructure and certified for the application.

Oracle offers solutions and documentation to make deploying applications on Oracle Cloud Infrastructure easier. Solutions are available for the following applications:

- [Oracle E-Business Suite](#)
Welcome to Oracle Cloud Infrastructure

• Oracle JD Edwards EnterpriseOne
• Oracle PeopleSoft

Setting Up Your Tenancy

After Oracle creates your tenancy in Oracle Cloud Infrastructure, an administrator at your company will need to perform some set up tasks and establish an organization plan for your cloud resources and users. Use the information in this topic to help you get started.

Tip:
To quickly get some users up and running while you are still in the planning phase, see Adding Users on page 57.

Create a Plan

Before adding users and resources you should create a plan for your tenancy. Fundamental to creating your plan is understanding the components of the Oracle Cloud Infrastructure Identity and Access Management (IAM). Ensure that you read and understand the features of IAM. See "Overview of the IAM" in the Oracle Cloud Infrastructure User Guide.

Your plan should include the compartment hierarchy for organizing your resources and the definitions of the user groups that will need access to the resources. These two things will impact how you write policies to manage access and so should be considered together.

Use the following primer topics to help you get started with your plan:

• Understanding Compartments on page 122
• Consider Who Should Have Access to Which Resources on page 123

Understanding Compartments

Compartments are the primary building blocks you use to organize your cloud resources. You use compartments to organize and isolate your resources to make it easier to manage and secure access to them.

When your tenancy is provisioned, a root compartment is created for you. Your root compartment holds all of your cloud resources. You can think of the root compartment like a root folder in a file system.

The first time you sign in to the Console and select a service, you will see your one, root compartment.
Welcome to Oracle Cloud Infrastructure

You can create compartments under your root compartment to organize your cloud resources in a way that aligns with your resource management goals. As you create compartments, you control access to them by creating policies that specify what actions groups of users can take on the resources in those compartments.

Keep in mind the following when you start working with compartments:

• At the time you create a resource (for example, instance, block storage volume, VCN, subnet), you must decide in which compartment to put it.
• Compartments are logical, not physical, so related resource components can be placed in different compartments. For example, your cloud network subnets with access to an internet gateway can be secured in a separate compartment from other subnets in the same cloud network.
• You can create a hierarchy of compartments up to six compartments deep under the tenancy (root compartment).
• When you write a policy rule to grant a group of users access to a resource, you always specify the compartment to apply the access rule to. So if you choose to distribute resources across compartments, remember that you will need to provide the appropriate permissions for each compartment for users that will need access to those resources.
• In the Console, compartments behave like a filter for viewing resources. When you select a compartment, you only see resources that are in the compartment selected. To view resources in another compartment, you must first select that compartment. You can use the Search feature to get a list of resources across multiple compartments. See Overview of Search on page 3626.
• You can use the tenancy explorer to get a complete view of all the resources (across regions) that reside in a specific compartment. See Viewing All Resources in a Compartment on page 235.
• If you want to delete a compartment, you must delete all resources in the compartment first.
• Finally, when planning for compartments you should consider how you want usage and auditing data aggregated.

Consider Who Should Have Access to Which Resources

Another primary consideration when planning the setup of your tenancy is who should have access to which resources. Defining how different groups of users will need to access the resources will help you plan how to organize your resources most efficiently, making it easier to write and maintain your access policies.

For example, you might have users who need to:
• View the Console, but not be allowed to edit or create resources
Welcome to Oracle Cloud Infrastructure

- Create and update specific resources across several compartments (for example, network administrators who need to manage your cloud networks and subnets)
- Launch and manage instances and block volumes, but not have access to your cloud network
- Have full permissions on all resources, but only in a specific compartment
- Manage other users' permissions and credentials

To see some sample policies, see "Common Policies" in the Oracle Cloud Infrastructure User Guide.

Sample Approaches to Setting Up Compartments

Put all your resources in the tenancy (root compartment)

If your organization is small, or if you are still in the proof-of-concept stage of evaluating Oracle Cloud Infrastructure, you might consider placing all of your resources in the root compartment (tenancy). This approach makes it easy for you to quickly view and manage all your resources. You can still write policies and create groups to restrict permissions on specific resources to only the users who need access.

High-level tasks to set up the single compartment approach:

1. (Best practice) Create a sandbox compartment. Even though your plan is to maintain your resources in the root compartment, Oracle recommends setting up a sandbox compartment so that you can give users a dedicated space to try out features. In the sandbox compartment you can grant users permissions to create and manage resources, while maintaining stricter permissions on the resources in your tenancy (root) compartment. See Create a Sandbox Compartment.


Create compartments to align with your company projects

Consider this approach if your company has multiple departments that you want to manage separately or if your company has several distinct projects that would be easier to manage separately.

In this approach, you can add a dedicated administrators group for each compartment (project) who can set the access policies for just that project. (Users and groups still must be added at the tenancy level.) You can give one group control over all their resources, while not allowing them administrator rights to the root compartment or any other projects. In this way, you can enable different groups at your company to set up their own "sub-clouds" for their own resources and administer them independently.

High-level tasks to set up the multiple project approach:

1. Create a sandbox compartment. Oracle recommends setting up a sandbox compartment so you can give users a dedicated space to try out features. In the sandbox compartment you can grant users permissions to create and manage resources, while maintaining stricter permissions on the resources in your tenancy (root) compartment.

2. Create a compartment for each project, for example, ProjectA, ProjectB.

3. Create an administrators group for each project, for example, ProjectA_Admins.

4. Create a policy for each administrators group.

   Example:
   
   Allow group ProjectA_Admins to manage all-resources in compartment ProjectA


6. Let the administrators for ProjectA and ProjectB create subcompartments within their designated compartment to manage resources.

7. Let the administrators for ProjectA and ProjectB create the policies to manage the access to their compartments.

Create compartments to align with your security requirements

Consider this approach if your company has projects or applications that require different levels of security.
A security zone is associated with a compartment and a security zone recipe. When you create and update resources in a security zone, Oracle Cloud Infrastructure validates these operations against the policies in the security zone recipe. If any security zone policy is violated, then the operation is denied.

In this approach, you create security zone compartments for projects that must comply with our maximum security architecture and best practices. You create standard compartments for projects that don't require this level of security compliance.

Security zone policies align with Oracle security principles, including:

- Data in a security zone can't be copied to a standard compartment because it might be less secure.
- Resources in a security zone must not be accessible from the public internet.
- Resources in a security zone must use only configurations and templates approved by Oracle.

**Caution:**

To ensure the integrity of your data, you can't move certain resources from a security zone compartment to a standard compartment.

Similar to the previous approach, you can add a dedicated administrator group for each compartment who can then set the access policies for that single project.

- Access (IAM) policies grant users the ability to manage certain resources in a compartment.
- Security zone policies ensure that management operations in a security zone compartment comply with Oracle security best practices.

To learn more, see [Security Zones](#).

**Getting Help and Contacting Support**

When using Oracle Cloud Infrastructure, sometimes you need to get help from the community or to talk to someone in Oracle support. This topic provides more information about accessing these tools.

**Tip:**

Console announcements appear at the top of the Console to communicate timely, important information about service status. For more information, see [Console Announcements](#).

1. **Use a search engine**

   For common issues, someone else has likely asked this question in the past. You can use scoped search to look for answers in our documentation and our forum platforms – Cloud Customer Connect and Stack Overflow. To perform a scoped search, go to your favorite search engine and specify the site URLs along with your specific search terms, as follows:

   ```
   <Your Search Terms> (site:docs.cloud.oracle.com/iaas OR site:cloudcustomerconnect.oracle.com OR site:stackoverflow.com)
   ```

2. **Use Live Chat in the Console**

   Use Live Chat in the Console to get immediate help with common issues. To start a live online chat with an Oracle Support or Sales representative, at the top of the Console, click the **Live Chat** button ( ). A chat window opens that connects you to Oracle Support.

3. **Post a question to our forums**

   If you can't find an answer to your question through search, submit a new question to one of the forums we support. This option is available to all customers.
Cloud Customer Connect

For any issue related to Oracle Cloud Infrastructure, including provisioning of new resources, Console issues, identity, networking, documentation, storage, database, Edge services, or other solutions, you can post a question to Cloud Customer Connect at:

https://cloudcustomerconnect.oracle.com/resources/9c8fa8f96f/summary

If you are using only Always Free resources or using a Free Tier account, use Cloud Customer Connect for support queries.

Stack Overflow

If you are creating an application that integrates with Oracle Cloud Infrastructure APIs, endpoints, or services, you can also use Stack Overflow forums for development-related questions. Tag your questions with oracle-cloud-infrastructure, as follows:

https://stackoverflow.com/questions/tagged/oracle-cloud-infrastructure

4. Open a support service request

This option is only available to paid accounts.

The first time you open a support request, you're automatically taken through a series of steps to provision your support account. If you want to make changes or if you run into problems, see Configuring Your Oracle Support Account on page 130.

Note:

Customers using only Always Free resources and customers using Free Tier accounts are not eligible for Oracle Support. You must upgrade to a paid account to access Oracle Support. If you need support, post a question to Cloud Customer Connect.

If the preceding options did not resolve your issue and you need to talk to someone, you can create a support request. In addition to support for technical issues, you can open support requests if you need to:

• Reset the password or unlock the account for the tenancy administrator
• Add or change a tenancy administrator
• Ask a question about billing and payments
• Request a service limit increase
• Request a root cause analysis (RCA)

Creating a Service Request Using the Console

To create a support ticket

1. Open the Help menu ( ), go to Support, and click Create support request.
2. Enter the following:
   • Issue Summary: Enter a title that summarizes your issue. Avoid entering confidential information.
   • Describe Your Issue: Provide a brief overview of your issue.
     • Include all the information that support needs to route and respond to your request. For example, "I am unable to connect to my Compute instance."
     • Include troubleshooting steps taken and any available test results.
   • Select the severity level for this request.
3. Click Create Request.

To request a root cause analysis (RCA)

To request a root cause analysis for an outage, create a support request and include Root Cause Analysis (RCA) Request in the Issue Summary field.
To request a service limit increase

1. Open the Help menu, go to Support and click Request service limit increase.
2. Enter the following:
   - **Primary Contact Details:** Enter the name and email address of the person making the request. Enter one email address only. A confirmation will be sent to this address.
   - **Service Category:** Select the appropriate category for your request.
   - **Resource:** Select the appropriate resource.
     Depending on your selection for resource, additional fields might display for more specific information.
   - **Reason for Request:** Enter a reason for your request. If your request is urgent or unusual, please provide details here.
3. Click Create Request.

After you submit the request, it is processed. A response can take anywhere from a few minutes to a few days. If your request is granted, a confirmation email is sent to the address provided in the primary contact details.

If we need additional information about your request, a follow-up email is sent to the address provided in the primary contact details.

To view support tickets

- Open the Help menu, go to Support and click View support requests.

To add a comment to a support ticket

1. Open the Help menu, go to Support and click View support requests.
   A list of technical support requests appears.
2. Click the name of the support request on which you want to comment.
3. Under Comments, click Add Comment.
   The Add Comment dialog appears.
4. Type your comment, and then click Add Comment.

To close a support ticket

1. Open the Help menu, go to Support and click View support requests.
   A list of technical support requests appears.
2. Click the name of the support request you want to close.
3. Click Close Request.
   The Request to close dialog appears.
4. Enter the reason for closing the ticket, and then click Close Request.

Creating a Service Request Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage support requests with the API, use the Support Management API.
Locating Oracle Cloud Infrastructure IDs

Use the following tips to help you locate identifiers you might be asked to provide.

Finding Your Customer Support Identifier (CSI)

The Customer Support Identifier (CSI) number is generated after you purchase Oracle Cloud services. This number can be found in several places, including in your contract document and also on your tenancy details page. You’ll need the CSI number to register and log support requests in My Oracle Support (MOS).

To find your CSI number:

1. Open the Profile menu and click Tenancy: <your_tenancy_name>.
2. The CSI number is shown under Tenancy Information.

Finding Your Tenancy OCID (Oracle Cloud Identifier)

Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the Tenancy Details page:

1. Open the Profile menu and click Tenancy: <your_tenancy_name>.
2. The tenancy OCID is shown under Tenancy Information. Click Copy to copy it to your clipboard.

Finding the OCID of a Compartment

The OCID (Oracle Cloud Identifier) of a resource is displayed when you view the resource in the Console, on the resource details page.
For example, to get the OCID for a Compute instance:

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Compartments**.
   A list of the compartments in your tenancy is displayed.
   A shortened version of the OCID is displayed next to each compartment.

   ![Compartments](image)

2. Click the shortened OCID string to view the entire value in a pop-up. Click **Copy** to copy the OCID to your clipboard. You can then paste it into the service request form field.

**Finding the OCID of a Resource**

The OCID (Oracle Cloud Identifier) of a resource is displayed when you view the resource in the Console, both in the list view and on the details page.

For example, to get the OCID for a compute instance:

1. Open the Console.
2. Select the **Compartment** to which the instance belongs from the list on the left side of the page.
   
   Note that you must have appropriate permissions in a compartment to view resources.
3. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. A list of instances in the selected compartment is displayed.
4. Click the instance that you're interested in.
   A shortened version of the OCID is displayed on the instance details page.
5. Click **Copy** to copy the OCID to your clipboard. You can then paste it into the service request form field.

**Finding Your opc-request-id in the Console**

To locate the opc-request-id value when you are using the Oracle Cloud Infrastructure Console, you must first access the developer tools in the browser in which you are running the Console. Depending on your browser, this is called either Developer Tools or Web Console and can be opened by clicking **F12**. In Safari on a Mac, it's called the Web Inspector.

1. Open your browser's developer tools by clicking **F12** (in Safari on Mac, click **Option + Cmd + i**).
2. Select the **Network** tab, then filter on XHR.

   ![Network Tab](image)

   **Note:**

   Different browsers present filtering options in different ways. Firefox present an XHR filtering button on the Network tab UI. Internet Explorer and Edge provide a filter icon with the label **Content type**, which you click to expose an XHR filter.

3. Select results that return a 500 error to view the request details.
4. In the request details pane, click the **Headers** tab.
5. Locate and copy both the opc-request-id and date values and include them in your support ticket.
Configuring Your Oracle Support Account

The first time you use Oracle Support in the Console, you're automatically taken through a series of steps to provision your support account. If you want to make changes or if you run into problems, this topic explains how to manually update your support account settings. If you're a tenancy administrator, the first time you use Oracle Support in the Console, you might need to approve yourself as a user in MOS.

The following steps are automatically completed for you during the provisioning process. These sections explain how to manually change your account settings.

- Approve pending users (administrators)
- Add an email to your IAM user account
- Create an Oracle Single Sign On (SSO) account
- Change your linked account

To use an identity provider other than IAM, IDCS, or Okta, follow the steps to link the identity provider account to your MOS account.

Approving Pending Users (Administrators)

If you're an administrator, you need to accept the MOS terms of service and approve pending users. Follow these steps to approve users in MOS:

1. Go to https://support.oracle.com and sign in.
2. Accept the terms and conditions, and then click Next.
3. Navigate to the My Account page: Go to your user name at the top of the page, open the menu, and then click My Account.
4. In the menu bar at the top of the page, click the Message Center icon, and then click Approve Pending User Request.
5. Approve the user.

Adding an Email to Your IAM User Account

To create support requests in the Console, your user account must have an associated email address. The first time you create a support request in the Console, the provisioning process adds this email for you. If you want to add the email manually, you can follow these steps.

If your user account already has an email address or you aren't an IAM user, this section does not apply.

1. Open the Profile menu ( altında) and click User Settings. Your Oracle Cloud Infrastructure IAM service User Details page is displayed.
2. Click Edit User.
3. In the Email field, enter your email, and then click Save Changes.

Creating an Oracle Single Sign On (SSO) Account

To create service requests with My Oracle Support, you need to have an Oracle Single Sign On account and register your Customer Support Identifier with My Oracle Support. The first time you create a support request in the Console, the provisioning process creates an Oracle Single Sign On account for you if needed. If you want to create the account manually, you can follow these steps.

- If you already have an Oracle SSO account with a registered CSI, use your existing account.
- If you have an Oracle SSO account but it doesn't have an associated CSI, see Registering Your CSI for Oracle Cloud Infrastructure on page 131.

Tip:

Before you begin this procedure, have your CSI number available. Not sure what that number is or how to locate it? See Finding Your Customer Support Identifier (CSI) on page 132.

To request an SSO account and register with My Oracle Support:
1. To create your Oracle Single Sign On account, go to the My Oracle Support Create Your Oracle Account page.
2. Enter your company email address in the Email address field, complete the rest of the form, and then click Create Account. A verification email is generated.

   **Important:**
   
   If you use an identity provider other than IAM, IDCS, or Okta, this email address must match the user name that you use with your identity provider.

3. Check your email account for an email from Oracle asking you to verify your email address.
4. Open the email and click Verify Email Address.
5. Sign in with the credentials you just set up.
6. At sign-in, you are prompted to enter a Note to the Approver and the Support Identifier (your CSI).
7. Click Request Access.
8. Enter the first five characters of the name of the organization that owns the Customer Support Identifier (listed in the Welcome letter), and then click Validate. The support identifier appears in the table.
9. Click Next.
10. Enter your contact information and click Next.
11. Accept the terms and click Next.

If you are the first person requesting this support identifier, the status of the request is pending until you receive approval from the Customer User Administrator (CUA) or from Oracle Support.

**Changing Your Linked Account**

If you want to change the Console user account linked to your MOS account, follow these steps. You might want to change your account if you have an Oracle support account that doesn't use your Oracle Cloud Infrastructure profile email. For information about IAM user accounts, see Signing In to the Console on page 41.

1. Open the Profile menu (👤) and click User Settings. Your Oracle Cloud Infrastructure IAM service User Details page is displayed.
2. Click More Actions > Link Support Account. The Oracle account sign-in page prompts you to enter your Oracle credentials.
3. Enter the User name and Password of the Oracle support account that you want to link to this user, and then click Sign in. The IAM user account is linked to the Oracle support account. The email address associated with the support account is displayed in the user details in the field My Oracle Support account.

**Using an Identity Provider Other than IAM, IDCS, or Okta**

If you use an identity provider other than IAM, IDCS, or Okta, to access support in the Console, your MOS email address must match the user name that you use with your identity provider.

If your identity provider user name and MOS email address do not match and you would like to access support in the Console, change your MOS email address to a value that matches your identity provider user name.

**Registering Your CSI for Oracle Cloud Infrastructure**

To submit support requests, your MOS account must be associated with your tenancy CSI number. If you already added the CSI for Oracle Cloud Infrastructure, these steps don't apply to you. If you previously registered for My Oracle Support but need to add the CSI for Oracle Cloud Infrastructure, the provisioning process registers your CSI for you, but if you want to register your CSI manually, you can follow these steps.

1. Go to https://support.oracle.com and sign in.
2. Navigate to the My Account page: Go to your user name at the top of the page, open the menu, and then click My Account.
3. The Support Identifiers region displays the accounts that your user name is associated with.
4. Click Request Access.
5. Enter a Note to the Approver and then enter the Support Identifier (your CSI).
6. Enter the first five characters of the name of the organization that owns the Customer Support Identifier (listed in the Welcome letter), and then click Validate. The support identifier appears in the table.
7. Click Next.
8. Enter your contact information and accept the terms. Click Next.

The status of the request is pending until you receive approval from the Customer User Administrator (CUA).

For more information about signing in and using My Oracle Support, see Registration, Sign In, and Accessibility Options in My Oracle Support Help.

Finding Your Customer Support Identifier (CSI)

The following steps explain how to locate your CSI number.

The Customer Support Identifier (CSI) number is generated after you purchase Oracle Cloud services. This number can be found in several places, including in your contract document and also on your tenancy details page. You’ll need the CSI number to register and log support requests in My Oracle Support (MOS).

To find your CSI number:

1. Open the Profile menu and click Tenancy: <your_tenancy_name>.
2. The CSI number is shown under Tenancy Information.

Task Mapping from My Services

This topic summarizes how to perform tasks that you previously performed in My Services prior to the Oracle Cloud Console updates.

Navigation and Task Flow Changes

The updates recently introduced to unify the Console experience enhance and simplify managing your cloud. To achieve the overall reduction in interfaces, some navigation paths and workflows have changed. The following tables summarize the changes to expect:

- Navigation and General Feature Changes on page 133
- Account Management Changes on page 133
- User Management and Identity Changes on page 134
- Platform Service Region Management Changes on page 134
# Navigation and General Feature Changes

<table>
<thead>
<tr>
<th>Task or Feature</th>
<th>Workflow in the Unified Console</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Landing page</strong></td>
<td>After signing in, you now land on the Oracle Cloud Console home page and access all services from this page. The navigation menu includes services that you previously navigated to through My Services. For general information about the Console home page, see Using the Console on page 42.</td>
</tr>
</tbody>
</table>
| **Navigate to Services**                | **Navigating to Platform Services**  
Open the navigation menu. Under More Oracle Cloud Services, go to Platform Services, and then click the service you want to access.  
**Navigating to Classic Data Management Services**  
Open the navigation menu. Under More Oracle Cloud Services, go to Classic Data Management Services, and then click the service you want to access.  
**Navigating to Classic Infrastructure Services**  
Open the navigation menu. Under More Oracle Cloud Services, go to Classic Infrastructure Services, and then click the service you want to access.  
**Navigating to the Applications Console**  
If your Cloud account also has Cloud Applications services provisioned, then you'll have access to the Applications Console.  
In the Console header, click Applications to switch to the Applications Console. |
| **View Platform or Classic Announcements** | Announcements for Platform and Classic services display in a banner above the header bar in the Console.                                                                                                                                 |
| **Navigate to My Home**                 | From the Oracle Cloud Console: Open the Profile menu (👤), and then click Service User Console.                                                                                                                                  |
| **Chat Support**                        | See Use Live Chat in the Console.                                                                                                                                                                                                 |

## Account Management Changes

<table>
<thead>
<tr>
<th>Task or Feature</th>
<th>Workflow in the Unified Console</th>
</tr>
</thead>
</table>
| **View Invoices**    | Open the navigation menu. Under Governance and Administration, go to Account Management and click Invoices.  
Your list of invoices is displayed. You can access your invoices in PDF format. |


<table>
<thead>
<tr>
<th>Task or Feature</th>
<th>Workflow in the Unified Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Services Cost Breakdown</td>
<td>View the breakdown of your Platform Services on the Cost Analysis page: Open the navigation menu. Under Governance and Administration, go to Account Management and click Cost Analysis.</td>
</tr>
</tbody>
</table>

**User Management and Identity Changes**

<table>
<thead>
<tr>
<th>Task or Feature</th>
<th>Workflow in the Unified Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone Cloud Administrator permissions</td>
<td>See Add a User with Oracle Cloud Administrator Permissions on page 58.</td>
</tr>
<tr>
<td>Add or revoke a Platform Service role (sometimes called a service entitlement) for a user</td>
<td>See Managing Oracle Identity Cloud Service Roles for Users on page 2379.</td>
</tr>
<tr>
<td>Add or revoke access to an instance</td>
<td>See Managing Instance Roles in the Console on page 2380.</td>
</tr>
<tr>
<td>Add roles to a group</td>
<td>See Managing Oracle Identity Cloud Service Roles for Groups on page 2381.</td>
</tr>
<tr>
<td>Edit an IDCS group name</td>
<td>See To edit details for an Oracle Identity Cloud Service group on page 2375.</td>
</tr>
<tr>
<td>Add users to an IDCS group</td>
<td>See To add users to a group on page 2376.</td>
</tr>
<tr>
<td>Change password</td>
<td>See Changing Your Password on page 52.</td>
</tr>
<tr>
<td>Open the Identity Cloud Service (IDCS) console</td>
<td>Open the navigation menu. Under Governance and Administration, go to Identity and click Federation. A list of the identity providers in your tenancy is displayed. Click the Oracle Identity Cloud Service Console link to open the Identity Cloud Service console.</td>
</tr>
</tbody>
</table>

**Platform Service Region Management Changes**

To view and subscribe to Platform Services regions

1. Open the Console, open the Region menu, and then click Manage Regions.
2. On the Manage Regions page, click Platform Services Regions.

The list of geographical regions is displayed. Regions that you have not subscribed to provide a button to create a subscription. A sample of the Platform Services Regions page is shown in the following screenshot:

3. To subscribe to a region, locate the region in the list and click Subscribe.

It might take several minutes to activate your tenancy in the new region.

Frequently Asked Questions

I’m not seeing Platform Services or Classic Services on my navigation menu. What happened?

Make sure that you are signing in with your Oracle Identity Cloud Service login credentials. To ensure that you sign in through IDCS:

2. Enter your tenancy name and click Next. The IDCS sign in page is displayed.
3. Enter your username and password and click Sign In.
4. On the Console, open the navigation menu. If your account has access to Platform or Classic services, you'll see them displayed on the menu under More Oracle Cloud Services. See also Navigating to More Oracle Cloud Services from the Console on page 44.

How do I get to my IDCS console?

To access the IDCS console:

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation. The list of identity providers is displayed. OracleIdentityCloudService is displayed in the list of identity providers, with details about the federation.
2. Click the link for **Oracle Identity Cloud Service Console**. An example is shown in the following screenshot.

![Oracle Identity Cloud Service Console](image)

The Oracle Identity Cloud service console opens in a new window.

**My team needs reports that were only available from My Services. How can I get back to the old dashboard?**

You can access the My Services dashboard by using this URL:

```plaintext
http://myservices-<tenancyname>.console.oraclecloud.com/mycloud/cloudportal/dashboard
```

where you replace `<tenancyname>` with your company's tenancy name.

**Where can I find more information about the changes to other task workflows and navigation?**

See [Task Mapping from My Services](#) on page 132.

**Where do I sign in to the Oracle Cloud Infrastructure Console?**

Go to [https://cloud.oracle.com](https://cloud.oracle.com).

You are prompted to enter your cloud tenant, your user name, and your password. Once authenticated, you are directed to a region your tenancy is subscribed to. You can **switch to other regions** you are subscribed to by using the region selector at the top of the Console.

If you need more help signing in, see [Signing In to the Console](#) on page 41.

**How do I find my tenancy home region?**

To find out what your home region is:

Open the **Profile** menu (🔗) and click **Tenancy: <your_tenancy_name>**.

The Tenancy details page shows your Home Region.

**What are my Oracle Cloud Infrastructure account service limits (or resource quotas) and can I request more?**

You can view your tenancy's service limits in the Console and request an increase. For more information and the default tenancy limits, see [Service Limits](#) on page 215.

**Where do I find information about what APIs are available?**

Oracle Cloud Infrastructure provides a set of APIs for the core services (network, compute, block volumes) as well as for the IAM and the Object Storage services.

See "API Requests" in the **Oracle Cloud Infrastructure User Guide.**
What browsers can I use with the Console?

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Why can't I sign in using Firefox?

If you are having trouble signing in to the Console using the Firefox browser, it might be due to one of the following conditions:

- You are in Private Browsing mode. The Console does not support Private Browsing mode. Open a new session of Firefox with Private Browsing turned off.
- You are not on the latest version of Firefox. Upgrade to the latest version. To check to see if you are on the latest version, follow these instructions: https://support.mozilla.org/en-US/kb/find-what-version-firefox-you-are-using
  When checking the version, note whether you are using Firefox or Firefox ESR.
- Your Firefox user profile is corrupted. To fix this issue:
  1. Upgrade to the latest version of Firefox.
  2. Create a new user profile and open Firefox with the new profile. See Mozilla Support for instructions on how to create a new user profile: https://support.mozilla.org/en-US/kb/profile-manager-create-and-remove-firefox-profiles

If none of the above resolves your issue, contact Oracle Support. In your problem description, make sure you specify whether you are using Firefox or Firefox ESR.

How do I know if I am in Private Browsing mode?

When you are in Private Browsing mode, a mask icon is displayed in the upper right corner of your Firefox window.

How do I change my password?

For Federated Users

If your company uses an identity provider (other than Oracle Identity Cloud Service) to manage user logins and passwords, you can't use the Console to update your password. You do that with your identity provider.

1. Sign in to the Console using the Oracle Cloud Infrastructure Username and Password.
2. After you sign in, go to the top-right corner of the Console, open the Profile menu (👤) and then click Change Password.

3. Enter the current password.
4. Follow the prompts to enter the new password, and then click Save New Password.

How do I reset my password if I forget it?

If you added an email address to your user settings, you can use the Forgot Password link on the sign-in page to have a temporary password sent to you. If you don’t have an email address included with your user details, then an administrator must reset your password. Contact your administrator to reset your password for you. Your administrator will give you a temporary password that is good for 7 days. If you do not use it in 7 days, the password will expire and you’ll need to get your administrator to create a new one-time password for you.

If you are the default or tenant administrator for your site and you forgot your password, contact Oracle Support. For tips on filing a service request, see Getting Help and Contacting Support on page 125.

How do I get support?

See Getting Help and Contacting Support on page 125.

Where do I find my Tenancy OCID?

Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the Tenancy Details page:

1. Open the Profile menu (👤) and click Tenancy: <your_tenancy_name>.
2. The tenancy OCID is shown under **Tenancy Information**. Click **Copy** to copy it to your clipboard.
Oracle Cloud Infrastructure Free Tier

Oracle Cloud Infrastructure's Free Tier includes a free time-limited promotional trial that allows you to explore a wide range of Oracle Cloud Infrastructure products, and a set of Always Free offers that never expire.

Free Trial

The Free Trial provides you with $300 of cloud credits that are valid for up to 30 days. You may spend these credits on any eligible Oracle Cloud Infrastructure service.

Getting Started

Start for Free

For more information, and to see a complete list of services available to you during the trial, visit the Free Trial website.

Note:

During sign up, choose your home region carefully. You can provision Always Free Autonomous Databases only in your home region.

For security purposes, most users will need a mobile phone number and a credit card to create an account. Your credit card will not be charged unless you upgrade your account.

When Your Trial Period Ends

After your trial ends, your account remains active. There is no interruption to the availability of the Always Free Resources you have provisioned. You can terminate and re-provision Always Free resources as needed.

Paid resources that were provisioned with your credits during your free trial are reclaimed by Oracle unless you upgrade your account.

Pay as You Go accounts are available with no commitment, or contact an Oracle sales representative in your location to learn about monthly and annual flex accounts that offers discounted pricing. For more information, see Oracle Cloud Infrastructure Pricing.

Always Free Resources

All Oracle Cloud Infrastructure accounts (whether free or paid) have a set of resources that are free of charge for the life of the account. These resources display the Always Free label in the Console.

Using the Always Free resources, you can provision a virtual machine (VM) instance, an Oracle Autonomous Database, and the networking, load balancing, and storage resources needed to support the applications that you want to build. With these resources, you can do things like run small-scale applications or perform proof-of-concept testing.

The following list summarizes the Oracle Cloud Always Free-eligible resources that you can provision in your tenancy:
Oracle Cloud Infrastructure Free Tier

- **Compute** (up to two instances)
- **Autonomous Database** (up to two database instances)
- **Load Balancing** (one load balancer)
- **Block Volume** (up to 100 GB total storage)
- **Object Storage** (up to 20 GiB)
- **Vault** (up to 20 keys and up to 150 secrets)

For detailed information about the Always Free resources, see Details of the Always Free Resources on page 142.

You can find your tenancy’s limits for Always Free resources in the Console. To check these limits: Open the navigation menu. Under Governance and Administration, go to Limits, Quotas and Usage.

**Quickly Launch Your Always Free Resources Using Resource Manager**

Oracle offers you the ability to automatically create a full set of Always Free resources in a few minutes using the Resource Manager service’s templates feature. Templates are pre-built Terraform configurations that help you easily create sets of resources used in common scenarios using a single, simple workflow. When you provision your Always Free resources using the provided template, your resources are created with the settings and configuration you need to start creating applications in the cloud. You don't need to have experience with Terraform to use the template. See To provision your Always Free using Terraform and Resource Manager for step-by-step instructions.

**To provision your Always Free using Terraform and Resource Manager**

**Tip:**
Note that Terraform refers to the set of resources being provisioned as a "stack". For a general introduction to Terraform and the "infrastructure-as-code" model, see Terraform: Write, Plan, and Create Infrastructure as Code.

1. Log into your Oracle Cloud Infrastructure account.
2. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
3. Click the Create Stack button to open the Create Stack dialog.
4. In the Create Stack dialog, click Sample Solution.
5. Click Select Solution to browse available solutions.
6. Select the check box for Sample E-Commerce Application.
7. Click Select Solution.
8. Optionally, provide a name for the new stack. If you don't provide a name, a default name is provided on the server. Avoid entering confidential information.
9. Optionally, provide a description for the stack.
10. Optionally, select a different compartment from your current compartment in which to create the stack. To do so, select a compartment from the Create In Compartment drop-down.
11. Click Next to proceed to the Configure Variables panel.
12. The variables displayed in the Configure Variables panel are auto-populated from the Terraform file that you uploaded. You don't need to change these variables if you are provisioning your Always Free resources using the Terraform file provided by Oracle.
13. Click Next to proceed to the Review panel.
14. Verify your stack configuration, then click Create to create your stack.

Your set of Always Free resources should take no more than a few minutes to provision.

**Upgrading to a Paid Account**

You can upgrade to a paid account at any time through the Oracle Cloud Infrastructure Console. To do so, click the Upgrade link in the banner at the top of the Console web page. If you don't see an Upgrade link on the page you are viewing, you can click the Oracle Cloud logo at the top of the Console and then look for the Upgrade link in the
sidebar on the right side of the Console home page. You will continue to have access to all of your cloud resources after upgrading your account.

Additional Information

See Frequenty Asked Questions: Oracle Cloud Infrastructure Free Tier on page 145 for answers to your questions about Free Tier accounts and resources.

Details of the Always Free Resources

This topic provides reference information about Oracle Cloud Infrastructure's Always Free resources.

Compute

All tenancies get two Always Free Compute virtual machine (VM) instances.

You must create the Always Free Compute instances in your home region.

Details of the Always Free Compute instance

- **Shape:** VM.Standard.E2.1.Micro
- **Processor:** 1/8th of an OCPU with the ability to use additional CPU resources
- **Memory:** 1 GB
- **Networking:** Includes one VNIC with one public IP address and up to 50 Mbps network bandwidth via the internet. Traffic to private IPs, on-premise endpoints via a Dynamic Routing Gateway, or to endpoints within the same Oracle Cloud region is up to 480 Mbps.
- **Operating System:** Your choice of one of the following Always Free-eligible operating systems:
  - Oracle Linux (including Oracle Autonomous Linux)
  - Canonical Ubuntu Linux
  - CentOS Linux

Tip:
The Linux operating systems labeled "Always Free Eligible" in the Console are compatible with Always Free Compute instances and incur no licensing fees. These operating systems are also compatible with paid resources and are available to users of paid accounts. To provision a Compute instance with an operating system that is not Always Free-eligible, you must have a paid account or a Free Trial account with available credits.

See Oracle-Provided Images on page 629 for more information about the available operating systems. For steps to create an Always Free-eligible Compute instance, see "Tutorial - Launching Your First Linux Instance" in the Oracle Cloud Infrastructure Getting Started Guide.

Database

All tenancies get two Always Free Oracle Autonomous Databases. The Autonomous Databases use shared Exadata infrastructure (meaning Oracle handles the database infrastructure provisioning and maintenance). For current regional availability, see the "Always Free Cloud Services" section of Data Regions for Platform and Infrastructure Services.

Details of the Always Free Oracle Autonomous Database instance

- **Processor:** 1 Oracle CPU processor (cannot be scaled)
- **Memory:** 8 GB RAM
• **Database Storage:** 20 GB storage (cannot be scaled)
• **Workload Type:** Your choice of either the transaction processing or data warehouse workload type
• **Maximum Simultaneous Database Sessions:** 20

**Tip:**
Always Free Autonomous Databases can be upgraded to paid instances after provisioning if you need features like more storage or CPU scaling.

**Note:**
• Before creating an Always Free Autonomous Database, check your home region for Always Free Autonomous Database support. See [Data Regions for Platform and Infrastructure Services](#).
• You cannot create an Always Free Autonomous Database in a Home Region where Always Free Autonomous Databases are not supported.
• Not all regions support the same database version. The supported version may be 19c-only or 21c-only, depending on the region.

See [Overview of the Always Free Autonomous Database](#) on page 1220 for additional product details. See [To create an Always Free Autonomous Database](#) on page 1159 for steps to create an Always Free Autonomous Database.

**Load Balancing**
All tenancies get one Always Free 10 Mbps load balancer.

**Details of the Always Free load balancer**
• **Shape:** Micro (10 Mbps)
• **Listeners:** 10
• **Virtual Hostnames:** 10
• **Backend Sets:** 10
• **Backend Servers:** 128

For information about provisioning an Always Free load balancer, see [Getting Started with Load Balancing](#) on page 103.

**Block Volume**
All tenancies receive a total of 100 GB of Always Free Block Volume storage, and five volume backups. These amounts apply to both boot volumes and block volumes combined. When you provision a Compute instance, the instance automatically receives a 50 GB boot volume for storage. You can also create and attach block volumes to expand the storage capacity of a Compute instance. For more information, see [Creating a Volume](#) on page 515 and [Attaching a Volume](#) on page 517.

**Details of the Always Free Block Volume resources**
• 100 GB total of combined boot volume and block volume Always Free Block Volume storage.
• Five total volume backups (boot volume and block volume combined).

When you create a Compute instance, the default boot volume size for the instance is 50 GB, which counts towards your allotment of 100 GB. You can customize the instance's boot volume size up to 100 GB; however, this will use up your full allotment of storage for Always Free Block Volume resources. Also, because the minimum boot volume size allowed for Compute instances is 50 GB, launching two instances will use all your Always Free Block Volume resources. Alternatively, you can launch one instance with the default boot volume size of 50 GB, and then create and attach a 50 GB block volume to expand the storage capacity of the instance. For more information, see [Creating a Volume](#) on page 515 and [Attaching a Volume](#) on page 517. Although it is possible to mix paid and Always Free resources, Oracle does not recommend this. If you have used up your allotment of Always Free Block Volume...
resources, you can free up block storage resources by terminating an Always Free instance and deleting the boot volume, or terminating an Always Free block volume.

You can have a maximum of five Always Free volume backups at any time. This applies to both boot volume and block volume backups. For example, you could have three boot volume backups for your Always Free instance and two block volume backups for your Always Free block volumes. In this example, if you try to create new backups, the operation will fail with an error until you delete existing Always Free volume backups. For more information about volume backups, see Overview of Block Volume Backups on page 540 and Overview of Boot Volume Backups on page 615.

Object Storage

All tenancies get a total of 20 GiB (gibibytes) of Always Free Object Storage.

Details of the Always Free Object Storage resources

If you have a free account (including trial accounts), Always Free includes the following:

- 20 GiB of combined Standard tier, Infrequent Access tier, and Archive tier data
- 50,000 Object Storage API requests per month

If you have a paid account, Always Free includes the following:

- 10 GiB of Standard tier data
- 10 GiB of Infrequent Access tier data
- 10 GiB of Archive tier data
- 50,000 Object Storage API requests per month

Important:

If you are participating in an Oracle Cloud Free Trial, you can store unlimited data and can use 20 GiB for free (your usage of the first 20 GiB incurs no deduction of your initial $300 trial credit balance). Upgrade to a paid account to continue access to unlimited storage. If you do not upgrade before your trial ends, your free account will be limited to 20 GiB of combined Standard tier, Infrequent Access tier, and Archive tier data. If you are using more than the 20-GiB limit when your Free Trial ends, all of your objects will be deleted. You can then upload objects until you reach your Always Free usage limits.

See Putting Data into Object Storage on page 82 for instructions on using your Always Free storage resources.

Resource Manager

All tenancies get the following Always Free resources for Resource Manager.

<table>
<thead>
<tr>
<th>Resource (per tenant)</th>
<th>Always Free resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration source providers</td>
<td>100</td>
</tr>
<tr>
<td>Jobs (concurrent)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Job duration: 24 hours</td>
</tr>
<tr>
<td>Private templates</td>
<td>10</td>
</tr>
</tbody>
</table>
## Resource (per tenant) | Always Free resources
---|---
Stacks | 10  
Variables per stack: 250  
Size per variable: 8192 bytes  
Zip file per stack: 11 MB

### Service Connector Hub

All tenancies get 2 Always Free service connectors.

**Details of the Always Free Service Connector Hub resources**

If you have a free account (including trial accounts), Always Free Service Connector Hub includes 2 Always Free service connectors.

If you have a paid account, see Service Connector Hub Limits on page 231.

### Vault

All master encryption keys protected by software are free. All tenancies get 20 key versions of master encryption keys protected by a hardware security module (HSM) and 150 Always Free Vault secrets. You can spread these keys or secrets across any number of vaults in the tenancy, although virtual private vaults are not included in the Always Free resources.

**Details of the Always Free Vault resources**

- all key versions of a master encryption key protected by software (across any number of keys or vaults)
- 20 total key versions of a master encryption key protected by an HSM (across any number of keys or vaults)
- 150 total Always Free secrets (across any number of vaults).
- 40 secret versions of any given secret (including up to 20 in some form of active use and 20 pending deletion).

If you have used up your allotment of Always Free secrets, you can release resources by scheduling a secret or secret version for deletion. At minimum, you do have to wait a day before the secret or secret version is deleted.

### Frequently Asked Questions: Oracle Cloud Infrastructure Free Tier

**I just signed up and I cannot access specific services. What can I do?**

Registering your account with all services and regions can take a few minutes. Check again after a few minutes have passed.

**How do I change which resources I want to designate as Always Free?**

In short, you cannot. Eligible resources are designated Always Free when they are created. After you provision an Always Free resource, the Always Free status is not transferable to another existing resource. However, you can delete an existing Always Free resource in order to create a new Always Free resource in its place.

**What happens when my Free Trial expires or my credits are used up?**

When you’ve reached the end of your 30 day trial, or used all of your Free Trial credits ( whichever comes first), you will no longer be able to create new paid resources. However, your account will remain active. Your existing resources will continue to run for a few days, allowing you to upgrade your account and keep your resources before they’re reclaimed by Oracle. (Note that reclaimed resources cannot be recovered—they are permanently deleted.)
Resources identified as Always Free will not be reclaimed. After your Free Trial expires, you'll continue to be able to use and manage your existing Always Free resources, and create new Always Free resources according to tenancy limits.

If I upgrade, do I keep my Free Trial credit balance?

Yes, if you upgrade during the Free Trial period, you will not be billed until you've reached the end of your 30 day trial, or used all of your Free Trial credits (whichever comes first). You will be notified by email when billing begins.

After I upgrade my account, can I downgrade?

There is no option to downgrade your account. However, with a paid account, you'll continue to have access to Always Free resources, and you'll only pay for the standard resources you use. No minimums and no prepayment are required for your paid account.

My resources no longer appear. How can I restore them?

If you have a Free Tier account and your resources no longer appear, it is likely that your Free Trial has expired and your paid resources have been reclaimed (terminated). You can verify this if this is the case by doing the following:

1. Log in to the Console
2. Check for a banner at the top of the Console with the following text: "You are using a Free Tier account. To access all services and resources, upgrade to a paid account."

If you see this message, your resources have been reclaimed and cannot be restored.

I get an "out of host capacity" error when I try to create an Always Free Compute instance. What can I do?

An "out of host capacity" error indicates a temporary lack of Always Free shapes in your home region. Oracle is working to provide more capacity, though it might take several days before additional capacity is available in your home region. Wait a while, and then try to launch the instance again.

Is it possible to extend my Free Trial?

If you need additional credits or time, you can schedule a call with an Oracle sales representative using the Upgrade page in the Console. Sales representatives have the authority to extend trials or issue additional credits if appropriate.

If you don't see an Upgrade link on the Console page you are viewing, you can click the Oracle Cloud logo at the top of the Console and then look for the Upgrade link in the sidebar on the right side of the page.

Is my Free Tier account eligible for support?

Community support through our forums is available to all customers. Customers using only Always Free resources are not eligible for Oracle Support. Limited support is available to Free Tier accounts with Free Trial credits. After you use all of your credits or after your trial period ends (whichever comes first), you must upgrade to a paid account to access Oracle Support. If you choose not to upgrade and continue to use Always Free Services, you will not be eligible to raise a service request in My Oracle Support. See Getting Help and Contacting Support on page 125.
Chapter 4

Oracle Cloud Infrastructure Government Cloud

Oracle Cloud Infrastructure includes the following government cloud services:

- Oracle Cloud Infrastructure US Government Cloud on page 148
- Oracle Cloud Infrastructure United Kingdom Government Cloud on page 171

Oracle Cloud Infrastructure US Government Cloud

Oracle Cloud Infrastructure US Government Cloud provides cloud services for two levels of government operators:

- Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization on page 157
- Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization on page 162

For All US Government Cloud Customers

This topic contains information common to both the US Government Cloud with FedRAMP High Joint Authorization Board authorization and to the US Federal Cloud with DISA Impact Level 5 authorization.

Shared Responsibilities

Oracle Cloud Infrastructure for government offers best-in-class security technology and operational processes to secure its enterprise cloud services. However, for you to securely run your workloads, you must be aware of your security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), and you are responsible for securely configuring your cloud resources. Security in the cloud is a shared responsibility between you and Oracle.

For more information about shared responsibilities in the Oracle Cloud, see the following white papers:

- Making Sense of the Shared Responsibility Model
- Oracle Cloud Infrastructure Security

Setting Up an Identity Provider for Your Tenancy

As a Government Cloud customer, you must bring your own identity provider that meets your agency’s compliance requirements and supports common access card/personal identity verification card (CAC/PIV) authentication. You can federate Oracle Cloud Infrastructure with SAML 2.0 compliant identity providers that also support CAC/PIV authentication. For instructions on setting up a federation, see Federating with Identity Providers on page 2362.

Remove the Oracle Cloud Infrastructure Default Administrator User and Any Other Non-Federated Users

When your organization signs up for an Oracle account and Identity Domain, Oracle sets up a default administrator for the account. This person will be the first IAM user for your company and will have full administrator access to your tenancy. This user can set up your federation.

After you have successfully set up the federation with your chosen identity provider, you can delete the default administrator user and any other IAM service local users you might have added to assist with setting up your tenancy.
Deleting the local, non-federated users ensures that only users in your chosen identity provider can access Oracle Cloud Infrastructure.

To delete the default administrator:

1. Sign in to the Console through your identity provider.
   
   **More details**
   
   a. Open a supported browser and go to the Government Cloud Console URL.
   b. Enter your Cloud Tenant and click Continue.
   c. On the Single Sign-On pane, select your identity provider and click Continue. You will be redirected to your identity provider to sign in.
   d. Enter your user name and password.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. The list of users is displayed.
3. On the User Type filter, select only Local Users.
4. For each local user, go to the the Actions icon (three dots) and click Delete.

**Using a Common Access Card/Personal Identity Verification Card to Sign in to the Console**

After you set up CAC/PIV authentication with your identity provider and successfully federate with Oracle Cloud Infrastructure, you can use your CAC/PIV credentials to sign in to the Oracle Cloud Infrastructure Console. See your identity provider's documentation for the specific details for your implementation.

In general, the sign in steps are:

1. Insert your CAC/PIV card into your card reader.
2. Navigate to the Oracle Cloud Infrastructure Console sign in page.
3. If prompted, enter your Cloud Tenant name and click Continue.
4. Select the Single Sign-On provider and click Continue.
5. On your identity provider's sign on page, select the appropriate card, for example, PIV Card.
6. If presented with a certificate picker, choose the appropriate certificate or other attributes set up by your organization.
7. When prompted, enter the PIN.

**IPv6 Support for Virtual Cloud Networks**

US Government Cloud customers have the option to enable IPv6 addressing for their VCNs. For more information, see IPv6 Addresses on page 2889.

**Setting Up Secure Access for Compute Hosts**

You can set up CAC/PIV authentication using third-party tools to enable multi-factor authentication for securely connecting to your compute hosts. Example tools include PuTTY-CAC for Windows and Open SC for macOS. For more information see the U.S. Government website, PIV Usage Guidelines.

**Enabling FIPS Mode for Your Operating System**

Government Cloud customers are responsible for enabling FIPS mode for the operating systems on their Compute hosts. To make your operating system compliant with Federal Information Processing Standard (FIPS) Publication 140-2, follow the guidelines for your operating system:

**Oracle Linux**

Follow the guidance provided at Enabling FIPS Mode on Oracle Linux.
**Ubuntu**

Follow the guidance provided at [Ubuntu Security Certifications](#).

**Windows Server 2012**

Follow the guidance provided at [Data Encryption for Web console and Reporting server Connections](#).

**Windows Server 2016 and Windows Server 2019**

First, follow the guidance provided at [How to Use FIPS Compliant Algorithms](#).

Next, go to the Microsoft document, [FIPS 140 Validation](#) and navigate to the topic [Information for System Integrators](#). Follow the instructions under "Step 2 – Setting FIPS Local/Group Security Policy Flag" to complete the FIPS enablement.

**CentOS**

The following guidance is for enabling FIPS on CentOS 7.5. These procedures are valid for both VM and bare metal instances, and only in NATIVE mode. These procedures can be modified for both Emulated and PV modes as needed. Note that this procedure provides an instance that contains the exact FIPS cryptographic modules EXCEPT kernel. However, the kernel module is the same major/minor version but is accelerated in revision, so can be considered compliant under most FIPS compliant models.

After you complete this procedure, Oracle strongly recommends that you do NOT run system-wide yum updates. The system-wide update will remove the FIPS modules contained herein.

**Verify that the version of the kernel, FIPS modules, and FIPS software are at the minimum version:**

1. Validate the current version of the kernel package meets the requirement:
   a. **Current version:** `kernel-3.10.0-693.el7`
   b. Execute `rpm -qa | grep kernel-3`

2. Execute the following and validate the major or minor version is the same as the requirements.
   a. Run
      
      ```
      yum list <package_name>
      ```
   b. Verify that the major/minor version matches the required ones.

      Required packages and versions are:
      - `fipscheck - fipscheck-1.4.1-6.el7`
      - `hmaccalc - hmaccalc-0.9.13-4.el7`
      - `dracut-fips - dracut-fips-033-502.el7`
      - `dracut-fips-aesni - dracut-fips-aesni-033-502.el7`
   c. For each version of package that is not installed, run
      
      ```
      yum install <package_name>
      ```
3. Download and install the following packages:

   a. Packages already installed as part of the image:
      1. Create a directory called `preinstall`.
      2. Download the following packages into this directory:
         openssl, openssl-libs – 1.0.2k-8.el7
         nss, nss-tools, nss-sysinit – 3.28.4-15.el7_4
         nss-util – 3.28.4-3.el7
         nss-softokn, nss-softokn-freebl – 3.28.3-8.el7_4
         openssh, openssh-clients, openssh-server – 7.4p1-11.el7
      3. In the preinstall directory, run
         
         ```
         yum -nogpgcheck downgrade *.rpm
         ```
   
   b. Packages to be added to the image:
      1. Create a directory called `newpackages`.
      2. Download the following packages into this directory:
         libreswan – 3.20-3.el7
         libgcrypt – 1.5.3-14.el7
         gnutls – 3.3.26-9.el7
         gmp – 6.0.0-15.el7
         nettle – 2.7.1-8.el7
      3. In the `newpackages` directory, run
         
         ```
         yum -nogpgcheck localinstall *.rpm
         ```

The URLs for the packages used for this installation are:

**Preinstall:**

- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nss-3.28.4-15.el7_4.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nss-util-3.28.4-3.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nss-tools-3.28.4-15.el7_4.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nss-sysinit-3.28.4-15.el7_4.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nss-softokn-freebl-3.28.3-8.el7_4.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nss-softokn-3.28.3-8.el7_4.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/openssl-1.0.2k-8.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/openssl-libs-1.0.2k-8.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/openssh-7.4p1-11.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/openssh-clients-7.4p1-11.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/openssh-server-7.4p1-11.el7.x86_64.rpm

**Newpackages:**

- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/libreswan-3.20-3.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/libgcrypt-1.5.3-14.el7.x86_64.rpm
- http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/gnutls-3.3.26-9.el7.x86_64.rpm
http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/gmp-6.0.0-15.el7.x86_64.rpm
http://linuxsoft.cern.ch/cern/centos/7/updates/x86_64/Packages/nettle-2.7.1-8.el7.x86_64.rpm

**Kernel FIPS module and initramfs validation installation.**

Perform this procedure as root:

1. Regenerate dracut:
   
   ```
   dracut -f -v
   ```

2. Add the fips argument to the end of the default kernel boot command line:
   
   a. Edit `/etc/default/grub`
   
   b. At the end of the line starting with “GRUB_CMDLINE_LINUX”, add
   
   ```
   fips=1
   ```

   inside the double quotes of the command.
   
   c. Save the result.

3. Generate a new `grub.cfg`:
   
   ```
   grub2-mkconfig -o /etc/grub2-efi.cfg
   ```

**Configure SSH to limit the encryption algorithms.**

1. Sudo to root.
2. Edit `/etc/ssh/sshd_config`.
3. Add the following lines to the bottom of the file:
   
   ```
   Protocol 2
   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
   Macs hmac-sha1
   ```

4. Reboot the instance.
5. After instance has rebooted, validate that FIPS mode has been enabled in the kernel:
   
   a. Sudo to root.
   
   b. Run the following command:

   ```
   cat /proc/sys/crypto/fips-enabled
   ```

   The result should be '1'.

To further secure CentOS7/RHEL 7.x systems as required by individual agency guidance, follow the checklist contained in the OpenSCAP guide. This guide can be found here: [https://static.open-scap.org/ssg-guides/ssg-centos7-guide-index.html](https://static.open-scap.org/ssg-guides/ssg-centos7-guide-index.html)

The STIG for evaluating compliance under multiple profiles can be found here: [https://iase.disa.mil/stigs/os/unix-linux/Pages/index.aspx](https://iase.disa.mil/stigs/os/unix-linux/Pages/index.aspx). Use the Red Hat Linux 7.x STIG for CentOS 7.5 releases.

**Required VPN Connect Parameters for Government Cloud**

If you use **VPN Connect** with the Government Cloud, you must configure the IPSec connection with the following FIPS-compliant IPSec parameters.

For some parameters, Oracle supports multiple values, and the recommended one is highlighted in **bold text**.
Oracle supports the following parameters for IKEv1 or IKEv2. Check the documentation for your particular CPE to confirm which parameters the CPE supports for IKEv1 or IKEv2.

### Phase 1 (ISAKMP)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAKMP protocol</td>
<td>Version 1</td>
</tr>
<tr>
<td>Exchange type</td>
<td>Main mode</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Pre-shared keys *</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>AES-256-cbc (recommended)</td>
</tr>
<tr>
<td></td>
<td>AES-192-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-128-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>SHA-2 384 (recommended)</td>
</tr>
<tr>
<td></td>
<td>SHA-2 256</td>
</tr>
<tr>
<td></td>
<td>SHA-1 (also called SHA or SHA1-96)</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>group 14 (MODP 2048)</td>
</tr>
<tr>
<td></td>
<td>group 19 (ECP 256)</td>
</tr>
<tr>
<td></td>
<td><strong>group 20 (ECP 384)</strong> (recommended)</td>
</tr>
<tr>
<td>IKE session key lifetime</td>
<td>28800 seconds (8 hours)</td>
</tr>
</tbody>
</table>

* Only numbers, letters, and spaces are allowed characters in pre-shared keys.

### Phase 2 (IPSec)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec protocol</td>
<td>ESP, tunnel mode</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td><strong>AES-256-gcm</strong> (recommended)</td>
</tr>
<tr>
<td></td>
<td>AES-192-gcm</td>
</tr>
<tr>
<td></td>
<td>AES-128-gcm</td>
</tr>
<tr>
<td></td>
<td>AES-256-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-192-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-128-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>If using GCM (Galois/Counter Mode), no authentication algorithm is required because authentication is included with GCM encryption.</td>
</tr>
<tr>
<td></td>
<td>If not using GCM, use HMAC-SHA-256-128.</td>
</tr>
<tr>
<td>IPSec session key lifetime</td>
<td>3600 seconds (1 hour)</td>
</tr>
</tbody>
</table>
Parameter | Options
---|---
Perfect Forward Secrecy (PFS) | enabled, group 14

**Oracle’s BGP ASN**

This section is for network engineers who configure an edge device for FastConnect or VPN Connect.

Oracle’s BGP ASN for the Government Cloud depends on the authorization level:

- US Government Cloud: 6142
- US Federal Cloud (Impact Level 5 authorization): 20054

**FIPS Compatible Terraform Provider**

To use Terraform in US Government Cloud regions, refer to Enabling FIPS Compatibility on page 4284 for installation and configuration information.

**Requesting a Service Limit Increase for Government Cloud Tenancies**

If you need to request a service limit increase, use the following instructions to create a service request in My Oracle Support.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Before you can create a service request, you must have an oracle.com account and you must register your Oracle Cloud Infrastructure CSI with My Oracle Support. See Requesting a Service Limit Increase for Government Cloud Tenancies on page 154 for details.</td>
</tr>
<tr>
<td>• Be aware that the support engineer that reviews the information in the service limit request might not be a U.S. citizen.</td>
</tr>
</tbody>
</table>

**Creating a Service Request**

To create a service request for Oracle Government Cloud:

1. Go to My Oracle Support and log in.
   - If you are not signed in to Oracle Cloud Support, click Switch to Cloud Support at the top of the page.
2. At the top of the page, click Service Requests.
3. Click Create Technical SR.
4. Select the following from the displayed menus:
   - **Service Type:** Select Oracle Cloud Infrastructure from the list.
   - **Service Name:** Select the appropriate option for your organization.
   - **Problem Type:** Select Account Provisioning, Billing and Termination, and then select Limit Increase from the submenu.
5. Enter your contact information.
6. Enter a Description, and then enter the required fields specific to your issue. If a field does not apply, you can enter n/a.

For help with any of the general fields in the service request or for information on managing your service requests, click Help at the top of the Oracle Cloud Support page.

**Locating Oracle Cloud Infrastructure IDs**

Use the following tips to help you locate identifiers you might be asked to provide:

**Finding Your tenancy OCID (Oracle Cloud Identifier)**
Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the Tenancy Details page:

1. Open the Profile menu (≡) and click Tenancy: <your_tenancy_name>.
2. The tenancy OCID is shown under Tenancy Information. Click Copy to copy it to your clipboard.

Finding the OCID of a Compartment

To find the OCID (Oracle Cloud Identifier) of a compartment:

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
   A list of the compartments in your tenancy is displayed.
   A shortened version of the OCID is displayed next to each compartment.

2. Click Copy to copy the OCID to your clipboard. You can then paste it into the service request form field.

Finding the OCID of a Resource

The OCID (Oracle Cloud Identifier) of a resource is displayed when you view the resource in the Console, both in the list view and on the details page.

For example, to get the OCID for a compute instance:

1. Open the Console.
2. Select the Compartment to which the instance belongs from the list on the left side of the page.
   Note that you must have appropriate permissions in a compartment to view resources.
3. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances. A list of instances in the selected compartment is displayed.
4. A shortened version of the OCID is displayed on the instance details page.
5. Click Copy to copy the OCID to your clipboard. You can then paste it into the service request form field.
Finding Your Customer Service Identifier (CSI)

The Customer Support Identifier (CSI) number is generated after you purchase Oracle Cloud services. This number can be found in several places, including in your contract document and also on your tenancy details page. You’ll need the CSI number to register and log support requests in My Oracle Support (MOS).

To find your CSI number:

1. Open the Profile menu (_profile) and click Tenancy: <your_tenancy_name>.
2. The CSI number is shown under Tenancy Information.

Using My Oracle Support for the First Time

Before you can create service requests with My Oracle Support, you need to have an Oracle Single Sign On (SSO) account and you need to register your Customer Support Identifier (CSI) with My Oracle Support.

**Tip:** Before you begin this procedure, have your CSI handy (see Requesting a Service Limit Increase for Government Cloud Tenancies on page 154).

To request an SSO account and register with My Oracle Support

1. Go to [https://support.oracle.com](https://support.oracle.com).
2. Click New user? Register here to create your Oracle Single Sign On (SSO) account.
3. Enter your company e-mail address in the Email address field, complete the rest of the form, and then click Create Account. A verification email is generated.
4. Check your email account for an email from Oracle asking you to verify your email address.
5. Open the email and click Verify Email Address.
6. Sign in with the credentials you just set up.
7. At sign in, you are prompted to enter a Note to the Approver and the Support Identifier (your CSI).
8. Click Request Access.
9. Enter the first five characters of the name of the organization that owns the Customer Support Identifier (listed in the Welcome letter and on My Services), and then click Validate. The support identifier appears in the table.
10. Click Next.
11. Enter your contact information and click Next.
12. Accept the terms and click Next.

The status of the request is pending until you receive approval from the Customer User Administrator (CUA) or from Oracle Support if you are the first person requesting this support identifier.
If you have previously registered, but need to add the CSI for Oracle Cloud Infrastructure

1. Go to https://support.oracle.com and log in.
2. Navigate to the My Account page: Go to your user name at the of the page, open the menu, and then click My Account.
3. The Support Identifiers region displays the accounts that your user name is currently associated with.
4. Click Request Access.
5. Enter a Note to the Approver and then enter the Support Identifier (your CSI).
6. Click Request Access.
7. Enter the first five characters of the name of the organization that owns the Customer Support Identifier (listed in the Welcome letter and on My Services), and then click Validate. The support identifier appears in the table.
8. Click Validate.
9. The entry is validated. Close the dialog.

The status of the request is pending until you receive approval from the Customer User Administrator (CUA).

For more information about signing in and using My Oracle Support, see Registration, Sign In, and Accessibility Options in My Oracle Support Help.

Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization

This topic contains information specific to Oracle Cloud Infrastructure US Government Cloud with FedRAMP High Joint Authorization Board.

Authorizations

Oracle Cloud Infrastructure US Government Cloud has obtained the following authorizations:

- FedRAMP High
- DISA Impact Level 4

For information about the US Government Cloud, see For All US Government Cloud Customers on page 148.

Regions

The region names and identifiers for the US Government Cloud with FedRAMP High Joint Authorization Board are shown in the following table:

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region Identifier</th>
<th>Region Location</th>
<th>Region Key</th>
<th>Realm Key</th>
<th>Availability Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Gov East (Ashburn)</td>
<td>us-langley-1</td>
<td>Ashburn, VA</td>
<td>LFI</td>
<td>OC2</td>
<td>1</td>
</tr>
<tr>
<td>US Gov West (Phoenix)</td>
<td>us-luke-1</td>
<td>Phoenix, AZ</td>
<td>LUF</td>
<td>OC2</td>
<td>1</td>
</tr>
</tbody>
</table>

After your tenancy is created in one of these regions, you can subscribe to the other region. Tenancies in the FedRAMP-authorized regions cannot subscribe to the commercial regions, or to the US Federal Cloud regions. For information about subscribing to a region, see Managing Regions on page 2445.

Console Sign-in URLs

To sign in to the FedRAMP-authorized US Government Cloud, enter one of the following URLs in a supported browser:

- https://console.us-langley-1.oraclegovcloud.com/
- https://console.us-luke-1.oraclegovcloud.com/
US Government Cloud with FedRAMP Authorization API Reference and Endpoints

US Government Cloud with FedRAMP High Joint Authorization Board has these APIs and corresponding regional endpoints:

Announcements API

API reference

- https://announcements.us-langley-1.oraclegovcloud.com
- https://announcements.us-luke-1.oraclegovcloud.com

Autoscaling API

API reference

- https://autoscaling.us-langley-1.oci.oraclegovcloud.com
- https://autoscaling.us-luke-1.oci.oraclegovcloud.com

Core Services (covering Networking, Compute, and Block Volume)

The Networking, Compute, and Block Volume services are accessible with the following API:

Core Services API

API reference

- https://iaas.us-langley-1.oraclegovcloud.com
- https://iaas.us-luke-1.oraclegovcloud.com

Container Engine for Kubernetes API

API reference

- https://containerengine.us-langley-1.oci.oraclegovcloud.com
- https://containerengine.us-luke-1.oci.oraclegovcloud.com

Database API

API reference

- https://database.us-langley-1.oraclegovcloud.com
- https://database.us-luke-1.oraclegovcloud.com

You can track the progress of long-running Database operations with the Work Requests API.

Digital Assistant API

API reference

- https://digitalassistant.us-langley-1.oci.oraclegovcloud.com
- https://digitalassistant.us-luke-1.oci.oraclegovcloud.com

Email Delivery API

API reference

- https://ctrl.email.us-langley-1.oci.oraclegovcloud.com
- https://ctrl.email.us-luke-1.oci.oraclegovcloud.com

Events API

API reference
Note:

Use the Endpoint of Your Home Region for All IAM API Calls

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your home region. Your home region is where your IAM resources are defined. When you subscribe to a new region, your IAM resources are replicated in the new region, however, the master definitions reside in your home region and can only be changed there. Make all IAM API calls against your home region endpoint. The changes automatically replicate to all regions. If you try to make an IAM API call against a region that is not your home region, you will receive an error.

Key Management API (for the Vault service)

API reference

- https://kms.us-langley-1.oracle.govcloud.com
- https://kms.us-luke-1.oracle.govcloud.com

In addition to these endpoints, each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint.

Events API

API reference

- https://events.us-langley-1.oracle.govcloud.com
- https://events.us-luke-1.oracle.govcloud.com

Marketplace Service API

API reference

- https://marketplace.us-langley-1.oracle.govcloud.com
- https://marketplace.us-luke-1.oracle.govcloud.com

Monitoring API

API reference

- https://telemetry-ingestion.us-langley-1.oracle.govcloud.com
- https://telemetry-ingestion.us-luke-1.oracle.govcloud.com
- https://telemetry.us-langley-1.oracle.govcloud.com
- https://telemetry.us-luke-1.oracle.govcloud.com

Notifications API

API reference
The source service must be available in US Government Cloud regions for messages to be successfully sent through the Notifications service. If the source service is not available in these regions, then the message is not sent. For a list of unavailable services, see Services Not Supported in US Government Cloud with FedRAMP Authorization on page 161.

**Object Storage and Archive Storage APIs**

Both Object Storage and Archive Storage are accessible with the following APIs:

**Object Storage API**

API reference

- https://objectstorage.us-langley-1.oraclegovcloud.com
- https://objectstorage.us-luke-1.oraclegovcloud.com

**Amazon S3 Compatibility API**

API reference

- https://<object_storage_namespace>.compat.objectstorage.us-langley-1.oraclegovcloud.com
- https://<object_storage_namespace>.compat.objectstorage.us-luke-1.oraclegovcloud.com

**Swift API (for use with Oracle RMAN)**

- https://swiftobjectstorage.us-langley-1.oraclegovcloud.com
- https://swiftobjectstorage.us-luke-1.oraclegovcloud.com

**Oracle Cloud VMware Solution API**

API reference

- https://ocvps.us-langley-1.oci.oraclegovcloud.com
- https://ocvps.us-luke-1.oci.oraclegovcloud.com

**Registry**

- US Gov East (Ashburn)
  - ocir.us-langley-1.oci.oraclegovcloud.com
- US Gov West (Phoenix)
  - ocir.us-luke-1.oci.oraclegovcloud.com

**Resource Manager API**

API reference

- https://resourcemanager.us-langley-1.oci.oraclegovcloud.com
- https://resourcemanager.us-luke-1.oci.oraclegovcloud.com

**Streaming API**

API reference

- https://streaming.us-langley-1.oraclegovcloud.com
- https://streaming.us-luke-1.oraclegovcloud.com

| Tip: |
| See Understanding Object Storage Namespaces on page 3395 for information regarding how to find your Object Storage namespace. |
**Work Requests API (for Compute and Database work requests)**

API reference

- https://iaas.us-langley-1.oraclegovcloud.com
- https://iaas.us-luke-1.oraclegovcloud.com

**Oracle YUM Repo Endpoints**

The Oracle YUM repo regional endpoints for US Government Cloud with FedRAMP High Joint Authorization Board are shown in the following table:

<table>
<thead>
<tr>
<th>Region</th>
<th>YUM Server Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Gov East (Ashburn)</td>
<td>• <a href="https://yum.us-langley-1.oci.oraclegovcloud.com">https://yum.us-langley-1.oci.oraclegovcloud.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://yum-us-langley-1.oracle.com">https://yum-us-langley-1.oracle.com</a></td>
</tr>
<tr>
<td>US Gov West (Phoenix)</td>
<td>• <a href="https://yum-us-luke-1.oci.oraclegovcloud.com">https://yum-us-luke-1.oci.oraclegovcloud.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://yum-us-luke-1.oracle.com">https://yum-us-luke-1.oracle.com</a></td>
</tr>
</tbody>
</table>

**SMTP Authentication and Connection Endpoints**

Email Delivery only supports the AUTH PLAIN command when using SMTP authentication. If the sending application is not flexible with the AUTH command, an SMTP proxy/relay can be used. For more information about the AUTH command, see AUTH Command and its Mechanisms.

<table>
<thead>
<tr>
<th>Region</th>
<th>SMTP Connection Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Gov East (Ashburn)</td>
<td>smtp.email.us-langley-1.oci.oraclegovcloud.com</td>
</tr>
<tr>
<td>US Gov West (Phoenix)</td>
<td>smtp.email.us-luke-1.oci.oraclegovcloud.com</td>
</tr>
</tbody>
</table>

**SPF Record Syntax**

An SPF record is a TXT record on your sending domain that authorizes Email Delivery IP addresses to send on your behalf. SPF is required for subdomains of oraclegovcloud.com and recommended in other cases. The SPF record syntax for each sending region is shown in the following table:

<table>
<thead>
<tr>
<th>Realm Key</th>
<th>SPF Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC2</td>
<td>v=spf1 include:rp.email.oci.oraclegovcloud.com ~all</td>
</tr>
</tbody>
</table>

The Realm Key is applicable for any sending regions in that realm.

**Services Not Supported in US Government Cloud with FedRAMP Authorization**

The following services are currently not available or not supported for tenancies in the US Government Cloud with FedRAMP High Joint Authorization Board.

Database services not available:

- Autonomous Data Warehouse
- Autonomous Transaction Processing
- Data Safe

Solutions and Platform services not available:

- Analytics Cloud
- Fusion Analytics Warehouse
• Application Migration
• Compliance Documents
• Content and Experience
• DNS Zone Management
• Functions
• Health Checks
• Integration
• Traffic Management Steering Policies

Governance and Administration features not supported:
• Auto-federation with Oracle Identity Cloud Service
• WAF service

Integration with Oracle SaaS and PaaS services, including those listed here: Getting Started with Oracle Platform Services on page 119

**Additional Information for US Government Cloud with FedRAMP Authorization Customers**

• Shared Responsibilities on page 148
• Setting Up an Identity Provider for Your Tenancy on page 148
• Using a Common Access Card/Personal Identity Verification Card to Sign in to the Console on page 149
• IPv6 Support for Virtual Cloud Networks on page 149
• Setting Up Secure Access for Compute Hosts on page 149
• Enabling FIPS Mode for Your Operating System on page 149
• Required VPN Connect Parameters for Government Cloud on page 152
• Oracle's BGP ASN on page 154
• Requesting a Service Limit Increase for Government Cloud Tenancies on page 154

**Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization**

This topic contains information specific to Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 authorization.

**Note:**

DISA Impact Level 5 authorization is in process for the following services:

• Cloud Shell
• Data Transfer service
• Email Delivery service
• Oracle Cloud VMware Solution

FedRAMP High Joint Authorization Board accreditation for these services is complete.

**Compliance with Defense Cloud Security Requirements**

US Federal Cloud with DISA Impact Level 5 authorization supports applications that require Impact Level 5 (IL5) data, as defined in the Department of Defense Cloud Computing Security Requirements Guide (SRG).

**US Federal Cloud with DISA Impact Level 5 Authorization Regions**

The region names and identifiers for the US Federal Cloud with DISA Impact Level 5 authorization regions are shown in the following table:
After your tenancy is created in one of the US Federal Cloud with DISA Impact Level 5 authorization regions, you can subscribe to the other regions in the US Federal Cloud with DISA Impact Level 5 authorization. These tenancies cannot subscribe to any Oracle Cloud Infrastructure regions not belonging to the OC3 realm. For information about subscribing to a region, see Managing Regions on page 2445.

US Federal Cloud with DISA Impact Level 5 Authorization Console Sign-in URLs

To sign in to the US Federal Cloud with DISA Impact Level 5 authorization, enter one of the following URLs in a supported browser:

- https://console.us-gov-ashburn-1.oraclegovcloud.com/
- https://console.us-gov-chicago-1.oraclegovcloud.com/
- https://console.us-gov-phoenix-1.oraclegovcloud.com/

Note:
When you're logged in to the Console for one of the US Federal Government Cloud regions, the browser times out after 15 minutes of inactivity, and you need to sign in again to use the Console.

US Federal Cloud with DISA Impact Level 5 Authorization API Reference and Endpoints

This section includes the APIs and corresponding regional endpoints with US Federal Cloud DISA Impact Level 5 authorization.

Announcements API

API reference

- https://announcements.us-gov-ashburn-1.oraclegovcloud.com
- https://announcements.us-gov-chicago-1.oraclegovcloud.com
- https://announcements.us-gov-phoenix-1.oraclegovcloud.com

Autoscaling API

API reference

- https://autoscaling.us-gov-ashburn-1.oci.oraclegovcloud.com
- https://autoscaling.us-gov-chicago-1.oci.oraclegovcloud.com
- https://autoscaling.us-gov-phoenix-1.oci.oraclegovcloud.com

Core Services (covering Networking, Compute, and Block Volume)

The Networking, Compute, and Block Volume services are accessible with the following API:

Core Services API

API reference

- https://iaas.us-gov-ashburn-1.oraclegovcloud.com
- https://iaas.us-gov-chicago-1.oraclegovcloud.com
- https://iaas.us-gov-phoenix-1.oraclegovcloud.com

**Container Engine for Kubernetes API**

API reference

- https://containerengine.us-gov-ashburn-1.oci.oraclegovcloud.com
- https://containerengine.us-gov-chicago-1.oci.oraclegovcloud.com
- https://containerengine.us-gov-phoenix-1.oci.oraclegovcloud.com

**Database API**

API reference

- https://database.us-gov-ashburn-1.oraclegovcloud.com
- https://database.us-gov-chicago-1.oraclegovcloud.com
- https://database.us-gov-phoenix-1.oraclegovcloud.com

You can track the progress of long-running Database operations with the [Work Requests API](https://iaas.us-gov-chicago-1.oraclegovcloud.com).

**Digital Assistant API**

API reference

- https://digitalassistant.us-gov-ashburn-1.oci.oraclegovcloud.com
- https://digitalassistant.us-gov-chicago-1.oci.oraclegovcloud.com
- https://digitalassistant.us-gov-phoenix-1.oci.oraclegovcloud.com

**Email Delivery API**

API reference

- https://ctrl.email.us-gov-ashburn-1.oci.oraclegovcloud.com
- https://ctrl.email.us-gov-chicago-1.oci.oraclegovcloud.com
- https://ctrl.email.us-gov-phoenix-1.oci.oraclegovcloud.com

**Events API**

API reference

- https://events.us-gov-ashburn-1.oci.oraclegovcloud.com
- https://events.us-gov-chicago-1.oci.oraclegovcloud.com
- https://events.us-gov-phoenix-1.oci.oraclegovcloud.com

**File Storage API**

API reference

- https://filestorage.us-gov-ashburn-1.oraclegovcloud.com
- https://filestorage.us-gov-chicago-1.oraclegovcloud.com
- https://filestorage.us-gov-phoenix-1.oraclegovcloud.com

**IAM API**

API reference

- https://identity.us-gov-ashburn-1.oraclegovcloud.com
- https://identity.us-gov-chicago-1.oraclegovcloud.com
- https://identity.us-gov-phoenix-1.oraclegovcloud.com

**Note:**

Use the Endpoint of Your Home Region for All IAM API Calls
When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your home region. Your home region is where your IAM resources are defined. When you subscribe to a new region, your IAM resources are replicated in the new region, however, the master definitions reside in your home region and can only be changed there. Make all IAM API calls against your home region endpoint. The changes automatically replicate to all regions. If you try to make an IAM API call against a region that is not your home region, you will receive an error.

Key Management API (for the Vault service)

API reference
- https://kms.us-gov-ashburn-1.oraclegovcloud.com
- https://kms.us-gov-chicago-1.oraclegovcloud.com
- https://kms.us-gov-phoenix-1.oraclegovcloud.com

In addition to these endpoints, each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint.

Marketplace Service API

API reference

Monitoring API

API reference
- https://telemetry-ingestion.us-gov-ashburn-1.oraclegovcloud.com
- https://telemetry-ingestion.us-gov-chicago-1.oraclegovcloud.com
- https://telemetry-ingestion.us-gov-phoenix-1.oraclegovcloud.com
- https://telemetry.us-gov-ashburn-1.oraclegovcloud.com
- https://telemetry.us-gov-chicago-1.oraclegovcloud.com
- https://telemetry.us-gov-phoenix-1.oraclegovcloud.com

Notifications API

API reference
- https://notification.us-gov-ashburn-1.oraclegovcloud.com
- https://notification.us-gov-chicago-1.oraclegovcloud.com
- https://notification.us-gov-phoenix-1.oraclegovcloud.com

The source service must be available in US Government Cloud regions for messages to be successfully sent through the Notifications service. If the source service is not available in these regions, then the message is not sent. For a list of unavailable services, see Services Not Supported in US Federal Cloud with DISA Impact Level 5 Authorization on page 167.

Object Storage and Archive Storage APIs

Both Object Storage and Archive Storage are accessible with the following APIs:

Object Storage API

API reference
- https://objectstorage.us-gov-ashburn-1.oraclegovcloud.com
- https://objectstorage.us-gov-chicago-1.oraclegovcloud.com
- https://objectstorage.us-gov-phoenix-1.oraclegovcloud.com
Amazon S3 Compatibility API

API reference
- https://<object_storage_namespace>.compat.objectstorage.us-gov-ashburn-1.oraclegovcloud.com
- https://<object_storage_namespace>.compat.objectstorage.us-gov-chicago-1.oraclegovcloud.com
- https://<object_storage_namespace>.compat.objectstorage.us-gov-phoenix-1.oraclegovcloud.com

Tip:
See Understanding Object Storage Namespaces on page 3395 for information regarding how to find your Object Storage namespace.

Swift API (for use with Oracle RMAN)

- https://swiftobjectstorage.us-gov-ashburn-1.oraclegovcloud.com
- https://swiftobjectstorage.us-gov-chicago-1.oraclegovcloud.com
- https://swiftobjectstorage.us-gov-phoenix-1.oraclegovcloud.com

Oracle Cloud VMware Solution API

API reference
- https://ocvps.us-ashburn-1.oci.oraclegovcloud.com
- https://ocvps.us-chicago-1.oci.oraclegovcloud.com
- https://ocvps.us-phoenix-1.oci.oraclegovcloud.com

Registry

Registry
- US DoD East (Ashburn)
  - ocir.us-gov-ashburn-1.oci.oraclegovcloud.com
- US DoD North (Chicago)
  - ocir.us-gov-chicago-1.oci.oraclegovcloud.com
- US DoD North (Chicago)
  - ocir.us-gov-phoenix-1.oci.oraclegovcloud.com

Resource Manager API

API reference
- https://resourcemanager.us-ashburn-1.oci.oraclegovcloud.com
- https://resourcemanager.us-chicago-1.oci.oraclegovcloud.com
- https://resourcemanager.us-phoenix-1.oci.oraclegovcloud.com

Streaming API

API reference
- https://streaming.us-gov-ashburn-1.oraclegovcloud.com
- https://streaming.us-gov-chicago-1.oraclegovcloud.com
- https://streaming.us-gov-phoenix-1.oraclegovcloud.com

Work Requests API (for Compute and Database work requests)

API reference
- https://iaas.us-gov-ashburn-1.oraclegovcloud.com
- https://iaas.us-gov-chicago-1.oraclegovcloud.com
- https://iaas.us-gov-phoenix-1.oraclegovcloud.com
Oracle YUM Repo Endpoints

The Oracle YUM repo regional endpoints for US Federal Cloud with DISA Impact Level 5 authorization are shown in the following table:

<table>
<thead>
<tr>
<th>Region</th>
<th>YUM Server Endpoint</th>
</tr>
</thead>
</table>
| US DoD East (Ashburn)       | • https://yum.us-gov-ashburn-1.oci.oraclegovcloud.com  
                                • https://yum-us-gov-ashburn-1.oracle.com                                       |
| US DoD North (Chicago)      | • https://yum.us-gov-chicago-1.oci.oraclegovcloud.com  
                                • https://yum-us-gov-chicago-1.oracle.com                                          |
| US DoD West (Phoenix)       | • https://yum.us-gov-phoenix-1.oci.oraclegovcloud.com  
                                • https://yum-us-gov-phoenix-1.oracle.com                                           |

SMTP Authentication and Connection Endpoints

Email Delivery only supports the AUTH PLAIN command when using SMTP authentication. If the sending application is not flexible with the AUTH command, an SMTP proxy/relay can be used. For more information about the AUTH command, see AUTH Command and its Mechanisms.

<table>
<thead>
<tr>
<th>Region</th>
<th>SMTP Connection Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>US DoD East (Ashburn)</td>
<td>smtp.email.us-gov-ashburn-1.oci.oraclegovcloud.com</td>
</tr>
<tr>
<td>US DoD North (Chicago)</td>
<td>smtp.email.us-gov-chicago-1.oci.oraclegovcloud.com</td>
</tr>
<tr>
<td>US DoD West (Phoenix)</td>
<td>smtp.email.us-gov-phoenix-1.oci.oraclegovcloud.com</td>
</tr>
</tbody>
</table>

SPF Record Syntax

An SPF record is a TXT record on your sending domain that authorizes Email Delivery IP addresses to send on your behalf. SPF is required for subdomains of oraclegovcloud.com and recommended in other cases. The SPF record syntax for each sending region is shown in the following table:

<table>
<thead>
<tr>
<th>Realm Key</th>
<th>SPF Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC3</td>
<td>v=spf1 include:rp.email.oci.oraclegovcloud.com ~all</td>
</tr>
</tbody>
</table>

The Realm Key is applicable for any sending regions in that realm.

Services Not Supported in US Federal Cloud with DISA Impact Level 5 Authorization

Currently, the following services are not available or not supported for tenancies in the US Federal Cloud with DISA Impact Level 5 authorization.

Core Infrastructure services and features not available:
  • FastConnect with a provider (FastConnect in a colocation model is supported)
  • Data Transfer service

Database services not available:
  • Autonomous Data Warehouse
Oracle Cloud Infrastructure Government Cloud

- Autonomous Transaction Processing
- Data Safe

Solutions and Platform services not available:
- Analytics Cloud
- Fusion Analytics Warehouse
- Application Migration
- Compliance Documents
- Content and Experience
- DNS Zone Management
- Email Delivery
- Functions
- Health Checks
- Integration
- Traffic Management Steering Policies

Governance and Administration features not supported:
- Auto-federation with Oracle Identity Cloud Service
- WAF service

Integration with Oracle SaaS and PaaS services, including those listed here: Getting Started with Oracle Platform Services on page 119.

**Access to Multiple US Federal Cloud with DISA Impact Level 5 Authorization Regions**

This section shows how to give the on-premises resources that are part of NIPRNet access to multiple US Federal Cloud regions over a single FastConnect connection. This is important if one of the regions does not have a direct connection to the NIPRNet's *border cloud access point* (BCAP). The BCAP is also referred to as the *meet me point*.

**Overview**

Some US Federal Cloud regions have a direct connection to a NIPRNet BCAP, but others do not. You can use the Networking service to give on-premises resources that are part of NIPRNet access to a US Federal Cloud region that is not directly connected to the NIPRNet's BCAP. You might do this to extend your on-premises workloads into a particular US Federal Cloud region that you're interested in, or to use that region for disaster recovery (DR).

This scenario is illustrated in the following diagram.
In the diagram, US Federal Government Cloud region 1 has a direct connection to the NIPRNet's BCAP, but US Federal Government Cloud region 2 does not. Imagine that on-premises resources in NIPRNet (in subnet 172.16.1.0/24) need access to your virtual cloud network (VCN) in region 2 (with CIDR 10.0.3.0/24).

Optionally, there could also be a VCN with cloud resources in region 1 (with CIDR 10.0.1.0/24), but a VCN in region 1 is not required for this scenario. The intent of this scenario is for the on-premises resources to get access to resources in region 2.

In general, you set up two types of connections:

- **FastConnect** between the NIPRNet BCAP and region 1.
- **Remote peering connection** between region 1 and region 2.

Here are some details about the connections:

- That FastConnect has at least one physical connection, or cross-connect. You set up a private virtual circuit that runs on the FastConnect. The private virtual circuit enables communication that uses private IP addresses between the on-premises resources and the cloud resources.
- The remote peering connection is between a dynamic routing gateway (DRG) in region 1, and a DRG in region 2. A DRG is a virtual router that you typically attach to a VCN to give that VCN access to resources outside its Oracle region.
- You can control which on-premises subnets are advertised to the VCNs by configuring your BCAP edge router accordingly.
- The subnets in both VCN-1 and VCN-2 are advertised to your BCAP edge router over the FastConnect connection.
- You can optionally configure VCN security rules and other firewalls that you maintain to allow only certain types of traffic (such as SSH or SQL*NET) between the on-premises resources and VCNs.

Here are some basic requirements:

- The VCNs and DRGs in region 1 and region 2 must belong to the same tenancy, but they can be in different compartments within the tenancy.
- For accurate routing, the CIDR blocks of the on-premises subnets of interest and the VCNs must not overlap.
- To enable traffic to flow from a VCN to the on-premises subnets of interest, you must add a route rule to the VCN subnet route tables for each of the on-premises subnets. The preceding diagram shows the route rule for 172.16.1.0/24 in each VCN's route table.

**General Setup Process**
Task 1: Set up FastConnect to region 1

Summary: In this task, you set up the FastConnect between the NIPRNet BCAP and region 1. FastConnect has three connectivity models, and you generally follow the colocate with Oracle model. In this case, colocation occurs in the BCAP (the meet me point). The connection consists of both a physical connection (at least one cross-connect) and logical connection (private virtual circuit).

For instructions, follow the flow chart and tasks listed in Getting Started with FastConnect on page 3211, and notice these specific variations:

- In task 2, the instructions assume that you have a VCN (in region 1), but it is optional.
- In task 8, create a private virtual circuit (not a public one).

Task 2: Set up a VCN and DRG in region 2

Summary: If you don't yet have a VCN in region 2 (VCN-2 in the preceding diagram), you set it up in this task. You also create a DRG in region 2 and attach it to the VCN. Then, for each VCN-2 subnet that needs to communicate with the on-premises network, you update that subnet's route table to include a route rule for the on-premises subnet of interest. If there are multiple on-premises subnets that you want to route to, set up a route rule for each one.

For instructions, see these procedures:
1. To create a VCN on page 2825
2. To create a DRG on page 2929
3. To attach a DRG to a VCN on page 2930
4. To route a subnet's traffic to a DRG on page 2930

Important:

In step 4 in the preceding list, add a route rule with the following settings:
- Destination CIDR = the on-premises subnet of interest
- Target = the VCN's DRG

In the preceding diagram, it's the rule with 172.16.1.0/24 as the destination CIDR, and target as DRG-2. The second rule in the diagram (for 10.0.1.0/24 and DRG-2) is necessary only if resources in VCN-2 need to communicate with resources in VCN-1.

Task 3: Set up remote peering between region 1 and region 2

Summary: In this task, you set up a remote peering to enable private traffic between DRG-1 and DRG-2. The term remote peering typically means that resources in one VCN can communicate privately with resources in a VCN in a different region. In this case, the remote peering also enables private communication between the on-premises network and VCN-2.

For instructions, see Setting Up a Remote Peering on page 3284, and notice these important details:

- Optional region 1 VCN: The instructions assume that each region has a VCN, but in this situation, it is optional for region 1.
- Single VCN administrator: The instructions assume that there are two different VCN administrators: one for the VCN in region 1 and another for the VCN in region 2. In this situation, there might be only a single VCN administrator (you) who handles both regions and configures the remote peering connection.
- Unnecessary IAM policies: The instructions include a task for each VCN administrator to set up particular IAM policies to enable the remote peering connection. One policy is for the VCN administrator who is designated as the requestor, and one is for the VCN administrator who is designated as the acceptor. Those terms are further defined in Important Remote Peering Concepts on page 3282. However, if there's only a single VCN administrator with comprehensive networking permissions across the tenancy, those IAM policies are not necessary. For more information, read the tip that appears at the end of the task.
- RPC anchor points and connection: The remote peering actually consists of multiple components that you must set up. There's an anchor point on each DRG (shown as RPC-1 and RPC-2 in the preceding diagram), plus a
connection between those two RPC anchor points. The instructions include steps for creating those RPCs and the connection between them. Ensure that you create all the components.

**Additional Information for US Federal Cloud with DISA Impact Level 5 Authorization Customers**

- [Shared Responsibilities on page 148](#)
- [Setting Up an Identity Provider for Your Tenancy on page 148](#)
- [Using a Common Access Card/Personal Identity Verification Card to Sign in to the Console on page 149](#)
- [IPv6 Support for Virtual Cloud Networks on page 149](#)
- [Setting Up Secure Access for Compute Hosts on page 149](#)
- [Setting Up an Identity Provider for Your Tenancy on page 148](#)
- [Required VPN Connect Parameters for Government Cloud on page 152](#)
- [Oracle's BGP ASN on page 154](#)
- [Requesting a Service Limit Increase for Government Cloud Tenancies on page 154](#)

**Oracle Cloud Infrastructure United Kingdom Government Cloud**

This topic contains information specific to Oracle Cloud Infrastructure United Kingdom Government Cloud.

**Regions**

The region names and identifiers for the United Kingdom Government Cloud are shown in the following table:

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region Identifier</th>
<th>Region Location</th>
<th>Region Key</th>
<th>Realm Key</th>
<th>Availability Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Gov South (London)</td>
<td>uk-gov-london-1</td>
<td>London, United Kingdom</td>
<td>LTN</td>
<td>OC4</td>
<td>1</td>
</tr>
<tr>
<td>UK Gov West (Newport)</td>
<td>uk-gov-cardiff-1</td>
<td>Newport, United Kingdom</td>
<td>BRS</td>
<td>OC4</td>
<td>1</td>
</tr>
</tbody>
</table>

**Oracle's BGP ASN**

This section is for network engineers who configure an edge device for FastConnect or VPN Connect. Oracle's BGP autonomous system number (ASN) for the UK Government Cloud is 1218.

**Console Sign-in URLs**

To sign in to the United Kingdom Government Cloud, enter the following URL in a supported browser:

- [https://console.uk-gov-london-1.oraclegovcloud.uk/](https://console.uk-gov-london-1.oraclegovcloud.uk/)
- [https://console.uk-gov-cardiff-1.oraclegovcloud.uk/](https://console.uk-gov-cardiff-1.oraclegovcloud.uk/)

**API Reference and Endpoints**

Oracle Cloud Infrastructure United Kingdom Government Cloud has these APIs and corresponding regional endpoints:

**API Gateway API**

**API reference**

- [https://apigateway.uk-gov-london-1.oci.oraclegovcloud.uk](https://apigateway.uk-gov-london-1.oci.oraclegovcloud.uk)
- [https://apigateway.uk-gov-cardiff-1.oci.oraclegovcloud.uk](https://apigateway.uk-gov-cardiff-1.oci.oraclegovcloud.uk)
Analytics API

API reference

- https://analytics.uk-gov-london-1.oci.oraclegovcloud.uk
- https://analytics.uk-gov-cardiff-1.oci.oraclegovcloud.uk

Core Services (covering Networking, Compute, and Block Volume)

The Networking, Compute, and Block Volume services are accessible with the following API:

Core Services API

API reference

- https://iaas.uk-gov-london-1.oraclegovcloud.uk
- https://iaas.uk-gov-cardiff-1.oraclegovcloud.uk

Container Engine for Kubernetes API

API reference

- https://containerengine.uk-gov-london-1.oci.oraclegovcloud.uk
- https://containerengine.uk-gov-cardiff-1.oci.oraclegovcloud.uk

Database API

API reference

- https://database.uk-gov-london-1.oraclegovcloud.uk
- https://database.uk-gov-cardiff-1.oraclegovcloud.uk

You can track the progress of long-running Database operations with the Work Requests API.

Digital Assistant Service Instance API

API reference

- https://digitalassistant-api.uk-gov-london-1.oci.oraclegovcloud.uk
- https://digitalassistant-api.uk-gov-cardiff-1.oci.oraclegovcloud.uk

Email Delivery API

API reference

- https://ctrl.email.uk-gov-london-1.oci.oraclegovcloud.uk
- https://ctrl.email.uk-gov-cardiff-1.oci.oraclegovcloud.uk

Events API

API reference

- https://events.uk-gov-london-1.oci.oraclegovcloud.uk
- https://events.uk-gov-cardiff-1.oci.oraclegovcloud.uk

File Storage API

API reference

- https://filestorage.uk-gov-london-1.oci.oraclegovcloud.uk
- https://filestorage.uk-gov-cardiff-1.oci.oraclegovcloud.uk
Functions Service API

API reference
- https://functions.uk-gov-london-1.oci.oraclegovcloud.uk
- https://functions.uk-gov-cardiff-1.oci.oraclegovcloud.uk

IAM API

API reference
- https://identity.uk-gov-london-1.oraclegovcloud.uk
- https://identity.uk-gov-cardiff-1.oraclegovcloud.uk

**Note:**
Use the Endpoint of Your Home Region for All IAM API Calls

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your home region. Your home region is where your IAM resources are defined. When you subscribe to a new region, your IAM resources are replicated in the new region, however, the master definitions reside in your home region and can only be changed there. Make all IAM API calls against your home region endpoint. The changes automatically replicate to all regions. If you try to make an IAM API call against a region that is not your home region, you will receive an error.

Key Management API (for the Vault service)

API reference
- https://kms.uk-gov-london-1.oraclegovcloud.uk
- https://kms.uk-gov-cardiff-1.oraclegovcloud.uk

In addition to these endpoints, each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint.

Load Balancing API

API reference
- https://iaas.uk-gov-london-1.oraclegovcloud.uk
- https://iaas.uk-gov-cardiff-1.oraclegovcloud.uk

Marketplace Service API

API reference
- https://marketplace.uk-gov-london-1.oraclegovcloud.uk

Monitoring API

API reference
- https://telemetry-ingestion.uk-gov-london-1.oraclegovcloud.uk
- https://telemetry.uk-gov-london-1.oraclegovcloud.uk

Notifications API

API reference
Object Storage and Archive Storage APIs
Both Object Storage and Archive Storage are accessible with the following APIs:

Object Storage API
API reference
• https://objectstorage.uk-gov-london-1.oraclegovcloud.uk
• https://objectstorage.uk-gov-cardiff-1.oraclegovcloud.uk

Amazon S3 Compatibility API
API reference
• https://<object_storage_namespace>.compat.objectstorage.uk-gov-london-1.oraclegovcloud.uk
• https://<object_storage_namespace>.compat.objectstorage.uk-gov-cardiff-1.oraclegovcloud.uk

Tip:
See Understanding Object Storage Namespaces on page 3395 for information regarding how to find your Object Storage namespace.

Swift API (for use with Oracle RMAN)
• https://swiftobjectstorage.uk-gov-london-1.oraclegovcloud.uk
• https://swiftobjectstorage.uk-gov-cardiff-1.oraclegovcloud.uk

OS Management API
API reference
• https://osms.uk-gov-london-1.oci.oraclegovcloud.uk

Registry

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Available Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Gov South (London)</td>
<td>• ocir.uk-gov-london-1.oci.oraclegovcloud.uk</td>
</tr>
<tr>
<td>UK Gov West (Newport)</td>
<td>• ocir.uk-gov-cardiff-1.oci.oraclegovcloud.uk</td>
</tr>
</tbody>
</table>

Resource Manager API
API reference
• https://resourcemanager.uk-gov-london-1.oraclegovcloud.uk
• https://resourcemanager.uk-gov-cardiff-1.oraclegovcloud.uk

Search API
API reference
• https://query.uk-gov-london-1.oraclegovcloud.uk
• https://query.uk-gov-cardiff-1.oraclegovcloud.uk
Secret Management API (for the Vault service)

API reference

- https://vaults.uk-gov-london-1.oraclegovcloud.uk
- https://vaults.uk-gov-cardiff-1.oraclegovcloud.uk

Secret Retrieval API (for the Vault service)

API reference

- https://secrets.vaults.uk-gov-london-1.oraclegovcloud.uk
- https://secrets.vaults.uk-gov-cardiff-1.oraclegovcloud.uk

Streaming API

API reference

- https://streaming.uk-gov-london-1.oraclegovcloud.uk
- https://streaming.uk-gov-cardiff-1.oraclegovcloud.uk

Web Application Acceleration and Security API

API reference

- https://waas.uk-gov-london-1.oraclegovcloud.uk
- https://waas.uk-gov-cardiff-1.oraclegovcloud.uk

Work Requests API (for Compute and Database work requests)

API reference

- https://iaas.uk-gov-london-1.oraclegovcloud.uk
- https://iaas.uk-gov-cardiff-1.oraclegovcloud.uk

Services Not Supported in Oracle Cloud Infrastructure United Kingdom Government Cloud

The following services are currently not available for tenancies in the United Kingdom Government Cloud:

Solutions and Platform services not available:

- Announcements
- Application Migration
- Compliance Documents
- Big Data
- Blockchain Platform
- Health Checks

SMTP Authentication and Connection Endpoints

Email Delivery only supports the AUTH PLAIN command when using SMTP authentication. If the sending application is not flexible with the AUTH command, an SMTP proxy/relay can be used. For more information about the AUTH command, see AUTH Command and its Mechanisms.

<table>
<thead>
<tr>
<th>Region</th>
<th>SMTP Connection Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Gov South (London)</td>
<td>smtp.email.uk-gov-london-1.oci.oraclegovcloud.uk</td>
</tr>
<tr>
<td>UK Gov West (Newport)</td>
<td>smtp.email.uk-gov-cardiff-1.oci.oraclegovcloud.uk</td>
</tr>
</tbody>
</table>
SPF Record Syntax

An SPF record is a TXT record on your sending domain that authorizes Email Delivery IP addresses to send on your behalf. SPF is required for subdomains of oraclegovcloud.com and recommended in other cases. The SPF record syntax for the United Kingdom Government Cloud sending region is shown in the following table:

<table>
<thead>
<tr>
<th>Realm Key</th>
<th>SPF Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC4</td>
<td>v=spf1 include:rp.oraclegovemaildelivery.uk -all</td>
</tr>
</tbody>
</table>

The Realm Key is applicable for any sending regions in that realm.
Chapter 5

Service Essentials

The following topics provide essential information that applies across Oracle Cloud Infrastructure.

**Security Credentials** on page 179
The types of credentials you'll use when working with Oracle Cloud Infrastructure.

**Regions and Availability Domains** on page 180
An introduction to the concepts of regions and availability domains.

**Resource Identifiers** on page 197
A description of the different ways your Oracle Cloud Infrastructure resources are identified.

**Resource Monitoring** on page 199
Information about how to monitor your resources.

**Resource Tags** on page 211
Information about Oracle Cloud Infrastructure tags and how to apply them to your resources.

**Compartment Quotas** on page 243
Information about how to control resource consumption within compartments using quotas.

**Tenancy Explorer**
View all resources in a selected compartment, across regions.

**Service Limits** on page 215
A list of the default limits applied to your cloud resources and how to request an increase.

**Console Announcements** on page 260
Information about the announcements that occasionally appear in the Oracle Cloud Infrastructure Console

**Prerequisites for Oracle Platform Services on Oracle Cloud Infrastructure** on page 265
Instructions for setting up the resources required when running an Oracle Platform Service on Oracle Cloud Infrastructure.

**Renaming a Cloud Account** on page 272
Instructions for renaming an Oracle cloud account.
Billing and Payment Tools Overview on page 273
Information about billing and payment tools that you can use to analyze your service usage and manage your costs.

My Services Use Cases on page 300
Use cases for the Oracle Cloud My Services API, to help you interact programmatically with My Services.

Cloud Shell
A free-to-use browser-based terminal accessible from the Oracle Cloud Console that provides access to a Linux shell with pre-authenticated Oracle Cloud Infrastructure CLI and other useful tools.

Security Credentials
This section describes the types of credentials you'll use when working with Oracle Cloud Infrastructure.

Console Password
- **What it's for:** Using the Console.
- **Format:** Typical password text string.
- **How to get one:** An administrator will provide you with a one-time password.
- **How to use it:** Sign in to the Console the first time with the one-time password, and then change it when prompted. Requirements for the password are displayed there. The one-time password expires in seven days. If you want to change the password later, see To change your Console password on page 2459. Also, you or an administrator can reset the password in the Console or with the API (see To create or reset another user's Console password on page 2460). Resetting the password creates a new one-time password that you'll be prompted to change the next time you sign in to the Console. If you're blocked from signing in to the Console because you've tried 10 times in a row unsuccessfully, contact your administrator.
- **Note for Federated Users:** Federated users do not use a Console password. Instead, they sign in to the Console through their identity provider.

API Signing Key
- **What it's for:** Using the API (see Software Development Kits and Command Line Interface on page 4225 and Request Signatures on page 4383).
- **Format:** RSA key pair in PEM format (minimum 2048 bits required).
- **How to get one:** You can use the Console to generate the private/public key pair for you, or you can generate your own. See Required Keys and OCIDs on page 4179.
- **How to use it:** Use the private key with the SDK or with your own client to sign your API requests. Note that after you've added your first API key in the Console, you can use the API to upload any additional ones you want to use. If you provide the wrong kind of key (for example, your instance SSH key, or a key that isn't at least 2048 bits), you'll get an `InvalidKey` error.
- **Example:** The PEM public key looks something like this:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoTFqF...
...
-----END PUBLIC KEY-----
```

Instance SSH Key
- **What it's for:** Accessing a compute instance.
Service Essentials

- **Format**: For Oracle-provided images, these SSH key types are supported: RSA, DSA, DSS, ECDSA, and Ed25519. If you bring your own image, you're responsible for managing the SSH key types that are supported.

  For RSA, DSS, and DSA keys, a minimum of 2048 bits is recommended. For ECDSA keys, a minimum of 256 bits is recommended.

- **How to get one**: See Managing Key Pairs on Linux Instances on page 693. Optionally, you can use a key pair that is generated by Oracle Cloud Infrastructure when you create an instance in the Console.

- **How to use it**: When you launch an instance, provide the public key from the key pair.

- **Example**:

  A public key has the following format:

  

  `<key_type> <public_key> <optional_comment>`

  For example, an RSA public key looks like this:

  

  `ssh-rsa AAAAB3BzaC1yc2EAAAADAQABAAABAQD9BRwrUiLDki6P0+jZhsjS2muM... ...yXDus/5DQ== rsa-key-20201202`


Auth Token

- **What it's for**: Authenticating with third-party APIs that do not support Oracle Cloud Infrastructure's signature-based authentication. For example, use an auth token as your password with Swift clients.

- **Format**: Typical password text string.

- **How to get one**: See Working with Console Passwords and API Keys on page 2456.

- **How to use it**: Usage depends on the service you are authenticating with. Typically, you authenticate with third-party APIs by providing your Oracle Cloud Infrastructure Console login, your auth token provided by Oracle, and your organization's Oracle tenant name.

Regions and Availability Domains

This topic describes the physical and logical organization of Oracle Cloud Infrastructure resources.

About Regions and Availability Domains

Oracle Cloud Infrastructure is hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Most Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance. Traffic between availability domains and between regions is encrypted. Availability domains are isolated from each other, fault tolerant, and very unlikely to fail simultaneously. Because availability domains do not share infrastructure such as power or cooling, or the internal availability domain network, a failure at one availability domain within a region is unlikely to impact the availability of the others within the same region.

The availability domains within the same region are connected to each other by a low latency, high bandwidth network, which makes it possible for you to provide high-availability connectivity to the internet and on-premises, and to build replicated systems in multiple availability domains for both high-availability and disaster recovery.

Oracle is adding multiple cloud regions around the world to provide local access to cloud resources for our customers. To accomplish this quickly, we’ve chosen to launch regions in new geographies with one availability domain.

As regions require expansion, we have the option to add capacity to existing availability domains, to add additional availability domains to an existing region, or to build a new region. The expansion approach in a particular scenario is based on customer requirements as well as considerations of regional demand patterns and resource availability.
For any region with one availability domain, a second availability domain or region in the same country or geopolitical area will be made available within a year to enable further options for disaster recovery that support customer requirements for data residency where they exist.

Regions are independent of other regions and can be separated by vast distances—across countries or even continents. Generally, you would deploy an application in the region where it is most heavily used, because using nearby resources is faster than using distant resources. However, you can also deploy applications in different regions for these reasons:

- To mitigate the risk of region-wide events such as large weather systems or earthquakes.
- To meet varying requirements for legal jurisdictions, tax domains, and other business or social criteria.

Regions are grouped into realms. Your tenancy exists in a single realm and can access all regions that belong to that realm. You cannot access regions that are not in your realm. Currently, Oracle Cloud Infrastructure has multiple realms. There is one commercial realm. There are multiple realms for Government Cloud: US Government Cloud FedRAMP authorized and IL5 authorized, and United Kingdom Government Cloud.

The following table lists the regions in the Oracle Cloud Infrastructure commercial realm:

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region Identifier</th>
<th>Region Location</th>
<th>Region Key</th>
<th>Realm Key</th>
<th>Availability Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia East (Sydney)</td>
<td>ap-sydney-1</td>
<td>Sydney, Australia</td>
<td>SYD</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Australia Southeast</td>
<td>ap-melbourne-1</td>
<td>Melbourne, Australia</td>
<td>MEL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>sa-sao-paulo-1</td>
<td>Sao Paulo, Brazil</td>
<td>GRU</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>ca-montreal-1</td>
<td>Montreal, Canada</td>
<td>YUL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Chile (Santiago)</td>
<td>sa-santiago-1</td>
<td>Santiago, Chile</td>
<td>SCL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>eu-frankfurt-1</td>
<td>Frankfurt, Germany</td>
<td>FRA</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>India South (Hyderabad)</td>
<td>ap-hyderabad-1</td>
<td>Hyderabad, India</td>
<td>HYD</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>ap-mumbai-1</td>
<td>Mumbai, India</td>
<td>BOM</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>ap-osaka-1</td>
<td>Osaka, Japan</td>
<td>KIX</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td>ap-tokyo-1</td>
<td>Tokyo, Japan</td>
<td>NRT</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Netherlands Northwest</td>
<td>eu-amsterdam-1</td>
<td>Amsterdam, Netherlands</td>
<td>AMS</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Saudi Arabia West (Jeddah)</td>
<td>me-jeddah-1</td>
<td>Jeddah, Saudi Arabia</td>
<td>JED</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td>ap-seoul-1</td>
<td>Seoul, South Korea</td>
<td>ICN</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region Identifier</td>
<td>Region Location</td>
<td>Region Key</td>
<td>Realm Key</td>
<td>Availability Domains</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>South Korea North</td>
<td>ap-chuncheon-1</td>
<td>Chuncheon, South Korea</td>
<td>YNY</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>(Chuncheon)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland North</td>
<td>eu-zurich-1</td>
<td>Zurich, Switzerland</td>
<td>ZRH</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>(Zurich)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAE East (Dubai)</td>
<td>me-dubai-1</td>
<td>Dubai, UAE</td>
<td>DXB</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>UK South (London)</td>
<td>uk-london-1</td>
<td>London, United Kingdom</td>
<td>LHR</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>UK West (Newport)</td>
<td>uk-cardiff-1</td>
<td>Newport, United Kingdom</td>
<td>CWL</td>
<td>OC1</td>
<td>1</td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td>us-ashburn-1</td>
<td>Ashburn, VA</td>
<td>IAD</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>US West (Phoenix)</td>
<td>us-phoenix-1</td>
<td>Phoenix, AZ</td>
<td>PHX</td>
<td>OC1</td>
<td>3</td>
</tr>
<tr>
<td>US West (San Jose)</td>
<td>us-sanjose-1</td>
<td>San Jose, CA</td>
<td>SJC</td>
<td>OC1</td>
<td>1</td>
</tr>
</tbody>
</table>

To subscribe to a region, see Managing Regions on page 2445.

For a list of regions in the Oracle Government Cloud realms, see the following topics:

- Oracle Cloud Infrastructure US Government Cloud with FedRAMP Authorization on page 157
- Oracle Cloud Infrastructure US Federal Cloud with DISA Impact Level 5 Authorization on page 162
- Oracle Cloud Infrastructure United Kingdom Government Cloud on page 171

**Note:**

Your Tenancy's Availability Domain Names

Oracle Cloud Infrastructure randomizes the availability domains by *tenancy* to help balance capacity in the data centers. For example, the availability domain labeled PHX-AD-1 for tenancyA may be a different data center than the one labeled PHX-AD-1 for tenancyB. To keep track of which availability domain corresponds to which data center for each tenancy, Oracle Cloud Infrastructure uses tenancy-specific prefixes for the availability domain names. For example: the availability domains for your tenancy are something like *Uocm:PHX-AD-1*, *Uocm:PHX-AD-2*, and so on.

To get the specific names of your tenancy's availability domains, use the ListAvailabilityDomains operation, which is available in the IAM API. You can also see the names when you use the Console to launch an instance and choose which availability domain to launch the instance in.

**Fault Domains**

A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains provide anti-affinity: they let you distribute your instances so that the instances are not on the same physical hardware within a single availability domain. A hardware failure or Compute hardware maintenance event that affects one fault domain does not affect instances in other fault domains. In addition, the physical hardware in a fault domain has independent and redundant power supplies, which prevents a failure in the power supply hardware within one fault domain from affecting other fault domains.
To control the placement of your compute instances, bare metal DB system instances, or virtual machine DB system instances, you can optionally specify the fault domain for a new instance or instance pool at launch time. If you don't specify the fault domain, the system selects one for you. Oracle Cloud Infrastructure makes a best-effort anti-affinity placement across different fault domains, while optimizing for available capacity in the availability domain. To change the fault domain for a compute instance, edit the fault domain. To change the fault domain for a bare metal or virtual machine DB system instance, terminate it and launch a new instance in the preferred fault domain.

Use fault domains to do the following things:

- Protect against unexpected hardware failures or power supply failures.
- Protect against planned outages because of Compute hardware maintenance.

For more information:

- For recommendations about how to use fault domains when provisioning application and database servers, see Fault Domains on page 595 in Best Practices for Your Compute Instance on page 594.
- For more information about using fault domains when provisioning Oracle bare metal and virtual machine DB systems, see Virtual Machine DB Systems on page 1355 and Availability Domain and Fault Domain Considerations for Oracle Data Guard on page 1463.

### Subscribed Region Limits

Trial, free tier, and pay-as-you-go tenancies are limited to one subscribed region. You can request an increase to the limit for pay-as-you-go tenancies, see To request a subscribed region limit increase on page 183 for more information.

Universal monthly credit tenancies can subscribe to all publicly released commercial regions.

#### Requesting a Limit Increase to the Subscribed Region Count

You can submit a request to increase the subscribed region count for your tenancies from within the Console. If you try to subscribe to a region beyond the limit for your tenancy, you'll be prompted to submit a limit increase request. Additionally, you can launch the request from the service limits page or at any time by clicking the link under the Help menu (Help).  

#### To request a subscribed region limit increase

1. Open the Help menu (Help), go to Support and click Request service limit increase.
2. Enter the following:
   - **Primary Contact Details:** Enter the name and email address of the person making the request. Enter one email address only. A confirmation will be sent to this address.
   - **Service Category:** Select Regions.
   - **Resource:** Select Subscribed region count.
   - **Tenancy Limit:** Specify the limit number.
   - **Reason for Request:** Enter a reason for your request. If your request is urgent or unusual, please provide details here.
3. Click Submit Request.

After you submit the request, it is processed. A response can take anywhere from a few minutes to a few days. If your request is granted, a confirmation email is sent to the address provided in the primary contact details.

If we need additional information about your request, a follow-up email is sent to the address provided in the primary contact details.

### Service Availability Across Regions

All Oracle Cloud Infrastructure regions offer core infrastructure services, including the following:
• Compute: Compute (Intel-based bare metal & VM, DenseIO & Standard), Container Engine for Kubernetes, Registry
• Storage: Block Volume, File Storage, Object Storage, Archive Storage
• Networking: Virtual Cloud Network, Load Balancing, FastConnect (specific partners as available and requested)
• Database: Database, Exadata Cloud Service, Autonomous Data Warehouse, Autonomous Transaction Processing
• Edge: DNS
• Platform: Audit, Identity and Access Management, Monitoring, Notifications, Tagging, Work Requests
• Security: Vault

Generally available cloud services beyond those in the previous list are made available based on regional customer demand. Any service can be made available within a maximum of three months, with many services deploying more quickly. New cloud services are made available in regions as quickly as possible based on a variety of considerations, including regional customer demand, ability to achieve regulatory compliance where applicable, resource availability, and other factors. Because of Oracle Cloud Infrastructure's low latency interconnect backbone, you can use cloud services in other geographic regions with effective results when those services are not available in your home region, as long as data residency requirements do not prevent you from doing so. We regularly work with customers to help ensure effective access to required services.

Resource Availability

The following sections list the resource types based on their availability: across regions, within a single region, or within a single availability domain.

| Tip: |
| In general: IAM resources are cross-region. DB Systems, instances, and volumes are specific to an availability domain. Everything else is regional. Exception: Subnets were originally designed to be specific to an availability domain. Now, you can create regional subnets, which are what Oracle recommends. |

Cross-Region Resources

• API signing keys
• compartments
• detectors (Cloud Guard; regional to reporting region)
• dynamic groups
• federation resources
• groups
• managed lists (Cloud Guard)
• network sources
• policies
• responders (Cloud Guard; regional to reporting region)
• tag namespaces
• tag keys
• targets (Cloud Guard; regional to reporting region)
• users

Regional Resources

• alarms
• applications (Data Flow service)
• applications (Functions service)
• blockchain platforms (Blockchain Platform service)
• buckets: Although buckets are regional resources, they can be accessed from any location if you use the correct region-specific Object Storage URL for the API calls.
• clusters (Big Data service)
• clusters (Container Engine for Kubernetes service)
• cloudevents-rules
• config work requests (Logging Analytics)
• configuration source providers (Resource Manager)
• content and experience
• customer-premises equipment (CPE)
• dashboards (Management Dashboard)
• data catalogs
• database insights (Operations Insights)
• DB Systems (MySQL Database service)
• DHCP options sets
• dynamic routing gateways (DRGs)
• encryption keys
• entities (Logging Analytics)
• functions
• images
• internet gateways
• jobs (Database Management)
• jobs (Resource Manager)
• load balancers
• local peering gateways (LPGs)
• log groups (Logging Analytics)
• management agent install keys
• management agents
• managed database groups (Database Management)
• managed databases (Database Management)
• metrics
• models
• NAT gateways
• network security groups
• node pools
• notebook sessions
• object collection rules (Logging Analytics)
• private templates (Resource Manager)
• problems (Cloud Guard; regional to reporting region)
• projects
• queryjob work requests (Logging Analytics)
• repositories
• reserved public IPs
• route tables
• runs
• saved searches (Management Dashboard)
• scheduled tasks (Logging Analytics)
• secrets
• security lists
• service connectors
• service gateways
Service Essentials

- stacks (Resource Manager)
- storage work requests (Logging Analytics)
- subnets: When you create a subnet, you choose whether it's regional or specific to an availability domain. Oracle recommends using regional subnets.
- subscriptions
- tables
- tickets (Support Management service)
- topics
- vaults
- virtual cloud networks (VCNs)
- volume backups: They can be restored as new volumes to any availability domain within the same region in which they are stored.
- workspaces

Availability Domain-Specific Resources

- DB systems (Oracle Database service)
- ephemeral public IPs
- instances: They can be attached only to volumes in the same availability domain.
- subnets: When you create a subnet, you choose whether it is regional or specific to an availability domain. Oracle recommends using regional subnets.
- volumes: They can be attached only to an instance in the same availability domain.

Dedicated Regions

Dedicated regions are public regions assigned to a single organization. Region specific details, such as region ID and region key are not available in public documentation, check with your Oracle contact for this information for your dedicated region.

This topic provides general information for dedicated regions. For information about Oracle Cloud Infrastructure services, see Oracle Cloud Infrastructure.

Console URL

The Console URL you use to sign in to your region is constructed as follows:

```
http://console.<region_identifier>.oraclecloud8.com
```

To sign in to your region, enter the Console URL in a supported browser.

Service Endpoint Patterns

This section describes the pattern you use to construct endpoints for each service available in Oracle Cloud Infrastructure. Not all services listed here may be available in your specific region, confirm with your Oracle contact which services are available in your region.

Analytics API

API reference

Endpoint URL pattern:

- https://analytics.<region_identifier>.ocp.oraclecloud8.com

Announcements Service API

API reference

Endpoint URL pattern:
• https://announcements.<region_identifier>.oraclecloud8.com

**API Gateway API**

*API reference*

Endpoint URL pattern:

• https://apigateway.<region_identifier>.oci.oraclecloud8.com

**Application Migration API**

*API reference*

Endpoint URL pattern:

• https://applicationmigration.<region_identifier>.oraclecloud8.com

**Audit API**

*API reference*

Endpoint URL pattern:

• https://audit.<region_identifier>.oraclecloud8.com

**Autoscaling API**

*API reference*

Endpoint URL pattern:

• https://autoscaling.<region_identifier>.oci.oraclecloud8.com

**Big Data Service API**

*API reference*

Endpoint URL pattern:

• https://bigdataservice.<region_identifier>.oci.oraclecloud8.com

**Blockchain Platform Control Plane API**

*API reference*

Endpoint URL pattern:

• https://blockchain.<region_identifier>.oci.oraclecloud8.com

**Budgets API**

*API reference*

Endpoint URL pattern:

• https://usage.<region_identifier>.oci.oraclecloud8.com

**Cloud Advisor API**

*API reference*

Endpoint URL pattern:

• https://advisor.<region_identifier>.oraclecloud8.com

**Cloud Guard API**

*API reference*

Endpoint URL pattern:

• https://cloudguard-cp-api.<region_identifier>.oci.oraclecloud8.com
**Container Engine for Kubernetes API**

**API reference**

Endpoint URL pattern:
- https://containerengine.<region_identifier>.oci.oraclecloud8.com

**Core Services (covering Networking, Compute, and Block Volume)**

The Networking, Compute, and Block Volume services are accessible with the following API:

**API reference**

Endpoint URL pattern:
- https://iaas.<region_identifier>.oraclecloud8.com

**Data Catalog API**

**API reference**

Endpoint URL pattern:
- https://datacatalog.<region_identifier>.oci.oraclecloud8.com

**Data Flow API**

**API reference**

Endpoint URL pattern:
- https://dataflow.<region_identifier>.oci.oraclecloud8.com

**Data Integration API**

**API reference**

Endpoint URL pattern:
- https://dataintegration.<region_identifier>.oci.oraclecloud8.com

**Data Safe API**

**API reference**

Endpoint URL pattern:
- https://datasafe.<region_identifier>.oci.oraclecloud8.com

**Data Science API**

**API reference**

Endpoint URL pattern:
- https://datascience.<region_identifier>.oci.oraclecloud8.com

**Database API**

**API reference**

Endpoint URL pattern:
- https://database.<region_identifier>.oraclecloud8.com

You can track the progress of long-running Database operations with the [Work Requests](#) API.

**Digital Assistant Service Instance API**

**API reference**

Endpoint URL pattern:
- https://digitalassistant.<region_identifier>.oci.oraclecloud8.com
DNS API
API reference
Endpoint URL pattern:
• https://dns.<region_identifier>.oci.oraclecloud8.com

Email Delivery API
API reference
Endpoint URL pattern:
• https://ctrl.email.<region_identifier>.oci.oraclecloud8.com

Events API
API reference
Endpoint URL pattern:
• https://events.<region_identifier>.oci.oraclecloud8.com

File Storage API
API reference
Endpoint URL pattern:
• https://filestorage.<region_identifier>.oraclecloud8.com

Functions Service API
API reference
Endpoint URL pattern:
• https://functions.<region_identifier>.oci.oraclecloud8.com

Health Checks API
API reference
Endpoint URL pattern:
• https://healthchecks.<region_identifier>.oraclecloud8.com

IAM API
API reference
Endpoint URL pattern:
• https://identity.<region_identifier>.oraclecloud8.com

Load Balancing API
API reference
Endpoint URL pattern:
• https://iaas.<region_identifier>.oraclecloud8.com

LogAnalytics API
API reference
Endpoint URL pattern:
• https://loganalytics.<region_identifier>.oraclecloud8.com

Logging Ingestion API
API reference
Endpoint URL pattern:

- https://ingestion.logging.<region_identifier>.oraclecloud8.com

**Logging Management API**

**API reference**

Endpoint URL pattern:

- https://logging.<region_identifier>.oraclecloud8.com

**Logging Search API**

**API reference**

Endpoint URL pattern:

- https://logging.<region_identifier>.oraclecloud8.com

**Management Agent API**

**API reference**

Endpoint URL pattern:

- https://management-agent.<region_identifier>.oraclecloud8.com

**Management Dashboard API**

**API reference**

Endpoint URL pattern:

- https://managementdashboard.<region_identifier>.oraclecloud8.com

**Marketplace Service API**

**API reference**

Endpoint URL pattern:


**Monitoring API**

**API reference**

Endpoint URL pattern:

- https://telemetry-ingestion.<region_identifier>.oraclecloud8.com
- https://telemetry.<region_identifier>.oraclecloud8.com

**MySQL Database Service API**

**API reference**

Endpoint URL pattern:

- https://mysql.<region_identifier>.ocp.oraclecloud8.com

**NoSQL Database API**

**API reference**

Endpoint URL pattern:


**Notifications API**

**API reference**

Endpoint URL pattern:
Object Storage and Archive Storage APIs

Both Object Storage and Archive Storage are accessible with the following APIs:

**Object Storage API**

API reference

Endpoint URL pattern:

- https://objectstorage.<region_identifier>.oraclecloud8.com

**Amazon S3 Compatibility API**

API reference

Endpoint URL pattern:

- https://<object_storage_namespace>.compat.objectstorage.<region_identifier>.oraclecloud8.com

Tip:

See [Understanding Object Storage Namespaces](#) on page 3395 for information regarding how to find your Object Storage namespace.

**Swift API (for use with Oracle RMAN)**

API reference

Endpoint URL pattern:

- https://swiftobjectstorage.<region_identifier>.oraclecloud8.com

**Operations Insights API**

API reference

Endpoint URL pattern:

- https://operationsinsights.<region_identifier>.oci.oraclecloud8.com

**Oracle Cloud Agent API**

API reference

Endpoint URL pattern:

- https://faas.<region_identifier>.oraclecloud8.com

**Oracle Cloud My Services API**

API reference

Endpoint URL:

- https://itra.oraclecloud.com

**Oracle Cloud VMware Solution API**

API reference

Endpoint URL pattern:

- https://ocvps.<region_identifier>.oci.oraclecloud8.com

**Oracle Content and Experience API**

API reference

Endpoint URL pattern:

- https://cp.oce.<region_identifier>.ocp.oraclecloud8.com
Oracle Integration API

API reference

Endpoint URL pattern:
• https://integration.<region_identifier>.ocp.oraclecloud8.com

Organizations API

API reference

Endpoint URL pattern:
• https://organizations.<region_identifier>.oci.oraclecloud8.com

OS Management API

API reference

Endpoint URL pattern:
• https://osms.<region_identifier>.oci.oraclecloud8.com

Registry

API reference

Endpoint URL pattern:
• https://ocir.<region_identifier>.oci.oraclecloud8.com

Resource Manager API

API reference

Endpoint URL pattern:
• https://resourcemanager.<region_identifier>.oraclecloud8.com

Search API

API reference

Endpoint URL pattern:
• https://query.<region_identifier>.oraclecloud8.com

Service Connector Hub API

API reference

Endpoint URL pattern:
• https://service-connector-hub.<region_identifier>.oci.oraclecloud8.com

Service Limits API

API reference

Endpoint URL pattern:
• https://limits.<region_identifier>.oci.oraclecloud8.com

Streaming API

API reference

Endpoint URL pattern:
• https://streaming.<region_identifier>.oraclecloud8.com

Support Managements API

API reference
Endpoint URLs:

- https://incidentmanagement.us-ashburn-1.oraclecloud.com
- https://incidentmanagement.us-phoenix-1.oraclecloud.com

Usage API

API reference

Endpoint URL pattern:

- https://usageapi.<region_identifier>.oci.oraclecloud8.com

Vault Service Key Management API

API reference

Endpoint URL pattern:

- https://kms.<region_identifier>.oraclecloud8.com

In addition to these endpoints, each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint.

Vault Service Secret Management API

API reference

Endpoint URL pattern:

- https://vaults.<region_identifier>.oci.oraclecloud8.com

Vault Service Secret Retrieval API

API reference

Endpoint URL pattern:

- https://secrets.vaults.<region_identifier>.oci.oraclecloud8.com

Web Application Acceleration and Security API

API reference

Endpoint URL pattern:

- https://waas.<region_identifier>.oraclecloud8.com

Work Requests API (for Compute and Database work requests)

API reference

Endpoint URL pattern:

- https://iaas.<region_identifier>.oraclecloud8.com

IP Address Ranges

This topic provides information about public IP address ranges for services that are deployed in Oracle Cloud Infrastructure. Allow traffic to these CIDR blocks to ensure access to the services.

Endpoints for Oracle YUM repos are listed on this page. You can use DNS lookup to determine the public IP address for each endpoint.

Public IP Addresses for VCNs and the Oracle Services Network

Public IP address ranges for VCNs and the Oracle Services Network are published to a JSON file which you can download and view manually or consume programmatically.
The Oracle Services Network is a conceptual network in Oracle Cloud Infrastructure that is reserved for Oracle services. A service gateway offers private access to the Oracle Services Network from workloads in your VCN and your on-premises network. The published addresses correspond to the service CIDR label called All <region> Services in Oracle Services Network. For a list of the services available with a service gateway, see Service Gateway: Supported Cloud Services in Oracle Services Network.

**Downloading the JSON File**

Use this link to download the current list of public IP ranges.

You can poll the published file to check for new IP address ranges as frequently as every 24 hours. We recommend that you poll the published file at least weekly.

**JSON File Contents and Syntax**

IP addresses are published in the public_ip_ranges.json file with the fields in the following table.

**Example of the public_ip_ranges.json file**

```json
{
    "last_updated_timestamp": "2019-11-18T19:55:47.204985",
    "regions": [
        {
            "region": "us-phoenix-1",
            "cidrs": [
                {
                    "cidr": "129.146.0.0/21",
                    "tags": ["OCI"]
                },
                {
                    "cidr": "134.70.8.0/21",
                    "tags": ["OSN", "OBJECT_STORAGE"]
                }
            ]
        },
        {
            "region": "us-ashburn-1",
            "cidrs": [
                {
                    "cidr": "129.213.8.0/21",
                    "tags": ["OCI"]
                },
                {
                    "cidr": "134.70.24.0/21",
                    "tags": ["OSN", "OBJECT_STORAGE"]
                }
            ]
        }
    ]
}
```
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
<th>Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_updated_timestamp</td>
<td>File creation time in ISO 8601 format. Expressed as &lt;date&gt;T&lt;time&gt;</td>
<td>string</td>
<td>&quot;last_updated_timestamp&quot;: &quot;2019-11-18T19:55:47.204985&quot;</td>
</tr>
<tr>
<td>regions</td>
<td>IP CIDR ranges grouped by region.</td>
<td>array</td>
<td>See preceding Example of the public ip ranges.json file</td>
</tr>
<tr>
<td>region</td>
<td>The region of the IP CIDR ranges.</td>
<td>string</td>
<td>&quot;region&quot;: &quot;us-phoenix-1&quot;</td>
</tr>
<tr>
<td></td>
<td>Valid values: Any region in the Oracle Cloud Infrastructure commercial realm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For a complete list of regions, see Regions and Availability Domains on page 180.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>A group of IP address CIDR ranges.</td>
<td>array</td>
<td>See preceding Example of the public ip ranges.json file</td>
</tr>
<tr>
<td>cidr</td>
<td>One or more IPv4 IP addresses expressed in CIDR notation.</td>
<td>string</td>
<td>&quot;cidr&quot;: &quot;147.154.0.0/18&quot;</td>
</tr>
<tr>
<td>Field Name</td>
<td>Definition</td>
<td>Type</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>tags</td>
<td>The services associated with the IP address CIDR range. Valid values: • OCI: The VCN CIDR blocks. • OSN: The CIDR block ranges for the Oracle Services Network. • OBJECT_STORAGE: The CIDR block ranges used by the Object Storage service. For more information, see Overview of Object Storage on page 3392.</td>
<td>array of string values</td>
<td>&quot;tags&quot;: [ &quot;OCI&quot; ]</td>
</tr>
</tbody>
</table>

### Filtering the JSON file contents

After you download the JSON file, you can use a command line tool such as `jq` to filter the contents.

**Download jq**

Here are some examples of how you can use the tool to find and filter the information you need:

**Find the creation date of the JSON file:**

```bash
jq .last_updated_timestamp < public_ip_ranges.json
```

**Get all IPv4 addresses for a specific region:**

```bash
jq -r ".regions[] | select (.region=="us-phoenix-1") | .cidrs[] | select (.cidr | contains(".")) | .cidr ' < public_ip_ranges.json
```

### Public IP Addresses for the Oracle YUM Repos

The Oracle YUM repos have the following regional public endpoints.

<table>
<thead>
<tr>
<th>Region</th>
<th>YUM Server Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands Northwest (Amsterdam)</td>
<td><a href="https://yum-eu-amsterdam-1.oracle.com">https://yum-eu-amsterdam-1.oracle.com</a></td>
</tr>
<tr>
<td>Australia East (Sydney)</td>
<td><a href="https://yum-ap-sydney-1.oracle.com">https://yum-ap-sydney-1.oracle.com</a></td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td><a href="https://yum-ca-toronto-1.oracle.com">https://yum-ca-toronto-1.oracle.com</a></td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td><a href="https://yum-eu-frankfurt-1.oracle.com">https://yum-eu-frankfurt-1.oracle.com</a></td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td><a href="https://yum-ap-mumbai-1.oracle.com">https://yum-ap-mumbai-1.oracle.com</a></td>
</tr>
<tr>
<td>Region</td>
<td>YUM Server Endpoint</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td><a href="https://yum-ap-osaka-1.oracle.com">https://yum-ap-osaka-1.oracle.com</a></td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td><a href="https://yum-ap-tokyo-1.oracle.com">https://yum-ap-tokyo-1.oracle.com</a></td>
</tr>
<tr>
<td>Saudi Arabia West (Jeddah)</td>
<td><a href="https://yum-me-jeddah-1.oracle.com">https://yum-me-jeddah-1.oracle.com</a></td>
</tr>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td><a href="https://yum-ap-melbourne-1.oracle.com">https://yum-ap-melbourne-1.oracle.com</a></td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td><a href="https://yum-ap-seoul-1.oracle.com">https://yum-ap-seoul-1.oracle.com</a></td>
</tr>
<tr>
<td>UK South (London)</td>
<td><a href="https://yum-uk-london-1.oracle.com">https://yum-uk-london-1.oracle.com</a></td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td><a href="https://yum-us-ashburn-1.oracle.com">https://yum-us-ashburn-1.oracle.com</a></td>
</tr>
<tr>
<td>US West (Phoenix)</td>
<td><a href="https://yum-us-phoenix-1.oracle.com">https://yum-us-phoenix-1.oracle.com</a></td>
</tr>
</tbody>
</table>

You can use DNS lookup to determine the public IP address for each endpoint.

**Resource Identifiers**

This chapter describes the different ways your Oracle Cloud Infrastructure resources are identified.

**Oracle Cloud IDs (OCIDs)**

Most types of Oracle Cloud Infrastructure resources have an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). It's included as part of the resource's information in both the Console and API.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use the API, you need the OCID for your tenancy. For information about where to find it, see the next section.</td>
</tr>
</tbody>
</table>

OCIDs use this syntax:

```
ocid1.<RESOURCE TYPE>.<REALM>.[REGION].<FUTURE USE>.<UNIQUE ID>
```

- **ocid1**: The literal string indicating the version of the OCID.
- **resource type**: The type of resource (for example, instance, volume, vcn, subnet, user, group, and so on).
- **realm**: The realm the resource is in. A realm is a set of regions that share entities. Possible values are oc1 for the commercial realm, oc2 for the Government Cloud realm, or oc3 for the Federal Government Cloud realm. The regions in the commercial realm (OC1) belong to the domain oraclecloud.com. The regions in the Government Cloud (OC2) belong to the domain oraclegovcloud.com.
- **region**: The region the resource is in (for example, phx, iad, eu-frankfurt-1). With the introduction of the Frankfurt region, the format switched from a three-character code to a longer string. This part is present in the OCID only for regional resources or those specific to a single availability domain. If the region is not applicable to the resource, this part might be blank (see the example tenancy ID below).
- **future use**: Reserved for future use. Currently blank.
- **unique ID**: The unique portion of the ID. The format may vary depending on the type of resource or service.

**Example OCIDs**

Tenancy:

```
ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdos
```
Where to Find Your Tenancy's OCID

If you use the Oracle Cloud Infrastructure API, you need your tenancy's OCID in order to sign the API requests. You also use the tenancy ID in some of the IAM API operations.

Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the Tenancy Details page:

1. Open the Profile menu and click Tenancy: <your_tenancy_name>.
2. The tenancy OCID is shown under Tenancy Information. Click Copy to copy it to your clipboard.

The tenancy OCID looks something like this (notice the word "tenancy" in it):

`ocid1.tenancy.oc1..<unique_ID>`

Name and Description (IAM Only)

The IAM service requires you to assign a unique, unchangeable name to each of your IAM resources (users, groups, dynamic groups, federations, and policies). The name must be unique within the scope of the type of resource (for example, you can only have one user with the name BobSmith). Notice that this requirement is specific to IAM and not the other services.

The name you assign to a user at creation is their login for the Console.

You can use these names instead of the OCID when writing a policy (for example, Allow group <GROUP NAME> to manage all-resources in compartment <COMPARTMENT NAME>).

In addition to the name, you must also assign a description to each of your IAM resources (although it can be an empty string). It can be a friendly description or other information that helps you easily identify the resource. The description does not have to be unique, and you can change it whenever you like. For example, you might want to use the description to store the user's email address if you're not already using the email address as the user's unique name.

Display Name

For most of the Oracle Cloud Infrastructure resources you create (other than those in IAM), you can optionally assign a display name. It can be a friendly description or other information that helps you easily identify the resource. The display name does not have to be unique, and you can change it whenever you like. The Console shows the resource's display name along with its OCID.
Caution:
Avoid entering confidential information when assigning descriptions, tags, or friendly names to your cloud resources through the Oracle Cloud Infrastructure Console, API, or CLI.

Resource Monitoring
You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources when needed using queries or on a passive basis using alarms. Queries and alarms rely on metrics emitted by your resource to the Monitoring service.

Prerequisites
- IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.
- Metrics exist in Monitoring: The resources that you want to monitor must emit metrics to the Monitoring service.
- Compute instances: To emit metrics, the Compute Instance Monitoring plugin must be enabled on the instance, and plugins must be running. The instance must also have either a service gateway or a public IP address to send metrics to the Monitoring service. For more information, see Enabling Monitoring for Compute Instances on page 783.

Working with Resource Monitoring
Not all resources support monitoring. See Supported Services on page 2669 for the list of resources that support the Monitoring service, which is required for queries and alarms used in monitoring.

The Monitoring service works with the Notifications service to notify you when metrics breach. For more information about these services, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

To view default metric charts for a resource
On the page for the resource of interest, under Resources, click Metrics.

For example, to view metric data for a Compute instance:

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance you're interested in.
3. On the instance details page, under Resources, click Metrics.

   A chart is shown for each metric. For a list of metrics related to Compute instances, see Compute Instance Metrics on page 788.

The Console displays the last hour of metric data for the selected resource. A chart is shown for each metric emitted by the selected resource.

For a list of metrics emitted by your resource, see Supported Services on page 2669.

To view default metric charts for a set of resources

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Choose the **Metric Namespace** for the resource types of interest in the selected compartment.

   For example, choose **oci_lbaas** to see metrics for load balancers.

Default charts are displayed for all resources in the selected **Metric Namespace** and **Compartment**. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).

**Don't see all expected resources or metrics?**

- Try a different time range.
- Make sure the correct **Compartment** is selected.

Metric namespaces are shown only when associated resources exist in the selected compartment. For example, the **oci_autonomous_database** namespace is shown only when Autonomous Databases exist in the selected compartment.

- Confirm that the missing resources are emitting metrics. See Enabling Monitoring for Compute Instances on page 783.

- Review limits information. Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

**To create a query**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Metrics Explorer**.

   The **Metrics Explorer** page displays an empty chart with fields to build a query.

2. Fill in the fields for a new query.

   - **Compartment**: The compartment containing the resources that you want to monitor. By default, the first accessible compartment is selected.
   - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
   - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
   - **Metric Name**: The name of the metric. Only one metric can be specified. Metric selections depend on the selected compartment and metric namespace. Example: **CpuUtilization**
   - **Interval**: The aggregation window.

**Interval values**

Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the **1h** or **1d** interval values are supported.

- **1m** - 1 minute
- **5m** - 5 minutes
- **1h** - 1 hour
- **1d** - 1 day

**Note:**

For metric queries, the **interval** you select drives the default **resolution** of the request, which determines the maximum time range of data returned.

For more information about the resolution parameter as used in metric queries, see SummarizeMetricsData.

**Maximum time range returned for a query**

The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.
The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>

To specify a non-default resolution that differs from the interval, use the `SummarizeMetricsData` operation.

**See examples of returned data**

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of 1m, and the end time defaults to the current time (2019-01-08T10:00:00.789Z). This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z).

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th (2019-01-06T10:00:00.789Z), the earliest data point possible within this seven-day period would be 10:00 on January 1st.
• Statistic: The aggregation function.

**Statistic values**

- **COUNT**: The number of observations received in the specified time period.
- **MAX**: The highest value observed during the specified time period.
- **MEAN**: The value of Sum divided by Count during the specified time period.
- **MIN**: The lowest value observed during the specified time period.
- **P50**: The value of the 50th percentile.
- **P90**: The value of the 90th percentile.
- **P95**: The value of the 95th percentile.
- **P99**: The value of the 99th percentile.
- **P99.5**: The value of the 99.5th percentile.
- **RATE**: The per-interval average rate of change.
- **SUM**: All values added together.

• **Metric dimensions**: Optional filters to narrow the metric data evaluated.

**Dimension fields**

- **Dimension Name**: A qualifier specified in the metric definition. For example, the dimension `resourceId` is specified in the metric definition for `CpuUtilization`.

**Note:**

Long lists of dimensions are trimmed.

- To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
- To retrieve all dimensions for a given metric, use the following API operation: `ListMetrics`.

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **Additional dimension**: Adds another name-value pair for a dimension.

• **Aggregate Metric Streams**: Aggregates all results to plot a single aggregated average for all metric streams. This average is plotted as a single line on the metric chart. This operation is helpful when you want to plot a metric as one line for all resources.

3. **Click Update Chart**.

The chart shows the results of your new query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power). Units correspond to the selected metric and do not change by statistic.

**Troubleshooting Errors and Query Limits**

If you see an error that the query has exceeded the maximum number of `metric streams`, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams
by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

4. To customize the y-axis label or range, type the label you want into **Y-Axis Label** or type the minimum and maximum values you want into **Y-Axis Min Value** and **Y-Axis Max Value**.

   Only numeric characters are allowed for custom ranges. Custom labels and ranges are not persisted in shared queries (MQL).

5. To view the query as a Monitoring Query Language (MQL) expression, click **Advanced Mode**.

   **Advanced Mode** is located on the right, under the chart.

   Use Advanced Mode to edit your query using MQL syntax to aggregate results by group. The MQL syntax also supports additional parameter values. For more information about query parameters in Basic Mode and Advanced Mode, see Monitoring Query Language (MQL) Reference on page 2741.

6. To create another query, click **Add Query** below the chart.

### To create an alarm

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.

2. Click **Create alarm**.

   **Note:**
   
   You can also create an alarm from a predefined query on the **Service Metrics** page. Expand **Options** and click **Create an Alarm on this Query**. For more information about service metrics, see Viewing Default Metric Charts on page 2671.

3. On the **Create Alarm** page, under **Define alarm**, fill in or update the alarm settings:

   **Note:**
   
   To toggle between Basic Mode and Advanced Mode, click **Switch to Advanced Mode** or **Switch to Basic Mode** (to the right of **Define Alarm**).

**Basic Mode (default)**

By default, this page uses **Basic Mode**, which separates the metric from its dimensions and its trigger rule.

- **Alarm Name**:

  User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

**Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Rendering of the title</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Example: "High CPU usage alert. Follow runbook instructions for resolution."

- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description**: The metric to evaluate for the alarm condition.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Metric Name** (optional): The name of the metric. Only one metric can be specified. Example: `CpuUtilization`
  - **Interval**: The aggregation window, or the frequency at which data points are aggregated.

  **Interval values**

  **Note:**

  Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

  - **1m** - 1 minute
  - **5m** - 5 minutes
  - **1h** - 1 hour
  - **1d** - 1 day

  **Note:**

  For alarm queries, the specified `interval` has no effect on the `resolution` of the request. The only valid value of the resolution for an alarm...
query request is 1m. For more information about the resolution parameter as used in alarm queries, see Alarm.

- **Statistic**: The aggregation function.

  Statistic values
  - **COUNT**: The number of observations received in the specified time period.
  - **MAX**: The highest value observed during the specified time period.
  - **MEAN**: The value of Sum divided by Count during the specified time period.
  - **MIN**: The lowest value observed during the specified time period.
  - **P50**: The value of the 50th percentile.
  - **P90**: The value of the 90th percentile.
  - **P95**: The value of the 95th percentile.
  - **P99**: The value of the 99th percentile.
  - **P99.5**: The value of the 99.5th percentile.
  - **RATE**: The per-interval average rate of change.
  - **SUM**: All values added together.

- **Metric dimensions**: Optional filters to narrow the metric data evaluated.

  **Dimension fields**
  - **Dimension Name**: A qualifier specified in the metric definition. For example, the dimension `resourceId` is specified in the metric definition for `CpuUtilization`.

  **Note:**
  Long lists of dimensions are trimmed.
  - To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
• To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

• **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.

• **Additional dimension**: Adds another name-value pair for a dimension.

• **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.

• **Operator**: The operator used in the condition threshold.

  **Operator values**
  - greater than
  - greater than or equal to
  - equal to
  - less than
  - less than or equal to
  - **between** (inclusive of specified values)
  - **outside** (inclusive of specified values)
  - absent

• **Value**: The value to use for the condition threshold.

• **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click **Advanced Mode** or **Switch to Advanced Mode** to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See [Monitoring Query Language (MQL) Reference](#) on page 2741.

• **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

  **Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

• **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.

• **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."

• **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

• **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.

  • **Compartment**: The *compartment* containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  
  • **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  
  • **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  
  • **Query Code Editor** box: The alarm query as a Monitoring Query Language (MQL) expression.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.</td>
</tr>
</tbody>
</table>

Example alarm query:

```plaintext
CpuUtilization[1m]
{availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
```

For query syntax and examples, see Working with Metric Queries on page 2700.

• **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    - Available options:
      - **Notifications Service**.
  - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
  - **Topic**: The *topic* to use for notifications. Each topic supports a *subscription* protocol, such as PagerDuty.
  - **Create a topic**: Sets up a *topic* and *subscription* protocol in the selected compartment, using the specified destination service.
    - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team" for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
    - **Topic Description**: Description of the new topic.
    - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:
      - **Email subscription**
        - Sends an email message when you publish a *message* to the subscription's parent *topic*.
        - Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.
        - Some message types allow friendly formatting.
          - **Subscription Protocol**: Select Email.
          - **Subscription Email**: Type an email address.
      - **HTTPS (Custom URL) subscription**
        - Sends specified information when you publish a *message* to the subscription's parent *topic*.
        - Endpoint format (URL using HTTPS protocol):
          ```
          https://<anyvalidURL>
          ```
        - Basic access authentication is supported, allowing you to specify a username and password in the URL, as in `https://user:password@domain.com` or `https://user@domain.com`. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Subscription Protocol**: Select HTTPS (Custom URL).
- **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the PagerDuty documentation.

- **Subscription Protocol**: Select PagerDuty.
- **Subscription URL**: Type (or copy and paste) the *integration key* portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the Slack documentation.

- **Subscription Protocol**: Select Slack.
- **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: E.164 format.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service</td>
</tr>
</tbody>
</table>
Connector Hub. SMS messages sent by unsupported services are dropped. Troubleshoot dropped messages.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Available Countries and Regions

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
</tbody>
</table>
### Service Essentials

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
</tbody>
</table>

- **Additional destination service**: Adds another destination service and topic to use for notifications.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each alarm is limited to one destination per supported destination service.</td>
</tr>
</tbody>
</table>

- **Repeat Notification?**: While the alarm is in the firing state, resends notifications at the specified interval.
- **Notification Interval**: The period of time to wait before resending the notification.
- **Suppress Notifications**: Sets up a suppression time window during which to suspend evaluations and notifications. Useful for avoiding alarm notifications during system maintenance periods.
  - **Suppression Description**
  - **Start Time**
  - **End Time**

5. If you want to disable the new alarm, clear Enable This Alarm?.
6. Click Save alarm.

The new alarm is listed on the **Alarm Definitions** page.

### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To create a query, use the SummarizeMetricsData operation.

To create an alarm, use the CreateAlarm operation.

### Resource Tags

When you have many resources (for example, instances, VCNs, load balancers, and block volumes) across multiple compartments in your tenancy, it can become difficult to track resources used for specific purposes, or to aggregate them, report on them, or take bulk actions on them. **Tagging** allows you to define keys and values and associate them with resources. You can then use the tags to help you organize and list resources based on your business needs.

There are two types of tags:

- **Defined tags** are set up in your tenancy by an administrator. Only users granted permission to work with the defined tags can apply them to resources.

- **Free-form tags** can be applied by any user with permissions on the resource.

For more detailed information about tags and their features, see Tagging Overview on page 3906.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watch a video to introduce you to the concepts and features of tagging: Introduction to Tagging.</td>
</tr>
</tbody>
</table>
Caution:
Avoid entering confidential information when assigning descriptions, tags, or friendly names to your cloud resources through the Oracle Cloud Infrastructure Console, API, or CLI.

Working with Resource Tags

To bulk add defined tags
How to add multiple defined tags to existing resources. To apply defined tags, you must have permission to use the namespace.

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tenancy Explorer.
2. Select the resources to which you want to add tags. Optionally, use the Filter by resource type drop-down menu to narrow the list of resources.
3. In the Actions menu, click Manage Tags.

The Manage Tags page opens. The first table displays the tags currently applied to the selected resources. The second table displays the selected resources.
4. Under the list of existing tags, click + Add New.
   a. Select the Tag Namespace.
   b. Select the Tag Key.
   c. For Value, enter a value.
5. To apply another tag, repeat the previous step. To remove a row, click the Remove (x) button.
6. When you have added all the desired tags, click Next.

A confirmation page opens that lists the actions to take and the resources that the actions apply to.
7. Click Submit.

The Work Request page launches to show you the status of the work request to add tags to the resources.

To add defined tags to one existing resource
To apply a defined tag, you must have permission to use the namespace.

1. Open the Console, go to the details page of the resource you want to tag.

For example, to tag a compute instance: Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances. A list of the instances in your current compartment is displayed. Find the instance that you want to tag, and click its name to view its details page.
2. Click Apply Tags. Depending on the resource, this option might appear in the More Actions menu.
3. In the Apply Tags to the Resource dialog:
   a. Select the Tag Namespace.
   b. Select the Tag Key.
   c. In Value, either enter a value or select one from the list.
   d. To apply another tag, click + Additional Tag.
   e. When finished adding tags, click Apply Tag(s).

To add a free-form tag to an existing resource

1. Open the Console, go to the details page of the resource you want to tag.

For example, to tag a compute instance: Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances. A list of the instances in your current compartment is displayed. Find the instance that you want to tag, and click its name to view its details page.
2. Click Apply Tags. Depending on the resource, this option might appear in the More Actions menu.
3. In the **Apply Tags to the Resource** dialog:
   a. Select *None* (apply a free-form tag).
   b. Enter the *Tag Key*.
   c. Enter a *Value*.
   d. To apply another tag, click **+ Additional Tag**.
   e. When finished adding tags, click **Apply Tag(s)**.

**To add a tag during resource creation**

You can apply tags during resource creation. The location of the **Apply Tag(s)** option in the dialog varies by resource. The general steps are:

1. In the resource Create dialog, click **Apply Tags**.
   
   On some resources, you have to click **Show Advanced Options** to apply a tag.

2. In the **Apply Tags to the Resource** dialog:
   a. Select the **Tag Namespace**, or select *None* to apply a free-form tag.
   b. Select or enter the **Tag Key**.
   c. In **Value**, either enter a value or select one from the list.
   d. To apply another tag, click **+ Additional Tag**.
   e. Click **Apply Tag(s)**.

**To filter a list of resources by a tag**

Open the Console, click the service name and then click the resource you want to view. The left side of the page shows all the filters currently applied to the list.

For example, to view compute instances: Click **Compute** and then click **Instances**, to see the list of instances in your current compartment.

**To filter a list of resources by a defined tag**

1. Next to **Tag Filters**, click **add**.
2. In the **Apply a Tag Filter** dialog, enter the following:
   a. **Namespace**: Select the tag namespace.
   b. **Key**: Select a specific key.
   c. **Value**: Select from the following:
      • **Match Any Value** - returns all resources tagged with the selected namespace and key, regardless of the tag value.
      • **Match Any of the Following** - returns resources with the tag value you enter in the text box. Enter a single value in the text box. To specify multiple values for the same namespace and key, click **+** to display another text box. Enter one value per text box.
   d. Click **Apply Filter**.

**To filter a list of resources by a free-form tag**

1. Next to **Tag Filters**, click **add**.
2. In the **Apply a Tag Filter** dialog, enter the following:
   a. **Key**: Enter the tag key.
   b. **Value**: Select from the following:
      - **Match Any Value** - returns all resources tagged with the selected free-form tag key, regardless of the tag value.
      - **Match Any of the Following** - returns resources with the tag value you enter in the text box. Enter a single value in the text box. To specify multiple values for the same key, click + to display another text box. Enter one value per text box.
   c. Click **Apply Filter**.

### To bulk update defined tags

How to update defined tags applied to one or more resources.

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tenancy Explorer**.
2. Select the resources whose tags you want to update. Optionally, use the **Filter by resource type** drop-down menu to narrow the list of resources.
3. In the **Actions** menu, click **Manage Tags**.
   
   The Manage Tags page opens. The first table displays the tags currently applied to the selected resources. The second table displays the selected resources.
4. In the list of tags, find the tag that you want to update and enter a new value. To revert the change, click the **Undo** button.
5. For **Action**, select **Apply tag to all selected resources**.
6. If desired, update more tag values. Then, click **Next**.
   
   A confirmation page opens that lists the actions to take and the resources that the actions apply to.
7. Click **Submit**.

The Work Request page launches to show you the status of the work request to update the tags on the resources.

### To update a tag applied to a single resource

1. Open the Console, click the service name, and then click the resource you want to view.
   
   For example, to view compute instances: Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. A list of the instances in your current compartment is displayed. Find the instance that you want to update, and click its name to view its details page.
2. Click **Tags**.
   
   The list of tags applied to the resource is displayed.
3. Find the tag you want to update and click the pencil icon next to it.
4. Enter or select a new value.
5. Click **Save**.

### To bulk remove defined tags

How to remove multiple defined tags from resources.

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tenancy Explorer**.
2. Select the resources from which you want to remove tags. Optionally, use the **Filter by resource type** drop-down menu to narrow the list of resources.
3. In the **Actions** menu, click **Manage Tags**.
   
   The Manage Tags page opens. The first table displays the tags currently applied to the selected resources. The second table displays the selected resources.
4. In the list of tags, find the tag that you want to remove. For Action, select **Remove tag from all selected resources**.

5. To remove another tag, repeat the previous step.

6. Click **Next**.

   A confirmation page opens that lists the actions to take and the resources that the actions apply to.

7. Click **Submit**.

The Work Request page launches to show you the status of the work request to remove tags from the resources.

**To remove a tag from a single resource**

1. Open the Console, click the service name and then click the resource you want to view.

   For example, to view a compute instance: Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. A list of the instances in your current compartment is displayed. Find the instance that you want to remove the tag from, and click its name to view its details page.

2. Click **Tags**.

   The list of tags applied to the resource is displayed.

3. Find the tag you want to remove and click the pencil icon next to it.

4. Click **Remove Tag**.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- To apply a tag to an individual resource using the API, use the appropriate resource's `create` or `update` operation.
- `BulkEditTags` - adds, updates, and removes multiple tag key definitions on the selected resources
- `ListBulkEditTagsResourceTypes` - lists the resource types that support bulk tag editing

**Service Limits**

This topic describes the service limits for Oracle Cloud Infrastructure and the process for requesting a service limit increase.

**About Service Limits and Usage**

When you sign up for Oracle Cloud Infrastructure, a set of service limits is configured for your tenancy. The service limit is the quota or allowance set on a resource. For example, your tenancy is allowed a maximum number of compute instances per availability domain. These limits are generally established with your Oracle sales representative when you purchase Oracle Cloud Infrastructure. If you did not establish limits with your Oracle sales representative, or, if you signed up through the Oracle Store, default or trial limits are set for your tenancy. These limits may be increased for you automatically based on your Oracle Cloud Infrastructure resource usage and account standing. You can also request a service limit increase.

**Compartment Quotas**

Compartment quotas are similar to service limits; the biggest difference is that service limits are set by Oracle, and compartment quotas are set by administrators, using policies that allow them to allocate resources with a high level of flexibility. Compartment quotas are set using `policy statements` written in a simple declarative language that is similar to the IAM policy language.

To learn more, see **Compartment Quotas** on page 243.
Viewing Your Service Limits, Quotas, and Usage

You can view your tenancy's limits, quotas, and usage in the Console. Be aware that:

- The Console might not yet display limits and usage information for all of the Oracle Cloud Infrastructure services or resources.
- The usage level listed for a given resource type could be greater than the limit if the limit was reduced after the resources were created.
- If all the resource limits are listed as 0, this means your account has been suspended. For help, contact Oracle Support.

If you don't yet have a tenancy or a user login for the Console, or if you don't find a particular limit listed in the Console, see Limits by Service on page 218 for the default tenancy limits.

Service Limits API Policy

For the resource availability API (usage) the policy can be at the tenant or compartment level:

Allow group LimitsAndUsageViewers to read resource-availability in tenancy
Allow group LimitsAndUsageViewers to read resource-availability in compartment A

For limit definitions, services, and values APIs (only at the tenant level):

Allow group LimitsAndUsageViewers to inspect resource-availability in tenancy

For limit values APIs (does not include definitions or services), the following policy is also supported:

Allow group LimitsAndUsageViewers to inspect limits in tenancy

To view your tenancy's limits and usage (by region)

Note:

Required Permission

If you're in the Administrators group, you have permission to view the limits and usage. If you're not, here's an example IAM policy that grants the required permission to users in a group called LimitsAndUsageViewers:

Allow group LimitsAndUsageViewers to inspect resource-availability in tenancy

READ resource-availability is required to obtain the resource availability. There are four APIs:

- listServices
- listLimitDefinitions
- listLimitValues
- getResourceAvailability

listServices, listLimitDefinitions, and listLimitValues all require INSPECT at the tenancy level, while
getResourceAvailability requires READ at the compartment level to be able to read the data.

**Note:**
The Console may not display limits and usage information yet for all Oracle Cloud Infrastructure services or resources.

1. Open the Console. Open the navigation menu. Under Governance and Administration, go to Governance and click Limits, Quotas and Usage.

Your resource limits, quotas, and usage for the specific region are displayed, broken out by service. You can use the filter drop-down lists at the top of the list to filter by service, scope, resource, and compartment.

### When You Reach a Service Limit

When you reach the service limit for a resource, you receive an error when you try to create a new resource of that type. You are then prompted to submit a request to increase your limit. You cannot create a new resource until you are granted an increase to your service limit or you terminate an existing resource. Note that service limits apply to a specific scope, and when the service limit in one scope is reached you may still have resources available to you in other scopes (for example, other availability domains).

### Requesting a Service Limit Increase

**Note:**
Government Cloud customers can’t use the procedure here to request a service limit increase. Instead, see Requesting a Service Limit Increase for Government Cloud Tenancies on page 154.

You can submit a request to increase your service limits from within the Console. If you try to create a resource for which limit has been met, you'll be prompted to submit a limit increase request. Additionally, you can launch the request from the service limits page or at any time by clicking the link under the Help menu ( )

This procedure applies to requests for service limit increases. For details about the subscribed region limit and how to request an increase to that limit, see Subscribed Region Limits on page 183.

### To request a service limit increase

1. Open the Help menu ( ), go to Support and click Request service limit increase.
2. Enter the following:
   - **Primary Contact Details:** Enter the name and email address of the person making the request. Enter one email address only. A confirmation will be sent to this address.
   - **Service Category:** Select the appropriate category for your request.
   - **Resource:** Select the appropriate resource.
     - Depending on your selection for resource, additional fields might display for more specific information.
   - **Reason for Request:** Enter a reason for your request. If your request is urgent or unusual, please provide details here.
3. Click Create Request.

After you submit the request, it is processed. A response can take anywhere from a few minutes to a few days. If your request is granted, a confirmation email is sent to the address provided in the primary contact details.

If we need additional information about your request, a follow-up email is sent to the address provided in the primary contact details.
Limits by Service
The following tables list the default limits for each service. Note the scope that each limit applies to (for example, per availability domain, per region, per tenant, etc.).

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some services have additional limits. For more information, see the overview of each service.</td>
</tr>
</tbody>
</table>

### Analytics Cloud Limits
For Analytics Cloud limits, see Service Limits.

### API Gateway Limits
Limits apply to each tenancy.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>API gateways per region</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>API resources per region</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>API description length</td>
<td>1 MB</td>
<td>1 MB</td>
</tr>
<tr>
<td>Certificates per region</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

### Application Migration Limits
For Application Migration limits, see Service Limits.

### Big Data Limits
For Big Data limits, see Service Limits.

### Block Volume Limits
Volume limits apply to each availability domain. Volume backup limits apply to each region.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Volumes aggregated size</td>
<td>100 TB</td>
<td>30 TB</td>
</tr>
<tr>
<td>Backups</td>
<td>100,000</td>
<td>100,000</td>
</tr>
</tbody>
</table>

### Blockchain Platform Limits
For Blockchain Platform limits, see Service Limits.

### Cloud Guard Limits
Cloud Guard limits are regional.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detector Recipe Count</td>
<td>25</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>
### Service Essentials

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responder Recipe Count</td>
<td>15</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Target Count</td>
<td>50</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Managed List Count</td>
<td>20</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>

### Cloud Shell Limits

Limits apply to each region.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active User Count</td>
<td>75</td>
<td>50</td>
</tr>
<tr>
<td>Usage Hours Count</td>
<td>400</td>
<td>240</td>
</tr>
</tbody>
</table>

### Compute Limits

**Compute Instances**

Limits apply to each availability domain.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total OCPUs (cores) for shapes in the VM.Standard2 and BM.Standard2 series</td>
<td>3,460</td>
<td>6</td>
</tr>
<tr>
<td>Total OCPUs (cores) for shapes in the VM.Standard.E2.1.Micro series</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Total OCPUs (cores) for shapes in the VM.Standard.E2 and BM.Standard.E2 series</td>
<td>730</td>
<td>6</td>
</tr>
<tr>
<td>Total OCPUs (cores) for shapes in the VM.DenseIO2 and BM.DenseIO2 series</td>
<td>344</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Total GPUs for shapes in the VM.GPU3 and BM.GPU3 series</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Total GPUs for shapes in the BM.GPU4 series</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Resource</td>
<td>Monthly or Annual Universal Credits</td>
<td>Pay-as-You-Go or Promo</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Total OCPUs (cores) for shapes in the BM.HPC2 series</td>
<td>180</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Total OCPUs (cores) for DVH.Standard2.52 shapes</td>
<td>52</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>

**Note:**
Compute limits used to apply at the individual shape level. These limits have been deprecated. Although you can continue to use the deprecated shape-based limits, the limits are converted to the equivalent OCPU-based (core-based) values.

**Other Compute Resources**

Limits apply to different scopes, depending on the resource.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoscaling configurations</td>
<td>Region</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>Custom images</td>
<td>Region</td>
<td>100</td>
<td>25</td>
</tr>
<tr>
<td>Cluster networks</td>
<td>Tenancy</td>
<td>15</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Instance configurations</td>
<td>Region</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>Instance pools</td>
<td>Region</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Instances per instance pool</td>
<td>Region</td>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

**Container Engine for Kubernetes Limits**

Container Engine for Kubernetes limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clusters</td>
<td>3 clusters per OCI region</td>
<td>1 cluster per OCI region</td>
</tr>
<tr>
<td>Nodes</td>
<td>1000 nodes per cluster</td>
<td>1000 nodes per cluster</td>
</tr>
<tr>
<td>Pods</td>
<td>110 pods per node</td>
<td>110 pods per node</td>
</tr>
</tbody>
</table>

**Content and Experience Limits**

For Content and Experience limits, see Service Limits.

**Data Catalog Limits**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Catalog</td>
<td>Regional</td>
<td>2 data catalog instances per region</td>
</tr>
</tbody>
</table>
Data Flow Limits

Limits apply to each tenancy.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard2.1</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>VM.Standard2.2</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>VM.Standard2.4</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>VM.Standard2.8</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>VM.Standard2.16</td>
<td>0 # Contact Us</td>
<td>0</td>
</tr>
<tr>
<td>VM.Standard2.24</td>
<td>0 # Contact Us</td>
<td>0</td>
</tr>
<tr>
<td>VM.Total</td>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>

Data Integration Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace</td>
<td>Regional</td>
<td>5 workspaces per region</td>
</tr>
</tbody>
</table>

Data Safe Limits

For Data Safe limits, see Service Limits.

Note:
To register an Oracle Database with Data Safe, you must be using a paid account.

Data Science Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Volumes</td>
<td>150</td>
<td>30</td>
</tr>
<tr>
<td>Block Volume Size in GB</td>
<td>102400</td>
<td>10240</td>
</tr>
<tr>
<td>GPUs for VM.GPU2</td>
<td>3</td>
<td>Contact Us</td>
</tr>
<tr>
<td>GPUs for VM.GPU3</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Models</td>
<td>10000</td>
<td>1000</td>
</tr>
<tr>
<td>Notebook Sessions</td>
<td>10000</td>
<td>1000</td>
</tr>
<tr>
<td>Projects</td>
<td>10000</td>
<td>1000</td>
</tr>
<tr>
<td>VM.Standard2 Core</td>
<td>800</td>
<td>60</td>
</tr>
<tr>
<td>VM.Standard E2 Core</td>
<td>200</td>
<td>40</td>
</tr>
</tbody>
</table>

Data Transfer Limits

Data Transfer limits are regional.
Disk-Based Data Import

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-As-You-Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer package</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

File a service request at My Oracle Support to increase the service limits for Disk-Based Data Import. See Requesting a Service Limit Increase on page 217 for details.

Appliance-Based Data Import and Data Export

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-As-You-Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer appliances</td>
<td>2, Request Entitlement</td>
<td>Contact Your CSM</td>
</tr>
</tbody>
</table>

To place an order for the Oracle-provided Data Transfer Appliance used for appliance-based data transfer and data export jobs, request the required entitlement for your tenancy through the Console or CLI. See Requesting Appliance Entitlement on page 1024 for instructions.

The buyer of your tenancy will be required to e-sign a Terms and Conditions document. After Oracle receives the signed document you will have the entitlement to request and use the Data Transfer Appliance. Appliance-Based Data Import and Data Export each come with a service limit of 2. File a service request if you need to increase that number.

Database Limits

Database limits are per availability domain.

See Data Safe Limits on page 221 for information on Data Safe. See MySQL Database Limits on page 226 for information on MySQL Database.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Monthly Flex</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous Database on shared Exadata infrastructure - Total OCPUs</td>
<td>128 cores</td>
<td>8 cores</td>
</tr>
<tr>
<td>Contact Us Total OCPUs determined by the Exadata hardware shape (quarter rack, half rack, or full rack).</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Autonomous Database on dedicated Exadata infrastructure - Total OCPUs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always Free Autonomous Database</td>
<td>2 instances</td>
<td>2 instances</td>
</tr>
<tr>
<td>Always Free Autonomous Database - Total OCPUs</td>
<td>1 core</td>
<td>1 core</td>
</tr>
<tr>
<td>Always Free Autonomous Database - Total Block Storage</td>
<td>20 GB</td>
<td>20 GB</td>
</tr>
<tr>
<td>VM.Standard1 -Total OCPUs</td>
<td>10 cores</td>
<td>2 cores</td>
</tr>
<tr>
<td>Resources</td>
<td>Monthly Flex</td>
<td>Pay-as-You-Go or Promo</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>VM.Standard2 -Total OCPUs</td>
<td>100 cores (US West (Phoenix), US East (Ashburn)) 50 cores (Germany Central (Frankfurt), UK South (London))</td>
<td>2 cores</td>
</tr>
<tr>
<td>Total VM DB Block Storage (see note)</td>
<td>10TB</td>
<td>2TB</td>
</tr>
<tr>
<td>BM.DenseIO1.36 (see availability note)</td>
<td>1 instance</td>
<td>1 instance</td>
</tr>
<tr>
<td>Exadata.Base.48</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Exadata.Quarter1.84 - X6</td>
<td>Contact Us</td>
<td>Not available</td>
</tr>
<tr>
<td>Exadata.Half1.168 - X6</td>
<td>Contact Us</td>
<td>Not available</td>
</tr>
<tr>
<td>Exadata.Full1.336 - X6</td>
<td>Contact Us</td>
<td>Not available</td>
</tr>
<tr>
<td>Exadata.Quarter2.92 - X7</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Exadata.Half2.184 - X7</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Exadata.Full2.368 - X7</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Exadata.Quarter3.100 - X8</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Exadata.Half3.200 - X8</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Exadata.Full3.300 - X8</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>

**Note:**

- **Total VM DB Block Storage**: Includes block storage for all VM.Standard1 and VM.Standard2 virtual machine databases.
- **BM.DenseIO1.36**: This DB system shape is available only to monthly universal credit customers with tenancies existing on or before November 9th, 2018, in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.
- **Always Free Autonomous Database**: Each of the two Always Free Autonomous Databases available in your tenancy can be provisioned with your choice of Autonomous Transaction Processing or Autonomous Data Warehouse workload types.

**Digital Assistant Limits**

For Digital Assistant limits, see Service Limits.
DNS Limits
DNS limits are global.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zones</td>
<td>1,000 zones</td>
<td>1,000 zones</td>
</tr>
<tr>
<td>Records</td>
<td>25,000 per zone</td>
<td>25,000 per zone</td>
</tr>
<tr>
<td>Zone File Size</td>
<td>1 MB</td>
<td>1 MB</td>
</tr>
</tbody>
</table>

Email Delivery Limits
Limits apply to each tenant or availability domain on a per-region basis, as specified.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-As-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email volume</td>
<td>50,000 unique recipients among all emails sent per day</td>
<td>200 unique recipients among all emails sent per day</td>
</tr>
<tr>
<td>Maximum approved senders</td>
<td>10,000</td>
<td>2,000</td>
</tr>
<tr>
<td>SMTP credentials</td>
<td>2 per user</td>
<td>2 per user</td>
</tr>
<tr>
<td>Sending rate</td>
<td>18,000 emails per minute</td>
<td>10 emails per minute</td>
</tr>
</tbody>
</table>

Note:
The email volume limit applies to unique recipients among all emails sent. For example, a single email sent to 100 recipients would count the same as 100 individual emails each sent to a single recipient.

Note:
Email Delivery supports messages up to 2 MB, inclusive of message headers, body, and attachments. Customers can request this limit to be increased based on their requirement. The maximum size that can be requested is 60 MB.

Events Limits
Events limits are regional.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

File Storage Limits
Limits apply to each tenant or availability domain, as specified.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Pre-Paid</th>
<th>Pay-As-You-Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>File systems</td>
<td>1000 per tenant per availability domain</td>
<td>1000 per tenant per availability domain</td>
</tr>
<tr>
<td>Mount targets</td>
<td>2 per tenant per availability domain</td>
<td>2 per tenant per availability domain</td>
</tr>
</tbody>
</table>
## Service Essentials

### Maximum file system size

<table>
<thead>
<tr>
<th>Resource</th>
<th>Pre-Paid</th>
<th>Pay-As-You-Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum file system size</td>
<td>8 exabytes</td>
<td>8 exabytes</td>
</tr>
</tbody>
</table>

### Functions Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Region</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Functions</td>
<td>Region</td>
<td>500</td>
<td>50</td>
</tr>
<tr>
<td>Total memory for concurrent function execution</td>
<td>Availability Domain</td>
<td>60 GB</td>
<td>60 GB</td>
</tr>
</tbody>
</table>

### Health Checks Limits

Health Checks limits are **global**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint tests</td>
<td>1000 per account</td>
<td>1000 per account</td>
</tr>
</tbody>
</table>

### IAM Limits

IAM limits are **global**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go, Promo, &amp; Always Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users in a tenancy</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>Groups in a tenancy</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>Dynamic groups in a tenancy</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Network source groups in a tenancy</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Compartments in a tenancy</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Policies in a tenancy</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Statements in a policy</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Users per group in a tenancy</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>Groups per user in a tenancy</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>Identity providers in a tenancy</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Group mappings for an identity provider</td>
<td>250</td>
<td>250</td>
</tr>
</tbody>
</table>

### Integration Limits

For Integration limits, see [Service Limits](#).

---

Oracle Cloud Infrastructure User Guide 225
Load Balancing Limits
Load Balancing limits are regional.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>LB-Capacity-10Mbps</td>
<td>1 Load Balancer</td>
<td>1 Load Balancer</td>
</tr>
<tr>
<td>LB-Capacity-100Mbps</td>
<td>3 Load Balancers</td>
<td>1 Load Balancer</td>
</tr>
<tr>
<td>LB-Capacity-400Mbps</td>
<td>3 Load Balancers</td>
<td>1 Load Balancer</td>
</tr>
<tr>
<td>LB-Capacity-8000Mbps</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>

Logging Analytics Limits
Logging Analytics limits are regional.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>loganalytics-log-group</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>loganalytics-entity</td>
<td>10,000</td>
<td>10,000</td>
</tr>
</tbody>
</table>

Logging Limits
Logging limits are regional.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogGroups</td>
<td>Regional</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>LogObjects</td>
<td>Regional</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>UnifiedAgentConfigurations</td>
<td>Regional</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>MaximumQueriesPerMinute</td>
<td>Regional</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>MaximumConcurrentQueries</td>
<td>Regional</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Management Agent Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management agents</td>
<td>Tenant</td>
<td>5000</td>
</tr>
<tr>
<td>Management agent install keys</td>
<td>Tenant</td>
<td>300</td>
</tr>
</tbody>
</table>

MySQL Database Limits
MySQL Database limits are per availability domain unless explicitly specified.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly Flex</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL Database Block Storage</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database Manual Backup Count (regional)</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Resource</td>
<td>Monthly Flex</td>
<td>Pay-as-You-Go or Promo</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>MySQL Database VM Standard E2.1 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E2.2 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E2.4 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database BM Standard E2.64 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E2.8 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.1 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.16 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.2 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.24 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.32 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.36 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.4 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.64 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>MySQL Database VM Standard E3.8 instances</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>

**Monitoring Limits**

Monitoring limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Metrics (posted by services)</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

**Networking Limits**

Networking service limits apply to different scopes, depending on the resource.
## BYOIP Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOIP</td>
<td>Region</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

## Public IP Pool Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP pool</td>
<td>Region</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

## VCN and Subnet Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCN</td>
<td>Region</td>
<td>50</td>
<td>10</td>
</tr>
<tr>
<td>Subnets</td>
<td>VCN</td>
<td>300</td>
<td>300</td>
</tr>
</tbody>
</table>

## Gateway Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic routing gateways (DRGs)</td>
<td>Region</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Internet gateways</td>
<td>VCN</td>
<td>1*</td>
<td>1*</td>
</tr>
<tr>
<td>Local peering gateways (LPGs)</td>
<td>VCN</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>NAT gateways</td>
<td>VCN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Service gateways</td>
<td>VCN</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

* Limit for this resource cannot be increased

## IP Address Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved public IPs</td>
<td>Region</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Ephemeral public IPs</td>
<td>Instance</td>
<td>2 per VM instance 16 per bare metal instance</td>
<td>2 per VM instance 16 per bare metal instance</td>
</tr>
</tbody>
</table>

## DHCP Option Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP options</td>
<td>VCN</td>
<td>300</td>
<td>300</td>
</tr>
</tbody>
</table>
### Route Table Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route tables</td>
<td>VCN</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>Route rules</td>
<td>Route table</td>
<td>100*</td>
<td>100*</td>
</tr>
</tbody>
</table>

* Limit for this resource cannot be increased

### Network Security Group Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network security groups</td>
<td>VCN</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>VNICS</td>
<td>Network security group</td>
<td>A given network security group can have as many VNICS as are in the VCN. A given VNIC can belong to a maximum of 5 network security groups.*</td>
<td>A given network security group can have as many VNICS as are in the VCN. A given VNIC can belong to a maximum of 5 network security groups.*</td>
</tr>
<tr>
<td>Security rules</td>
<td>Network security group</td>
<td>120 (total ingress plus egress)</td>
<td>120 (total ingress plus egress)</td>
</tr>
</tbody>
</table>

* Limit for this resource cannot be increased

### Security List Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security lists</td>
<td>VCN</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>Security lists</td>
<td>Subnet</td>
<td>5*</td>
<td>5*</td>
</tr>
<tr>
<td>Security rules</td>
<td>Security list</td>
<td>200 ingress rules* and 200 egress rules*</td>
<td>200 ingress rules* and 200 egress rules*</td>
</tr>
</tbody>
</table>

* Limit for this resource cannot be increased

### IPSec VPN Connection Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec VPN connections</td>
<td>Region</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Customer-premises equipment objects (CPEs)</td>
<td>Region</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Dynamic routing gateways (DRGs)</td>
<td>Region</td>
<td>See Gateway Limits on page 228</td>
<td>See Gateway Limits on page 228</td>
</tr>
</tbody>
</table>
## FastConnect Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-connects</td>
<td>Region</td>
<td>Contact Us</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Virtual circuits</td>
<td>Region</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Dynamic routing gateways (DRGs)</td>
<td>Region</td>
<td>See Gateway Limits on page 228</td>
<td>See Gateway Limits on page 228</td>
</tr>
</tbody>
</table>

## VLAN Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANs</td>
<td>VCN</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

## NoSQL Database Cloud Limits

For Oracle NoSQL Database Cloud limits, see Service Limits.

## Notifications Limits

Notifications limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topics</td>
<td>50 (Active or Creating*) per tenancy</td>
<td>Contact Us</td>
</tr>
<tr>
<td>Subscriptions</td>
<td>10 (Active or Pending*) per topic</td>
<td>Contact Us</td>
</tr>
<tr>
<td></td>
<td>100 (Pending*) per tenancy</td>
<td></td>
</tr>
</tbody>
</table>

* A lifecycle state. See NotificationTopic Reference and Subscription Reference.

## Object Storage and Archive Storage Limits

Object Storage and Archive Storage limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>10,000 per tenancy</td>
<td>10,000 per tenancy</td>
</tr>
<tr>
<td>Objects per bucket</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

## Operations Insights Limits

Operations Insights limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database insights (ADBs) - Total OCPUs</td>
<td>800 cores</td>
<td>800 cores</td>
</tr>
</tbody>
</table>
# Registry Limits

Registry limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repositories</td>
<td>500 repositories per OCI region</td>
<td>500 repositories per OCI region</td>
</tr>
<tr>
<td>Images</td>
<td>100,000 images per repository</td>
<td>100,000 images per repository</td>
</tr>
<tr>
<td>Registry Storage</td>
<td>500 GB per OCI region or Contact Us</td>
<td>500 GB per OCI region or Contact Us</td>
</tr>
</tbody>
</table>

# Resource Manager Limits

Resource Manager limits are **regional**.

<table>
<thead>
<tr>
<th>Resource (per tenant)</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
<th>Always Free resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration source providers</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Jobs (concurrent)</td>
<td>10 (Job duration: 24 hours)</td>
<td>5 (Job duration: 24 hours)</td>
<td>2</td>
</tr>
<tr>
<td>Private templates</td>
<td>1000</td>
<td>100</td>
<td>10</td>
</tr>
<tr>
<td>Stacks</td>
<td>1000 (Variables per stack: 250, Size per variable: 8192 bytes, Zip file per stack: 11 MB)</td>
<td>100 (Variables per stack: 250, Size per variable: 8192 bytes, Zip file per stack: 11 MB)</td>
<td>10 (Variables per stack: 250, Size per variable: 8192 bytes, Zip file per stack: 11 MB)</td>
</tr>
</tbody>
</table>

# Service Connector Hub Limits

Service Connector Hub limits are **regional**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service connectors</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

# Streaming Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streams</td>
<td>Tenancy</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Stream pools</td>
<td>Tenancy</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Kafka connectors</td>
<td>Tenancy</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Partitions</td>
<td>Tenancy</td>
<td>5 or Contact Us</td>
<td>Contact Us</td>
</tr>
</tbody>
</table>
### Service Essentials

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum message retention period</td>
<td>Tenancy</td>
<td>7 days</td>
<td>7 days</td>
</tr>
<tr>
<td>Maximum message size</td>
<td>Tenancy</td>
<td>1 MB</td>
<td>1 MB</td>
</tr>
<tr>
<td>Maximum write rate</td>
<td>Partition</td>
<td>1 MB per second</td>
<td>1 MB per second</td>
</tr>
<tr>
<td>Maximum read rate</td>
<td>Partition</td>
<td>2 MB per second</td>
<td>2 MB per second</td>
</tr>
</tbody>
</table>

### Traffic Management Steering Policies Limits

Traffic Management Steering Policies limits are **global**.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>100 per tenant</td>
<td>100 per tenant</td>
</tr>
<tr>
<td>Attachments</td>
<td>1,000 per tenant</td>
<td>1,000 per tenant</td>
</tr>
</tbody>
</table>

### Vault Limits

Vault service limits apply to different scopes, depending on the resource.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Monthly or Annual Universal Credits</th>
<th>Always Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaults in a tenancy</td>
<td>10 or Contact Us</td>
<td>10 or Contact Us</td>
</tr>
<tr>
<td>Virtual private vaults in a tenancy</td>
<td>Contact Us</td>
<td>None</td>
</tr>
<tr>
<td>Resources</td>
<td>Monthly or Annual Universal Credits</td>
<td>Always Free</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Keys in a vault</td>
<td>1000 or <a href="#">Contact Us</a></td>
<td>100 (software-protected)</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td>20 (hardware-protected)</td>
</tr>
<tr>
<td></td>
<td>• Key versions can exist across a varying combination of keys or vaults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Key versions, whether enabled or disabled, count against your limits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When calculating usage for asymmetric keys, each key version increments the count by two when calculating usage against service limits in order to account for both the public key and the private key.</td>
<td></td>
</tr>
<tr>
<td>Resources</td>
<td>Monthly or Annual Universal Credits</td>
<td>Always Free</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Keys in a virtual private vault</td>
<td>1000 or Contact Us</td>
<td>None</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Key versions can exist across a varying combination of keys or vaults.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Key versions, whether enabled or disabled, count against your limits.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• When calculating usage for asymmetric keys, each key version increments the count by two when calculating usage against service limits in order to account for both the public key and the private key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secrets in a tenancy</td>
<td>5000 or Contact Us</td>
<td>150</td>
</tr>
<tr>
<td>(Secret versions, regardless of rotation state, count against your limits. All secret versions can be in one vault or spread across the allowable number of vaults.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secret versions in a secret</td>
<td>50 or Contact Us</td>
<td>40</td>
</tr>
<tr>
<td>(You can have up to 30 secret versions in active use and 20 secret versions pending deletion.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**VMware Solution Limits**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDCs</td>
<td>Region</td>
<td>Not applicable</td>
<td>Not available</td>
</tr>
<tr>
<td>ESXi hosts</td>
<td>Region</td>
<td>52 cores per host</td>
<td>Not available</td>
</tr>
</tbody>
</table>

**WAF Limits**

WAF limits are global.
### Service Logs

You can enable service logs for some resources. Service logs provide diagnostic information about the resources in your tenancy. When you enable logging on resources, you receive information about the resource in a log file. This information allows you to analyze, optimize, and troubleshoot your resources.

#### Working with Service Logs

Not all resources support Logging. See Supported Services for the list of services with resources that produce logs.

To enable logs on a resource, you must have permission to update the resource and permission to create the log in the log group. See Required Permissions for Working with Logs and Log Groups, and Enabling Logging for a Resource on page 2591.

For more information about Logging, see Overview of the Logging Service.

#### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To enable logging for a resource using the API, use the appropriate resource's create or update operation.

- Logging Management API
- Logging Ingestion API
- Logging Search API

#### Viewing All Resources in a Compartment

This topic describes how you can use the tenancy explorer to get a cross-region view of all resources in a compartment.

#### Tenancy Explorer Highlights

- The tenancy explorer lets you view all your resources in a compartment, across all regions in your tenancy.
- You can choose to view just the resources that reside in the selected compartment, or you can choose to view all the resources in all the subcompartments as well, to get a full view of the compartment tree.
- You can take actions on resources from the tenancy explorer. You can delete or move a single or multiple resources at a time. The tenancy explorer is a convenient option when you need to perform bulk delete or move actions on multiple resources.

The following image highlights these features:
When using the tenancy explorer, be aware of the following:

- If you recently created a resource, it might not show up in the tenancy explorer immediately. Similarly, if you recently updated a resource, your changes might not immediately appear.
- You must be in the same region as the resource to navigate to its details page. The tenancy explorer displays the resource's region. Use the region selector at the top of the Console to change to the same region as the resource to enable these actions.
- When taking bulk actions, you can monitor progress on the Work Requests page.

**Work Requests**

Tenancy explorer is one of the Oracle Cloud Infrastructure features that is integrated with the Work Requests API. For general information on using work requests in Oracle Cloud Infrastructure, see Work Requests in the user guide, and the Work Requests API.

**Resources Supported by the Tenancy Explorer**

The tenancy explorer is powered by the Search service and supports the same resource types. Most resources are supported.

**Supported resources**

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Migration</td>
<td>amsmigration</td>
<td>See Migration Reference</td>
</tr>
<tr>
<td>Application Migration</td>
<td>amssource</td>
<td>See Source Reference.</td>
</tr>
<tr>
<td>Analytics Cloud</td>
<td>analyticsinstance</td>
<td>See AnalyticsInstance Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apideployment</td>
<td>See Deployment Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apigateway</td>
<td>See Gateway Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apigatewayapi</td>
<td>See Api Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apigatewaycertificate</td>
<td>See Certificate Reference.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Big Data</td>
<td>bigdataservice</td>
<td>See BdsInstance Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>bootvolume</td>
<td>See BootVolume Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>bootvolumebackup</td>
<td>See BootVolumeBackup Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volume</td>
<td>See Volume Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumebackup</td>
<td>See VolumeBackup Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumegroup</td>
<td>See VolumeGroup Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumegroupbackup</td>
<td>See VolumeGroupBackup Reference.</td>
</tr>
<tr>
<td>Blockchain Platform</td>
<td>blockchainplatforms</td>
<td>See BlockchainPlatform Reference.</td>
</tr>
<tr>
<td>Budgets</td>
<td>budget</td>
<td>See Budget Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguarddetectorrecipe</td>
<td>See DetectorRecipe Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguardmanagedlist</td>
<td>See ManagedList Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguardresponderrecipe</td>
<td>See ResponderRecipe Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguardtarget</td>
<td>See Target Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>autoscalingconfiguration</td>
<td>See AutoScalingConfiguration Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Queries for the policies attribute are not supported.</td>
</tr>
<tr>
<td>Compute</td>
<td>clusternetwork</td>
<td>See ClusterNetwork Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Queries for the primarySubnetId, secondaryVnicSubnets, and timeUpdated attributes are not supported.</td>
</tr>
<tr>
<td>Compute</td>
<td>consolehistory</td>
<td>See ConsoleHistory Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>dedicatedvmhost</td>
<td>See DedicatedVmHost Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>image</td>
<td>See Image Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>instance</td>
<td>See Instance Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Queries for the privateIp or publicIp attribute of a vnic will include the related instance, if one exists, and is running, in the query results.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compute</td>
<td>instanceconfiguration</td>
<td>See InstanceConfiguration Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>instancepool</td>
<td>See InstancePool Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Queries for the primarySubnetId, faultDomains, secondaryVnicSubnets, and loadBalancers attributes are not supported.</td>
</tr>
<tr>
<td>Content and Experience</td>
<td>oceinstance</td>
<td>See OceInstance Reference.</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>datacatalog</td>
<td>See Catalog Reference.</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>datacatalogprivateendpoint</td>
<td>See CatalogPrivateEndpoint Reference.</td>
</tr>
<tr>
<td>Data Flow</td>
<td>application</td>
<td>See Application Reference.</td>
</tr>
<tr>
<td>Data Flow</td>
<td>run</td>
<td>See Run Reference.</td>
</tr>
<tr>
<td>Data Integration</td>
<td>disworkspace</td>
<td>See Workspace Reference.</td>
</tr>
<tr>
<td>Data Safe</td>
<td>datasafeprivateendpoint</td>
<td>See DataSafePrivateEndpoint Reference.</td>
</tr>
<tr>
<td>Data Science</td>
<td>datasciencemodel</td>
<td>See Model Reference.</td>
</tr>
<tr>
<td>Data Science</td>
<td>datasciencenotebooksession</td>
<td>See NotebookSession Reference.</td>
</tr>
<tr>
<td>Data Science</td>
<td>datascienceproject</td>
<td>See Project Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomouscontainerdatabase</td>
<td>See AutonomousContainerDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomousdatabase</td>
<td>See AutonomousDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomousexadatainfrastru</td>
<td>See AutonomousExadataInfrastructure Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomousvmcluster</td>
<td>See AutonomousVmCluster Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>backupdestination</td>
<td>See BackupDestination Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>cloudexadatainfrastru</td>
<td>See CloudExadataInfrastructure Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>cloudvmcluster</td>
<td>See CloudVmCluster Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>database</td>
<td>See Database Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>dbhome</td>
<td>See DbHome Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>dbsystem</td>
<td>See DbSystem Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>exadatainfrastru</td>
<td>See ExadataInfrastructure Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externalcontainerdatabase</td>
<td>See ExternalContainerDatabase Reference.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database</td>
<td>externaldatabaseconnector</td>
<td>See ExternalDatabaseConnector Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externalnoncontainerdatabase</td>
<td>See ExternalNonContainerDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externalpluggabledatabase</td>
<td>See ExternalPluggableDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>vmcluster</td>
<td>See VmCluster Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>vmclusternetwork</td>
<td>See VmClusterNetwork Reference.</td>
</tr>
<tr>
<td>Digital Assistant</td>
<td>odainstance</td>
<td>See OdaInstance Reference.</td>
</tr>
<tr>
<td>Email Delivery</td>
<td>emailsender</td>
<td>See Sender Reference.</td>
</tr>
<tr>
<td>Events</td>
<td>eventrule</td>
<td>See Rule Reference.</td>
</tr>
<tr>
<td>File Storage</td>
<td>filesystem</td>
<td>See FileSystem Reference.</td>
</tr>
<tr>
<td>File Storage</td>
<td>mounttarget</td>
<td>See MountTarget Reference.</td>
</tr>
<tr>
<td>Functions</td>
<td>functionsapplication</td>
<td>See Application Reference.</td>
</tr>
<tr>
<td>Functions</td>
<td>functionsfunction</td>
<td>See Function Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>compartment</td>
<td>See Compartment Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>group</td>
<td>See Group Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>identityprovider</td>
<td>See IdentityProvider Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>policy</td>
<td>See Policy Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>tagdefault</td>
<td>See TagDefault Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>tagnamespace</td>
<td>See TagNamespace Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>user</td>
<td>See User Reference.</td>
</tr>
<tr>
<td>Integration Cloud</td>
<td>integrationinstance</td>
<td>See IntegrationInstance Reference.</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>loadbalancer</td>
<td>See LoadBalancer Reference.</td>
</tr>
<tr>
<td>Management Agent</td>
<td>management-agents</td>
<td>See ManagementAgent Reference.</td>
</tr>
<tr>
<td>Management Agent</td>
<td>management-agent-install-keys</td>
<td>See ManagementAgentInstallKey Reference.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>alarm</td>
<td>See Search-Supported Attributes for Alarms on page 2664.</td>
</tr>
<tr>
<td>MySQL Database</td>
<td>dbsystem</td>
<td>See DBSystem Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>byoiprange</td>
<td>See ByoipRange Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>cpe</td>
<td>See Cpe Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>crossconnect</td>
<td>See CrossConnect Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>crossconnectgroup</td>
<td>See CrossConnectGroup Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>dhcpoptions</td>
<td>See DhcpOptions Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>drg</td>
<td>See Drg Reference.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Networking</td>
<td>internetgateway</td>
<td>See InternetGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>ipseccconnection</td>
<td>See IPSecConnection Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>ipv6</td>
<td>See IPv6 Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>localpeeringgateway</td>
<td>See LocalPeeringGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>natgateway</td>
<td>See NatGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>networksecuritygroup</td>
<td>See NetworkSecurityGroup Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>publicip</td>
<td>See PublicIp Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>publicippool</td>
<td>See PublicIpPool Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>privateip</td>
<td>See PrivateIp Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>remotepeeringconnection</td>
<td>See RemotePeeringConnection Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>routetable</td>
<td>See RouteTable Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>servicegateway</td>
<td>See ServiceGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>subnet</td>
<td>See Subnet Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>vcn</td>
<td>See Vcn Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>virtualcircuit</td>
<td>See VirtualCircuit Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>vnic</td>
<td>See Vnic Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Queries for the privateIp or publicIp attribute of a vnic will include the related instance, if one exists and is running, in the query results.</td>
</tr>
<tr>
<td>NoSQL Database Cloud</td>
<td>table</td>
<td>See Table Reference.</td>
</tr>
<tr>
<td>Notifications</td>
<td>onssubscription</td>
<td>See Subscription Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Queries for the endpoint attribute are not supported.</td>
</tr>
<tr>
<td>Notifications</td>
<td>onstopic</td>
<td>See NotificationTopic Reference.</td>
</tr>
<tr>
<td>Object Storage</td>
<td>bucket</td>
<td>See Bucket Reference.</td>
</tr>
<tr>
<td>OS Management</td>
<td>osmsmanagedinstancegroup</td>
<td>See ManagedInstanceGroup Reference.</td>
</tr>
<tr>
<td>OS Management</td>
<td>osmsscheduledjob</td>
<td>See ScheduledJob Reference.</td>
</tr>
<tr>
<td>OS Management</td>
<td>osmssoftwaresource</td>
<td>See SoftwareSource Reference.</td>
</tr>
<tr>
<td>Registry</td>
<td>containerimage</td>
<td>See ContainerImage Reference.</td>
</tr>
</tbody>
</table>
### Service Essentials

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry</td>
<td>containerrepository</td>
<td>See ContainerRepository Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormconfigsourceprovider</td>
<td>See ConfigurationSourceProvider Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormjob</td>
<td>See Job Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormstack</td>
<td>See Stack Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormtemplate</td>
<td>See Template Reference.</td>
</tr>
<tr>
<td>Service Connector Hub</td>
<td>serviceconnector</td>
<td>See ServiceConnector Reference.</td>
</tr>
<tr>
<td>Service Limits</td>
<td>quota</td>
<td>See Quota Reference.</td>
</tr>
<tr>
<td>Streaming</td>
<td>connectharness</td>
<td>See ConnectHarness Reference.</td>
</tr>
<tr>
<td>Streaming</td>
<td>stream</td>
<td>See Stream Reference.</td>
</tr>
<tr>
<td>Vault</td>
<td>key</td>
<td>See Key Reference.</td>
</tr>
<tr>
<td>Vault</td>
<td>vault</td>
<td>See Vault Reference.</td>
</tr>
<tr>
<td>Vault</td>
<td>vaultsecret</td>
<td>See Secret Reference.</td>
</tr>
<tr>
<td>VMware solution</td>
<td>vmwareesxihost</td>
<td>See EsxiHost Reference.</td>
</tr>
<tr>
<td>VMware solution</td>
<td>vmwaresddc</td>
<td>See Sddc Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>httpredirect</td>
<td>See HttpRedirect Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waasaddresslist</td>
<td>See AddressList Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waascertificate</td>
<td>See Certificate Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waascustomprotectionrule</td>
<td>See CustomProtectionRule Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waaspolicy</td>
<td>See WaasPolicy Reference.</td>
</tr>
</tbody>
</table>

### Required IAM Policy to Work with Resources in the Tenancy Explorer

The resources that you see in the tenancy explorer depend on the permissions you have in place for the resource type.

You do not necessarily see results for everything in the compartment. For example, if your user account is not associated with a policy that grants you the ability to, at a minimum, inspect the instance resource type, then you can't view instances in the tenancy explorer. For more information about policies, see How Policies Work on page 2136. For information about the permissions required for the list API operation for a specific resource type, see the Policy Reference on page 2167 for the appropriate service.

### Required Permissions to View Work Requests

Work requests inherit the permissions of the operation that spawns the work request. So if you have the permissions to move or delete a resource, you also have permission to see the work requests associated with this action.

To enable users to list all work requests in a tenancy, use a policy like the following:

`Allow group <My_Group> to inspect work-requests in tenancy`

### Navigating to the Tenancy Explorer and Viewing Resources

Open the navigation menu. Under Governance and Administration, go to Governance and click Tenancy Explorer.
The tenancy explorer opens with a view of the root compartment. Select the compartment you want to explore from the compartment picker on the left side of the Console. After you select a compartment, the resources that you have permission to view are displayed. The **Name** and **Description** of the compartment you are viewing are displayed at the top of the page. To also list all resources in the subcompartments of the selected compartment, select **Show resources in subcompartments**. When viewing resources in all subcompartments, it is helpful to use the **Compartment** column in the results list to see the compartment hierarchy where the resource resides.

**Filtering Displayed Resources**

To view only specific resource types, select the resource types you are interested in from the **Filter by resource type** menu. You can select multiple resources to include in the filtered list. You can also filter the list by tags.

**Opening the Resource Details Page**

Detail page navigation is not supported for all resource types. If detail page navigation is not supported, the resource name does not display as a link and the option is grayed out on the Actions menu.

To open the details page for a resource:

1. Locate the resource in the list.
2. Verify that you are in the same region as the resource. The resource's region is listed in the tenancy explorer results. If it is not the same as the region you are currently in (shown at the top of the Console), then select the appropriate region from the **Regions** menu.
3. To open the details page, you can either:
   - Click the name.
   - Click the the Actions icon (three dots) and select **View Details**.

**Moving Resources to a Different Compartment**

Not all resource-types can be moved to a different compartment. If the resource cannot be moved, the option is not selectable on the Actions menu. You must have the appropriate permissions for the resources you want to move in both the original and destination compartments.

**Important:**

Ensure that you understand the impact of moving a resource before you perform this action. See the resource's service documentation for details.

**To move a single resource to a different compartment**

1. Locate the resource in the list.
2. Click the the Actions icon (three dots) and select **Move Resource**.
3. In the dialog, choose the destination compartment from the list.
4. Click **Move Resource**.

**To move multiple resources to a different compartment**

To move multiple resources, the resources must be in the same compartment.

1. Locate and select the resources in the list.
2. Click **Move Selected**.
3. In the dialog, choose the destination compartment from the list.
4. Click **Move Resource**.

The Work Request page launches to show you the status of the work request to move the resources.
Deleting Resources

Not all resource-types can be deleted using the tenancy explorer. If delete is not supported, the option is not selectable on the Actions menu.

Also, if a resource is in use by another resource, you can't delete it. For example, to delete a VCN, it must first be empty and have no related resources or attached gateways.

To delete a single resource

1. Locate the resource in the list.
2. Click the Actions icon (three dots) and select Delete.
3. In the confirmation dialog, click Delete.
4. You are taken to the details page for the deleted resource.

To delete multiple resources

To delete multiple resources, the resources must be in the same compartment.

1. Locate and select the resources in the list.
2. Click Delete Selected.
3. In the confirmation dialog, click Delete.

The Work Request page launches to show you the status of the work request to move the resources.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to move or delete multiple resources at once:

- ListBulkActionResourceTypes - use this API to help you provide the correct resource-type information to the BulkDeleteResources and BulkMoveResources operations. The returned list of resource-types provides the appropriate resource-type name to use as input and the required identifying information for each resource-type. Most resource-types only require the OCID to identity a specific resource, but some resources, such as buckets, require you to provide other identifying information.
- BulkDeleteResources
- BulkMoveResources

Compartment Quotas

This topic describes compartment quotas for Oracle Cloud Infrastructure.

Compartment quotas give tenant and compartment administrators better control over how resources are consumed in Oracle Cloud Infrastructure, enabling administrators to easily allocate resources to compartments using the Console. Along with compartment budgets, compartment quotas create a powerful toolset to manage your spending in Oracle Cloud Infrastructure tenancies.

You can start using compartment quotas from any compartment detail page in the Console.

About Compartment Quotas

Compartment quotas are similar to Service Limits on page 215. The biggest difference is that service limits are set by Oracle, and compartment quotas are set by administrators, using policies that allow them to allocate resources with a high level of flexibility.

Compartment quotas are set using policy statements written in a simple declarative language that is similar to the IAM policy language.
There are three types of quota policy statements:

- **set** - sets the maximum number of a cloud resource that can be used for a compartment
- **unset** - resets quotas back to the default service limits
- **zero** - removes access to a cloud resource for a compartment

The quota policy statements look like this:

```
<table>
<thead>
<tr>
<th>Set statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set family quota name to value in location conditions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unset statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unset family quota name in location conditions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zero statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero family quota name in location conditions</td>
</tr>
</tbody>
</table>
```

The language components for a quota policy statement are:

- The **action** keyword, which corresponds to the type of quota being defined. This can be set, unset, or zero.
- The name of the service family; for example: compute-core.
- The **quota** or **quotas** keyword.
- The name of the quota, which varies by service family. For example, a valid quota in the compute-core family is standard2-core-count.
  - You can also use wildcards to specify a range of names. For example, "/standard*/" matches all Compute quotas that start with the phrase "standard."
- For set statements, the value of the quota.
- The compartment that the quota covers.
- An optional condition. For example where request.region = 'us-phoenix-1'. Currently supported conditionals are request.region and request.ad.

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For common policies used to authorize users, see Common Policies on page 2142. To manage quotas in a compartment, you must belong to a group that has the correct permissions. For example:

```
allow group QuotaAdmins to { QUOTA_READ, QUOTA_CREATE, QUOTA_DELETE, QUOTA_UPDATE, QUOTA_INSPECT } in tenancy
```

For in-depth information on granting users permissions for the Quotas service, see Details for the Quotas Service in the IAM policy reference.
Permissions and Nesting

Compartment quotas can be set on the root compartment. An administrator (who must be able to manage quotas on the root compartment) can set quotas on their own compartments and any child compartments. Quotas set on a parent compartment override quotas set on child compartments. This way, an administrator of a parent compartment can create a quota on a child compartment that cannot be overridden by the child.

Scope

Quotas can have different scopes, and work at the availability domain, the region, or globally. There are a few important things to understand about scope when working with compartment quotas:

- When setting a quota at the availability domain (AD) level, the quota is allocated to each AD. So, for example, setting a quota of 120 X7 OCPUs on a compartment actually sets a limit of 120 OCPUs per AD. To target a specific AD, use the request.ad parameter in the where clause.
- Regional quotas apply to each region. For example, if a quota of 10 functions is set on a compartment, 10 functions will be allocated per region. To target a specific region, use the request.region parameter in the where clause.
- Usage for sub-compartment counts towards usage for the main compartment.

For more information, see Regions and Availability Domains on page 180.

Quota Evaluation and Precedence

The following rules apply when quota statements are evaluated:

- Within a policy, quota statements are evaluated in order, and later statements supersede previous statements that target the same resource.
- In cases where more than one policy is set for the same resource, the most restrictive policy is applied.
- Service limits always take precedence over quotas. Although it is possible to specify a quota for a resource that exceeds the service limit for that resource, the service limit will still be enforced.

Usage Examples

The following example sets the quota for VM.Standard2 and BM.Standard2 compute series to 240 OCPUs (cores) in each AD on compartment MyCompartment in the US West (Phoenix) region:

```bash
set compute-core quota standard2-core-count to 240 in compartment MyCompartment
where request.region = us-phoenix-1
```

The next example shows how to make an allowlist, setting every quota in a family to zero and then explicitly allocating resources:

```bash
zero compute-core quotas in tenancy
set compute-core quota standard2-core-count to 240 in tenancy
```

This example shows how to limit creating dense I/O compute resources to only one region:

```bash
zero compute-core quotas / *dense-io*/ in tenancy
set compute-core quota / *dense-io*/ to 48 in tenancy
where request.region = us-phoenix-1
```

You can clear quotas by using an unset statement, which removes the quota for a resource - any limits on this resource will now be enforced by the service limits:

```bash
zero compute-core quotas in tenancy
unset compute-core quota standard2-core-count in tenancy
```

Using the Console

To create a quota

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Quota Policies.
2. On the Quota Policies screen, click Create Quota.
3. Enter the following:
   - Enter a name for your quota in the **Name** field. Avoid entering confidential information.
   - Enter a description for your quota in the **Description** field.
   - Enter a quota policy string in the **Quota Policy** field.

4. Click **Create Quota Policy**.

   **Note:**
   New policies can take up to 10 minutes to start working.

**To edit a quota**

1. On the **Quota Policies** screen, click the quota you want to edit to display the quota policy details page, then click the **Edit Quota** button.
2. Edit the quota.
3. Click **Save Changes**.

**To delete a quota**

1. There are two ways to delete a quota from the console:
   - On the main **Quota Policies** page, click the context menu to the right of the quota you want to delete, then select **Delete**.
   - Click the quota you want to delete, then from the quota policy detail page click **Delete**.
2. From the **Confirm Delete** dialog, click **Delete** or **Cancel**.

**Available Quotas by Service**

**Analytics Cloud**

For Analytics Cloud quotas and examples, see **Service Quotas**.

**Big Data**

For Big Data quotas and examples, see **Service Quotas**.

**Block Volume Quotas**

Family name: `block-storage`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup-count</td>
<td>Regional</td>
<td>Total number of block and boot volume backups</td>
</tr>
<tr>
<td>total-storage-gb</td>
<td>Availability domain</td>
<td>Maximum storage space of block and boot volumes, in GB</td>
</tr>
<tr>
<td>volume-count</td>
<td>Availability domain</td>
<td>Total number of block and boot volumes</td>
</tr>
</tbody>
</table>

**Example**

```bash
set block-storage quota volume-count to 10 in compartment MyCompartment
```

**Blockchain Platform Quotas**

For Blockchain Platform quotas and examples, see **Service Quotas**.
Compute Quotas

Compute Instances

Quotas for Compute instances are available per core (OCPU) and per shape.

Core-Based Quotas

Family name: compute-core

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard1-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.Standard1 and BM.Standard1 series</td>
</tr>
<tr>
<td>standard-b1-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.Standard.B1 and BM.Standard.B1 series</td>
</tr>
<tr>
<td>standard2-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.Standard2 and BM.Standard2 series</td>
</tr>
<tr>
<td>standard-e2-micro-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.Standard.E2.1.Micro series</td>
</tr>
<tr>
<td>standard-e2-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.Standard.E2 and BM.Standard.E2 series</td>
</tr>
<tr>
<td>standard-e3-core-ad-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.Standard.E3 and BM.Standard.E3 series</td>
</tr>
<tr>
<td>dense-io1-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.DenseIO1 and BM.DenseIO1 series</td>
</tr>
<tr>
<td>dense-io2-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the VM.DenseIO2 and BM.DenseIO2 series</td>
</tr>
<tr>
<td>gpu2-count</td>
<td>Availability</td>
<td>Total number of GPUs for shapes in the VM.GPU2 and BM.GPU2 series</td>
</tr>
<tr>
<td>gpu3-count</td>
<td>Availability</td>
<td>Total number of GPUs for shapes in the VM.GPU3 and BM.GPU3 series</td>
</tr>
<tr>
<td>gpu4-count</td>
<td>Availability</td>
<td>Total number of GPUs for shapes in the BM.GPU4 series</td>
</tr>
<tr>
<td>hpc2-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for shapes in the BM.HPC2 series</td>
</tr>
<tr>
<td>dvh-standard2-core-count</td>
<td>Availability</td>
<td>Total number of OCPUs for DVH.Standard2.52 shapes</td>
</tr>
</tbody>
</table>

Example

```
set compute-core quota standard2-core-count to 480 in compartment MyCompartment
```

Shape-Based Quotas

Family name: compute
<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bm-standard1-36-count</td>
<td>Availability domain</td>
<td>Number of BM.Standard1.36 instances</td>
</tr>
<tr>
<td>bm-standard-b1-44-count</td>
<td>Availability domain</td>
<td>Number of BM.Standard.B1.44 instances</td>
</tr>
<tr>
<td>bm-standard2-52-count</td>
<td>Availability domain</td>
<td>Number of BM.Standard2.52 instances</td>
</tr>
<tr>
<td>bm-standard-e2-64-count</td>
<td>Availability domain</td>
<td>Number of BM.Standard.E2.64 instances</td>
</tr>
<tr>
<td>bm-dense-io1-36-count</td>
<td>Availability domain</td>
<td>Number of BM.DenseIO1.36 instances</td>
</tr>
<tr>
<td>bm-dense-io2-52-count</td>
<td>Availability domain</td>
<td>Number of BM.DenseIO2.52 instances</td>
</tr>
<tr>
<td>bm-gpu2-2-count</td>
<td>Availability domain</td>
<td>Number of BM.GPU2.2 instances</td>
</tr>
<tr>
<td>bm-gpu3-8-count</td>
<td>Availability domain</td>
<td>Number of BM.GPU3.8 instances</td>
</tr>
<tr>
<td>bm-hpc2-36-count</td>
<td>Availability domain</td>
<td>Number of BM.HPC2.36 instances</td>
</tr>
<tr>
<td>vm-standard1-1-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard1.1 instances</td>
</tr>
<tr>
<td>vm-standard1-2-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard1.2 instances</td>
</tr>
<tr>
<td>vm-standard1-4-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard1.4 instances</td>
</tr>
<tr>
<td>vm-standard1-8-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard1.8 instances</td>
</tr>
<tr>
<td>vm-standard1-16-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard1.16 instances</td>
</tr>
<tr>
<td>vm-standard2-1-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.1 instances</td>
</tr>
<tr>
<td>vm-standard2-2-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.2 instances</td>
</tr>
<tr>
<td>vm-standard2-4-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.4 instances</td>
</tr>
<tr>
<td>vm-standard2-8-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.8 instances</td>
</tr>
<tr>
<td>vm-standard2-16-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.16 instances</td>
</tr>
<tr>
<td>vm-standard2-24-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.24 instances</td>
</tr>
<tr>
<td>vm-standard-e2-1-micro-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard.E2.1.Micro instances</td>
</tr>
<tr>
<td>Name</td>
<td>Scope</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>vm-standard-e2-1-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard.E2.1 instances</td>
</tr>
<tr>
<td>vm-standard-e2-2-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard.E2.2 instances</td>
</tr>
<tr>
<td>vm-standard-e2-4-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard.E2.4 instances</td>
</tr>
<tr>
<td>vm-standard-e2-8-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard.E2.8 instances</td>
</tr>
<tr>
<td>standard-e3-core-ad-count</td>
<td>Availability domain</td>
<td>Total number of OCPUs for shapes in the VM.Standard.E3 and BM.Standard.E3 series</td>
</tr>
<tr>
<td>vm-dense-io1-4-count</td>
<td>Availability domain</td>
<td>Number of VM.DenseIO1.4 instances</td>
</tr>
<tr>
<td>vm-dense-io1-8-count</td>
<td>Availability domain</td>
<td>Number of VM.DenseIO1.8 instances</td>
</tr>
<tr>
<td>vm-dense-io1-16-count</td>
<td>Availability domain</td>
<td>Number of VM.DenseIO1.16 instances</td>
</tr>
<tr>
<td>vm-dense-io2-8-count</td>
<td>Availability domain</td>
<td>Number of VM.DenseIO2.8 instances</td>
</tr>
<tr>
<td>vm-dense-io2-16-count</td>
<td>Availability domain</td>
<td>Number of VM.DenseIO2.16 instances</td>
</tr>
<tr>
<td>vm-dense-io2-24-count</td>
<td>Availability domain</td>
<td>Number of VM.DenseIO2.24 instances</td>
</tr>
<tr>
<td>vm-gpu2-1-count</td>
<td>Availability domain</td>
<td>Number of VM.GPU2.1 instances</td>
</tr>
<tr>
<td>vm-gpu3-1-count</td>
<td>Availability domain</td>
<td>Number of VM.GPU3.1 instances</td>
</tr>
<tr>
<td>vm-gpu3-2-count</td>
<td>Availability domain</td>
<td>Number of VM.GPU3.2 instances</td>
</tr>
<tr>
<td>vm-gpu3-4-count</td>
<td>Availability domain</td>
<td>Number of VM.GPU3.4 instances</td>
</tr>
<tr>
<td>dvh-standard2-52-count</td>
<td>Availability domain</td>
<td>Number of DVH.Standard2.52 instances</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
set compute quota vm-dense-io2-8-count to 10 in compartment MyCompartment where request.ad = 'us-phoenix-1-ad-2'
```

**Custom Images**

Family name: `compute`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom-image-count</td>
<td>Regional</td>
<td>Number of custom images</td>
</tr>
</tbody>
</table>
Example

```
set compute quota custom-image-count to 15 in compartment MyCompartment
```

**Instance Configurations, Instance Pools, and Cluster Networks**

Family name: `compute-management`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-network-count</td>
<td>Regional</td>
<td>Number of cluster networks</td>
</tr>
<tr>
<td>config-count</td>
<td>Regional</td>
<td>Number of instance configurations</td>
</tr>
<tr>
<td>pool-count</td>
<td>Regional</td>
<td>Number of instance pools</td>
</tr>
</tbody>
</table>

Example

```
set compute-management quota config-count to 10 in compartment MyCompartment
```

**Autoscaling**

Family name: `auto-scaling`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-count</td>
<td>Regional</td>
<td>Number of autoscaling configurations</td>
</tr>
</tbody>
</table>

Example

```
Set auto-scaling quota config-count to 10 in compartment MyCompartment
```

**Content and Experience Quotas**

For Content and Experience quotas and examples, see [Service Quotas](#).

**Data Catalog Quotas**

Family name: `data-catalog`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>catalog-count</td>
<td>Regional</td>
<td>Number of data catalogs</td>
</tr>
</tbody>
</table>

Example

```
set data-catalog quota catalog-count to 1 in compartment <MyCompartment>
```

**Data Integration Quotas**

Family name: `dataintegration`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workspace-count</td>
<td>Regional</td>
<td>Number of workspaces</td>
</tr>
</tbody>
</table>

Example

```
set dataintegration quota workspace-count to 1 in compartment <MyCompartment>
```
Example

```
set dataintegration quota workspace-count to 10 in compartment <compartment_name>
```

### Data Science Quotas

Family name: data-science

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds-block-volume-count</td>
<td>Regional</td>
<td>Number of block volumes</td>
</tr>
<tr>
<td>ds-block-volume-gb</td>
<td>Regional</td>
<td>Block Volume Size in GB</td>
</tr>
<tr>
<td>ds-gpu2-count</td>
<td>Regional</td>
<td>GPUs for VM.GPU2</td>
</tr>
<tr>
<td>ds-gpu3-count</td>
<td>Regional</td>
<td>GPUs for VM.GPU3</td>
</tr>
<tr>
<td>ds-standard2-core-regional-count</td>
<td>Regional</td>
<td>Number of VM.Standard2 cores</td>
</tr>
<tr>
<td>ds-standard-e2-core-regional-count</td>
<td>Regional</td>
<td>Number of VM.Standard E2 cores</td>
</tr>
<tr>
<td>model-count</td>
<td>Regional</td>
<td>Number of models</td>
</tr>
<tr>
<td>notebook-session-count</td>
<td>Regional</td>
<td>Number of notebook sessions</td>
</tr>
<tr>
<td>project-count</td>
<td>Regional</td>
<td>Number of projects</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to limit the number of data science projects in a specified compartment:

```
set data-science quota project-count to 10 in compartment MyCompartment
```

### Data Transfer Quotas

Family name: data-transfer

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-appliance-count</td>
<td>Regional</td>
<td>Number of approved transfer appliances</td>
</tr>
<tr>
<td>appliance-count</td>
<td>Regional</td>
<td>Number of transfer appliances</td>
</tr>
<tr>
<td>job-count</td>
<td>Regional</td>
<td>Number of transfer jobs</td>
</tr>
</tbody>
</table>

**Example**

```
zero data-transfer quota job-count in tenancy
set data-transfer quota job-count to 1 in compartment Finance
set data-transfer quota appliance-count to 3 in compartment Finance
```
# Database Quotas

Family name: database

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adb-free-count</td>
<td>Regional</td>
<td>Number of Always Free Autonomous Databases. Tenancies can have a total of two Always Free Autonomous Databases, and these resources must be provisioned in the home region. For each database, you can choose the workload type (Autonomous Transaction Processing or Autonomous Data Warehouse).</td>
</tr>
<tr>
<td>adw-dedicated-ocpu-count</td>
<td>Availability domain</td>
<td>Number of Autonomous Data Warehouse OCPUs for databases using dedicated Exadata infrastructure. (See note about &quot;n/a&quot; values on the Limits, Quotas and Usage page of the Console.)</td>
</tr>
<tr>
<td>adw-dedicated-total-storage-tb</td>
<td>Availability domain</td>
<td>Amount of storage (in TB) for Autonomous Data Warehouse databases using dedicated Exadata infrastructure. (See note following this table about &quot;n/a&quot; values on the Limits, Quotas and Usage page of the Console.)</td>
</tr>
<tr>
<td>adw-ocpu-count</td>
<td>Regional</td>
<td>Number of Autonomous Data Warehouse OCPUs for databases using shared Exadata infrastructure.</td>
</tr>
<tr>
<td>adw-total-storage-tb</td>
<td>Regional</td>
<td>Amount of storage (in TB) for Autonomous Data Warehouse databases using shared Exadata infrastructure.</td>
</tr>
<tr>
<td>atp-dedicated-ocpu-count</td>
<td>Availability domain</td>
<td>Number of Autonomous Data Warehouse OCPUs for databases using dedicated Exadata infrastructure. (See note following this table about &quot;n/a&quot; values on the Limits, Quotas and Usage page of the Console.)</td>
</tr>
<tr>
<td>atp-dedicated-total-storage-tb</td>
<td>Availability domain</td>
<td>Amount of storage (in TB) for Autonomous Transaction Processing databases using dedicated Exadata infrastructure. (See note following this table about &quot;n/a&quot; values on the Limits, Quotas and Usage page of the Console.)</td>
</tr>
<tr>
<td>atp-ocpu-count</td>
<td>Regional</td>
<td>Number of Autonomous Transaction Processing OCPUs for databases using shared Exadata infrastructure.</td>
</tr>
<tr>
<td>atp-total-storage-tb</td>
<td>Regional</td>
<td>Amount of storage (in TB) for Autonomous Transaction Processing databases using shared Exadata infrastructure.</td>
</tr>
<tr>
<td>bm-dense-io1-36-count</td>
<td>Availability domain</td>
<td>Number of BM.DenseIO1.36 DB systems</td>
</tr>
<tr>
<td>bm-dense-io2-52-count</td>
<td>Availability domain</td>
<td>Number of BM.DenseIO2.52 DB systems</td>
</tr>
<tr>
<td>exadata-base-48-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Base.48 DB systems</td>
</tr>
<tr>
<td>exadata-full1-336-x6-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Full1.336 - X6 DB systems</td>
</tr>
<tr>
<td>exadata-full2-368-x7-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Full2.368 - X7 DB systems and Autonomous Exadata Infrastructure</td>
</tr>
<tr>
<td>exadata-half1-168-x6-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Half1.168 - X6 DB systems</td>
</tr>
<tr>
<td>Name</td>
<td>Scope</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exadata-half2-184-x7-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Half2.184 - X7 DB systems and Autonomous Exadata Infrastructure</td>
</tr>
<tr>
<td>exadata-quarter1-84-x6-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Quarter1.84 - X6 DB systems</td>
</tr>
<tr>
<td>exadata-quarter2-92-x7-count</td>
<td>Availability domain</td>
<td>Number of Exadata.Quarter2.92 - X7 DB systems and Autonomous Exadata Infrastructure</td>
</tr>
<tr>
<td>vm-block-storage-gb</td>
<td>Availability domain</td>
<td>Total size of block storage attachments across all virtual machine DB systems, in GB</td>
</tr>
<tr>
<td>vm-standard1-ocpu-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard1.x OCPUs</td>
</tr>
<tr>
<td>vm-standard2-ocpu-count</td>
<td>Availability domain</td>
<td>Number of VM.Standard2.x OCPUs</td>
</tr>
</tbody>
</table>

**Note:**

When viewing the Limits, Quotas and Usage page of the Console, you will see the value "n/a" in the Service Limit column for storage and OCPU resources related to Autonomous Transaction Processing and Autonomous Data Warehouse with dedicated Exadata infrastructure. You might also see this value in the Available column for these resources. This is because limits for these resources are based on the capacity of your provisioned Exadata hardware, and are not service limits controlled by Oracle Cloud Infrastructure. If you define compartment quota policies for either of these resources, the Available column will display a value for the amount that is available to be allocated, based on your existing usage in the Exadata hardware.

For information about shapes that are not listed, including non-metered shapes, contact Oracle Support.

**Examples**

The following example shows how to limit the number of Autonomous Data Warehouse resources in a compartment:

```bash
#Limits the Autonomous Data Warehouse CPU core count to 2 in the MyCompartment compartment
set database quota adw-ocpu-count to 2 in compartment MyCompartment
```

This example shows how to set a quota for OCPU cores in an Autonomous Data Warehouse with dedicated Exadata infrastructure:

```bash
#Limits the number of Autonomous Data Warehouse dedicated Exadata infrastructure OCPUs to 20 in the MyCompartment compartment
set database quota adw-dedicated-ocpu-count to 20 in compartment MyCompartment
```

This example shows how to set a quota for Autonomous Exadata Infrastructure quarter rack resources in a compartment:

```bash
#Limits the usage of Exadata.Quarter2.92 X7 shapes to 1 in the MyCompartment compartment
```
To limit the number of virtual machine DB systems in a compartment, you must set a quota for the number of CPU cores and a separate quota for the block storage:

```sql
set database quota exadata-quarter2-92-x7-count to 1 in compartment MyCompartment
```

The following example shows how to prevent the usage of all database resources in the tenancy except for two Exadata full rack X7 resources in a specified compartment:

```sql
zero database quotas in tenancy
set database quota exadata-full2-368-x7-count to 2 in compartment MyCompartment
```

This example of nested quotas shows how to distribute limits for a resource type in a compartment among its subcompartments:

```sql
# Allows usage of 3 Autonomous Data Warehouse OCPUs in parent compartment Compartment1
set database quota adw-ocpu-count to 3 in compartment Compartment1

# Allows usage of 1 Autonomous Data Warehouse OCPU in child compartment Compartment1.1
set database quota adw-ocpu-count to 1 in compartment Compartment1.1

# Allows usage of 2 Autonomous Data Warehouse OCPUs in child compartment Compartment1.2
set database quota adw-ocpu-count to 2 in compartment Compartment1.2
```

**Digital Assistant Quotas**

For Digital Assistant quotas and examples, see Service Quotas.

**DNS Quotas**

Family name: dns

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global-zone-count</td>
<td>Global</td>
<td>Number of public DNS zones</td>
</tr>
<tr>
<td>steering-policy-count</td>
<td>Global</td>
<td>Number of traffic management steering policies</td>
</tr>
<tr>
<td>steering-policy-attachment-count</td>
<td>Global</td>
<td>Number of traffic management steering policy attachments</td>
</tr>
</tbody>
</table>

**Example**

```sql
zero dns quotas in compartment MyCompartment
zero dns quota global-zone-count in compartment MyCompartment
zero dns quota steering-policy-count in compartment MyCompartment
```
Events Quotas

Family name: events

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule-count</td>
<td>Regional</td>
<td>Number of rules</td>
</tr>
</tbody>
</table>

Example

- Set events quota rule-count to 10 in compartment MyCompartment
- Zero events quota rule-count in compartment MyCompartment

Email Delivery Quotas

Family name: email-delivery

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>approved-sender-count</td>
<td>Regional</td>
<td>Number of approved senders</td>
</tr>
</tbody>
</table>

Example

- Zero email-delivery quota approved-sender-count in compartment MyCompartment

File Storage Quotas

Family name: filesystem

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mount-target-count</td>
<td>Availability domain</td>
<td>Number of mount targets</td>
</tr>
<tr>
<td>file-system-count</td>
<td>Availability domain</td>
<td>Number of file systems</td>
</tr>
</tbody>
</table>

Example

- Set filesystem quota file-system-count to 5 in compartment MyCompartment
- Zero filesystem quota file-system-count in compartment MyCompartment
- Set filesystem quota mount-target-count to 1 in compartment MyCompartment
- Zero filesystem quota mount-target-count in compartment MyCompartment

Management Agent Quotas

Family name: management-agent

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>management-agent-count</td>
<td>Regional</td>
<td>Number of management agents</td>
</tr>
</tbody>
</table>
Examples

The following example limits the number of management agents that users can install in MyCompartment to 200.

```
set management-agent quota management-agent-count to 200 in compartment MyCompartment
```

The following example limits the number of management agent install keys that users can create in MyCompartment to 10.

```
set management-agent quota management-agent-install-key-count to 10 in compartment MyCompartment
```

Networking Quotas

VCN Quotas

Family name: vcn

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcn-count</td>
<td>Regional</td>
<td>Number of virtual cloud networks</td>
</tr>
<tr>
<td>reserved-public-ip-count</td>
<td>Regional</td>
<td>Number of reserved regional public IP addresses</td>
</tr>
</tbody>
</table>

Example

```
Set vcn quota vcn-count to 10 in compartment MyCompartment
```

NoSQL Database Cloud Quotas

For Oracle NoSQL Database Cloud quotas and examples, see Service Quotas.

Notifications Quotas

Family name: notifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topic-count</td>
<td>Regional</td>
<td>Number of topics</td>
</tr>
</tbody>
</table>

Example

```
set notifications quota topic-count to 10 in compartment MyCompartment
```

Object Storage Quotas

Family name: object-storage
<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage-bytes</td>
<td>Regional</td>
<td>Total storage size in bytes</td>
</tr>
</tbody>
</table>

**Examples**

Set object-storage quota storage-bytes to 10000000000 in tenancy

Set object-storage quota storage-bytes to 5000000000 in compartment MyCompartment

Zero object-storage quota storage-bytes in compartment AnotherCompartment

Unset object-storage quota storage-bytes in tenancy

**Resource Manager Quotas**

Family name: resource-manager

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>concurrent-job-count</td>
<td>Regional</td>
<td>Number of concurrent Jobs per compartment</td>
</tr>
<tr>
<td>configuration-source-provider-count</td>
<td>Regional</td>
<td>Number of configuration source providers per compartment</td>
</tr>
<tr>
<td>stack-count</td>
<td>Regional</td>
<td>Number of stacks per compartment</td>
</tr>
<tr>
<td>template-count</td>
<td>Regional</td>
<td>Number of private templates per compartment</td>
</tr>
</tbody>
</table>

**Example**

set resource-manager quota concurrent-job-count to 1 in compartment MyCompartment

zero resource-manager quota stack-count in compartment MyCompartment

set resource-manager quota configuration-source-provider-count to 5 in compartment MyCompartment

set resource-manager quota template-count to 3 in compartment MyCompartment

**Service Connector Hub Quotas**

Family name: service-connector-hub

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-connector-count</td>
<td>Regional</td>
<td>Number of service connectors</td>
</tr>
</tbody>
</table>

**Example**

set service-connector-hub quota service-connector-count to 10 in compartment MyCompartment

preview
## Streaming Quotas

Family name: `streaming`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>partition-count</code></td>
<td>Regional</td>
<td>Number of partitions</td>
</tr>
</tbody>
</table>

**Example**

```
set streaming quota partition-count to 10 in compartment MyCompartment
```

## Vault Quotas

Family name: `kms`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>virtual-private-vault-count</code></td>
<td>Regional</td>
<td>Number of virtual private vaults</td>
</tr>
</tbody>
</table>

**Example**

```
set kms quota virtual-private-vault-count to 1 in compartment MyCompartment
```

## WAF Quotas

Family name: `waas`

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>waas-policy-count</code></td>
<td>Regional</td>
<td>Number of WAF policies</td>
</tr>
</tbody>
</table>

**Example**

```
zero waas quota waas-policy-count in compartment MyCompartment
```

## Work Requests

This topic describes the work requests feature documented in the Work Requests API. The following Oracle Cloud Infrastructure services are integrated with this API:

- Compute
- Database
- Tenancy Explorer

**Note:**

Some Oracle Cloud Infrastructure services offer work requests supported by the service API rather than the Work Requests API discussed in this topic. For information about work requests in these services, see the following topics:

- **Application Migration:** View the State of a Work Request
- **Blockchain Platform:** Integration: Work Requests
Work requests allow you to monitor long-running operations such as Database backups or the provisioning of Compute instances. When you launch such an operation, the service spawns a work request. A work request is an activity log that enables you to track each step in the operation's progress. Each work request has an OCID that allows you to interact with it programmatically and use it for automation.

If an operation fails, a work request can help you determine which step of the process had an error.

Some operations affect multiple resources. For example, creating an instance pool also affects instances and instance configurations. A work request provides a list of the resources that an operation affects.

For workflows that require sequential operations, you can monitor each operation’s work request and confirm that the operation has completed before proceeding to the next operation. For example, say that you want to create an instance pool with autoscaling enabled. To do this, you must first create the instance pool, and then configure autoscaling. You can monitor the work request for creating the instance pool to determine when that workflow is complete, and then configure autoscaling after it is done.

Work requests are retained for 12 hours.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: Work requests inherit the permissions of the operation that spawns the work request. To enable users to view the work requests, logs, and error messages for an operation, write a policy that grants users permission to do the operation. For example, to let users see the work requests associated with launching instances, write a policy that enables users to launch instances.

To enable users to list all work requests in a tenancy, use the following policy:

```
Allow group SupportTeam to inspect work-requests in tenancy
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Work Request States**

**Note:** Work requests for some services or operations may support only a subset of the following statuses.

**ACCEPTED**

The request is in the work request queue to be processed.

**IN_PROGRESS**

A work request record exists for the specified request, but there is no associated WORK_COMPLETED record.
SUCCEEDED

A work request record exists for this request and an associated WORK_COMPLETED record has the state SUCCEEDED.

FAILED

A work request record exists for this request and an associated WORK_COMPLETED record has the state FAILED.

CANCELING

The work request is in the process of canceling.

CANCELED

The work request has been canceled.

Using the Console to View Work Requests

The steps to view a work request are similar for Oracle Cloud Infrastructure services that support work requests.

1. Navigate to resource whose work requests you want to see.

   For example, to see the work requests for a Compute instance: Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.

2. If the resource is displayed in a list view, click the resource name to view the resource details.

3. Under Resources, click Work Requests. The status of all work requests appears on the page.

4. To see the log messages, error messages, and resources that are associated with a specific work request, click the operation name. Then, select an option in the More information section.

   For associated resources, you can click the the Actions icon (three dots) next to a resource to copy the resource's OCID.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to monitor the state of work requests:

- ListWorkRequests
- GetWorkRequest
- ListWorkRequestErrors
- ListWorkRequestLogs

Console Announcements

This topic describes the announcements that Oracle Cloud Infrastructure displays in the Console. Console announcements appear at the top of the page to communicate timely, important information about service status. You can also view a list of past and ongoing announcements.

Note:

- If you use Oracle Platform Cloud Services or Oracle Cloud Applications and you have announcements about those service entitlements, the Console displays a banner with a link that you can use to access those announcements. For more information about these announcements, including how to set notification preferences, see Monitoring Notifications.
Types of Announcements

Announcements belong to different categories. An announcement's prefix helps you understand, at a glance, the type and relative severity of the information and whether there's anything you can or must do. Announcement types currently include the following, in order of most important to least:

- **Required action.** You must take specific action within your environment.
- **Emergency change.** There is a time period during which an unplanned, but urgent, change associated with your environment will take place.
- **Recommended action.** You have specific action to take within your environment, but the action is not required.
- **Planned change.** There is a time period during which a planned change associated with your environment will take place.
- **Planned change extended.** The scheduled change period has extended beyond what was previously communicated.
- **Planned change rescheduled.** The planned change to your environment has been postponed to a later time or date.
- **Production event.** An impactful change to your environment either recently occurred or is actively occurring.
- **Planned change completed.** The planned change to your environment has been completed and regular operations have resumed.
- **Information.** There is information that you might find useful, but is not urgent and does not require action on your part.

For announcements that require action and affect Oracle Cloud Infrastructure Compute instances, you will get 30 days of advance notice. If you need to delay the actions described in the announcement, contact support to request one of the alternate dates listed in the announcement. Critical vulnerabilities might not be eligible for delay.

**Required IAM Policy**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

Depending on whether you have access, you might not see any announcements. With access to announcements, you can either see only the summary version of any given announcement or you can also view announcement details.

For administrators: for typical policies that give users access to announcements, see Restrict user access to view only summary announcements and Let users view details of announcements. For more information, see Details for the Announcements Service.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Email Delivery**

As part of your service agreement, Oracle Cloud Infrastructure also contacts you with service status announcements through email. These emails help alert you to upcoming changes that will impact your tenancy, such as those involving data centers or instances you use, or about required action on your part. Whenever possible, we try to provide advance notice of impactful events. Oracle sends these announcements to the default tenancy administrator email address on record. You can opt out of emails with operational information that is not urgent and does not require administrator action. (In the Console, these announcements are marked with the type, "Information." For more information about announcement types, see Types of Announcements on page 261.) If you want to change the default tenancy administrator email address on record, contact Oracle Support. For more information, see Contacting Support.
To manage email preferences for announcements

1. Click the Announcements icon (いません).
2. Click Manage Email Preferences.
3. Do one of the following:
   - If you want Oracle to email a copy of all announcements, click Opt in.
   - If you want Oracle to withhold email copies of informational announcements that don't require action on your part, click Opt out.

Viewing Announcements

This section describes how to view announcements. The Console displays announcements as banners that span the width of the top of your browser window. As long as an announcement remains in effect and you have the access to view announcements, the banner announcement displays each time you sign in to the Console until you mark it as read. You can also view all past announcements. The Announcements icon displays a green dot if you have any unread announcements.

To dismiss a banner announcement

- To close a banner announcement until the next time you sign in to the Console, click the X at the far right edge of the banner. If you want to stop seeing an announcement as a banner altogether, you must mark it as read. For more information, see To mark an announcement as read on page 263.

To view the details of an announcement

1. Do one of the following:
   - If you are viewing a banner, click the Show details link near the far right edge of the banner.
   - If you are viewing a list of announcements, under the Summary column, click the announcement summary.
2. On the Announcement Details page, you can view the following information:
   - Description. This describes the issue or event in greater detail than the summary text of the announcement.
   - OCID. This is the announcement's unique, Oracle-assigned identifier.
   - Reference Ticket Number. You can use this number to refer to the issue when talking to Support.
   - Type. This is one of several predefined categories that helps to set expectations about the nature and severity of the issue described.
   - Affected Service. This indicates the Oracle Cloud Infrastructure services affected by the issue or event.
   - Region. This tells you what Oracle Cloud Infrastructure regions are impacted.
   - Start Time. This is when the issue or event was first detected.
   - End Time. This is when the issue or event was resolved.
   - Required After. This is the date after which you must address any required actions described in the announcement.
   - Created. This is when the announcement was created.
   - Updated. This is when the announcement was updated.
   - Additional Information. This includes information such as workarounds or background material.
   - Impacted Resources. This shows the resources that were affected in some way by the event that prompted the announcement.
3. Optionally, if you want to refer to the list of impacted resources later, click Download Impacted Resources List.

To view a list of all announcements

1. Click the Announcements icon (いたします).
2. The **Announcements** page displays all announcements. From this page, you can do the following:

- **Filter.** You can filter announcements by type or by start or end date.
- **Sort.** You can sort announcements by summary, type, event start time, or publish time (which indicates when the announcement was last updated).
- **Mark as read.** You can mark announcements as read if you want stop seeing them as banners in the Console in subsequent sessions.
- **View announcement details.** You can view the details of an announcement.

### To filter a list of announcements

1. Click the Announcements icon (🌐).
2. To filter the list, under **Filters**, do one of the following:
   - Click **Type**, and then click a type from the list.
   - Click **Start Date**, and then choose a date to see only events that started on that date.
   - Click **End Date**, and then choose a date to see only events that ended on that date.
3. To clear a filter on a date, click the X next to the date.

### To sort a list of announcements

1. Click the Announcements icon (🌐).
2. By default, the list displays announcements according to the event start time, from most recent to least. To sort the list another way, do one of the following:
   - Click **Summary.** The list sorts alphabetically, according to the summary of the announcement.
   - Click **Type.** The list sorts according to the importance of the announcement.
   - Click **Start Time.** The list sorts according to the start time of the event described in the announcement. If you begin by viewing the default sort order, the sort order will change to show the oldest announcement at the beginning of the list.
   - Click **Publish Time.** The list sorts according to the time that an announcement was last updated. You might find it helpful to sort by this column if you want to track an ongoing issue or if an announcement requires action on your part.
3. To sort the list again, repeat the previous step.

### To mark an announcement as read

1. Click the Announcements icon (🌐).
2. Find the announcement that you want to mark as read, click the Actions icon (three dots), and then click **Mark As Read.**

### Using the Command Line Interface (CLI)

For information about using the CLI, see [Command Line Interface (CLI)](https://docs.oracle.com/en-us/iaas/Content/API/Concepts/usingapi.htm). For a complete list of flags and options available for CLI commands, see the [Command Line Reference](https://docs.oracle.com/en-us/iaas/Content/API/Concepts/usingapi.htm).

### To view the details of an announcement

Open a command prompt and run `oci announce announcements get` to view detailed information about an announcement:

```bash
oci announce announcements get --announcement-id <announcement_OCID>
```

For example:
To view a list of all announcements
Open a command prompt and run `oci announce announcements list` to view a list of all announcements:

```
oci announce announcements list --compartment-id <compartment_OCID>
```

For example:

```
oci announce announcements list --compartment-id ocid1.tenancy.oc1..exampleati4wjo6cbxq4iusld5ltipeskcfy7lr4a6wfauxuwrwed5bsdea
```

To filter a list of announcements
Open a command prompt and run `oci announce announcements list` to filter a list of announcements.
To filter a list of announcements by announcement type:

```
oci announce announcements list --compartment-id <compartment_OCID> --announcement-type <announcement_type>
```

For example:

```
oci announce announcements list --compartment-id ocid1.tenancy.oc1..exampleati4wjo6cbxq4iusld5ltipeskcfy7lr4a6wfauxuwrwed5bsdea --announcement-type ACTION_REQUIRED
```

To sort a list of announcements
Open a command prompt and run `oci announce announcements list` to sort a list of announcements.
To sort a list of announcements in ascending order of time created, from oldest to newest:

```
oci announce announcements list --compartment-id <compartment_OCID> --sort-order ASC
```

For example:

```
oci announce announcements list --compartment-id ocid1.tenancy.oc1..exampleati4wjo6cbxq4iusld5ltipeskcfy7lr4a6wfauxuwrwed5bsdea --sort-order ASC
```

To mark an announcement as read
Open a command prompt and run `oci announce user-status update` to mark an announcement as read:

```
oci announce user-status update --announcement-id <announcement_OCID> --user-status-announcement-id <announcement_OCID> --user-id <user_OCID> --time-acknowledged <date_and_time>
```

For example:
oci announce user-status update --announcement-id ocid1.announcement.region1..examplear73oue4jdywjvietoc6im3cvb6xae4falm3fau5us3iwra3t6q --user-status-announcement-id ocid1.announcement.region1..examplear73oue4jdywjvietoc6im3cvb6xae4falm3fau5us3iwra3t6q --user-id ocid1.user.region1..exampleaorxz3psplonigcvbzy5oaiwiubh7k7ip6zgklfauxic67kksu4oq --time-acknowledged 2019-01-06T20:14:00+00:00

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage announcements:

- GetAnnouncement
- GetAnnouncementUserStatus
- ListAnnouncements
- UpdateAnnouncementUserStatus

Prerequisites for Oracle Platform Services on Oracle Cloud Infrastructure

This topic describes procedures that are required by some Oracle Platform Services before you can launch them on Oracle Cloud Infrastructure. The information in this topic applies only to the following services:

- Oracle Database Cloud Service
- Oracle Data Hub Cloud Service
- Oracle Event Hub Cloud Service
- Oracle Java Cloud Service
- Oracle SOA Cloud Service

For a list of all services supported on Oracle Cloud Infrastructure, see Information About Supported Platform Services on page 271.

Accessing Oracle Cloud Infrastructure

Oracle Cloud Infrastructure has a different interface and credential set than your Oracle Platform Services. You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Required Identity and Access Management (IAM) Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

See Common Policies on page 2142 for more information and examples.
Resources Created in Your Tenancy by Oracle

Oracle creates a compartment in your tenancy for Oracle Platform Services. This compartment is specially configured by Oracle for the Oracle Cloud Infrastructure resources that you create through the Platform Services. You can't choose another compartment for Oracle to use.

Along with this compartment, Oracle creates the IAM policies to allow Oracle Platform Services access to the resources.

The compartment that Oracle creates for Oracle Platform Services is named: ManagedCompartmentForPaaS.

The policies that Oracle creates for Oracle Platform Services are:

- **PSM-root-policy**
  
  This policy is attached to the root compartment of your tenancy.

- **PSM-mgd-comp-policy**
  
  This policy is attached to the ManagedCompartmentForPaaS compartment.

Caution: Do not make any changes to these resources. Editing or renaming the policies or the compartment can result in loss of functionality.

Prerequisites for Oracle Platform Services

Before you can create instances of an Oracle Platform Service on Oracle Cloud Infrastructure, you need to have the following resources in your Oracle Cloud Infrastructure tenancy:

- A compartment for your resources
- A virtual cloud network (VCN) with at least one public subnet
- IAM policies to allow Oracle Platform Services to access the VCN
- An Object Storage bucket
- Credentials to use with Object Storage

Some of the Platform Services automatically create some of these resources for you. See details about your service in the following sections.

Setting Up the Prerequisites

Note: To use Autonomous Data Warehouse Cloud, you don't need to set up any of the resources listed in this prerequisites section. However, if you optionally choose to use Oracle Cloud Infrastructure Object Storage for data loading, you need to perform these two tasks:

Create a bucket
Create an auth token

Following are two scenarios with procedure sets. If you need to set up all the required resources, follow Scenario 1. If you already have a VCN in your Oracle Cloud Infrastructure tenancy that you want to use for Oracle Platform Services, follow Scenario 2.

To follow a tutorial on how to set up the prerequisites for Scenario 1, see Creating the Infrastructure Resources Required for Oracle Platform Services.

Scenario 1: I need to create all the prerequisite resources
Scenario 2: I have an existing VCN in Oracle Cloud Infrastructure that I want to use for my Oracle Platform Services instance

You can use an existing VCN. The VCN must have at least one public subnet. Perform these tasks to complete the prerequisites:

Create a compartment

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot use the ManagedCompartmentForPaaS for your VCN and bucket.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
2. A list of the existing compartments in your tenancy is displayed.
3. Click Create Compartment.
4. Enter the following:
   - **Name:** For example, PaaSResources. Restrictions for compartment names are: Maximum 100 characters, including letters, numbers, periods, hyphens, and underscores. The name must be unique across all the compartments in your tenancy. Avoid entering confidential information.
   - **Description:** A friendly description.
5. Click Create Compartment.

Set up your virtual cloud network

This procedure creates a VCN with these characteristics:

- A VCN with the CIDR of your choice (example: 10.0.0.0/16).
- A regional public subnet with access to the VCN's internet gateway. You can choose the subnet's CIDR (example: 10.0.0.0/24).
- A regional private subnet with access to the VCN's NAT gateway and service gateway (and therefore the Oracle Services Network). You can choose the subnet's CIDR (example: 10.0.1.0/24).
- Use of the Internet and VCN Resolver for DNS, so your instances can use their hostnames instead of their private IP addresses to communicate with each other.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following VCN quickstart procedure is useful for getting started and trying out Oracle Platform Services on Oracle Cloud Infrastructure. For production, use the procedure in VCNs and Subnets on page 2821. That topic explains features such as how to specify the CIDR ranges for your VCN and subnets, and how to secure your network. When you use the advanced procedure in that topic, remember that the VCN that you create must have a public subnet for Oracle Platform Services to use.</td>
</tr>
</tbody>
</table>

1. Open the Region menu and select the region in which you want to create the Oracle PaaS service instance.
   - Select a region that's within the default data region of your account. For example, if your default data region is EMEA, then select Germany Central (Frankfurt) or UK South (London).
2. From the Compartment list, select the compartment you created.
3. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
4. Click Networking Quickstart.
5. Select VCN with Internet Connectivity, and then click Start Workflow.
6. Enter the following:
   • **VCN Name:** Enter a name for your cloud network, for example, `<your_initials>_Network`. The name is incorporated into the names of all the related resources that are automatically created. Avoid entering confidential information.
   • **Compartment:** Leave the default value (the compartment you're currently working in). All the resources will be created in this compartment.
   • **VCN CIDR Block:** Enter a valid CIDR block for the VCN. For example 10.0.0.0/16.
   • **Public Subnet CIDR Block:** Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block. For example: 10.0.0.0/24.
   • **Private Subnet CIDR Block:** Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block and not overlap with the public subnet's CIDR block. For example: 10.0.1.0/24.
   • Accept the defaults for any other fields.

7. Click **Next**.

8. Review the list of resources that the workflow will create for you. Notice that the workflow will set up security list rules and route table rules to enable basic access for the VCN.

9. Click **Create** to start the short workflow.

**Permit Oracle Platform Services to access resources**

1. In the Console, navigate to the root compartment of your tenancy by clicking your tenancy name in the **Compartment** list.
2. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**.
3. Click **Create Policy**.
4. Enter the following:
   • **Name:** A unique name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later.
   • **Description:** A friendly description. You can change this later if you want to.
   • **Statement:** To allow Oracle Platform Services access to use the network in your compartment, enter the following policy statements. Replace `<compartment_name>` with your compartment name. Click + after each statement to add another.

   ```plaintext
   Allow service PSM to inspect vcns in compartment `<compartment_name>`
   Allow service PSM to use subnets in compartment `<compartment_name>`
   Allow service PSM to use vnics in compartment `<compartment_name>`
   Allow service PSM to manage security-lists in compartment `<compartment_name>`
   ```

   For more information about policies, see **Policy Basics** on page 2137 and also **Policy Syntax** on page 2164.

5. (Optional) If you want to enable the use of an Autonomous Transaction Processing or Oracle Cloud Infrastructure Database instance in your compartment as the infrastructure schema database for your Oracle Java Cloud Service instance, then add the following statements:

   ```plaintext
   Allow service PSM to inspect autonomous-database in compartment `<compartment_name>`
   Allow service PSM to inspect database-family in compartment `<compartment_name>`
   ```

6. Click **Create**.
Create a bucket

1. Open the Region menu and select the region in which you want to create the Oracle PaaS service instance.

   Select a region that's within the default data region of your account. For example, if your default data region is EMEA, then select Germany Central (Frankfurt) or UK South (London).

2. Open the navigation menu. Under Core Infrastructure, click Object Storage.

3. Choose the compartment you created.

4. Click Create Bucket.

5. In the Create Bucket dialog, enter a bucket name, for example: PaasBucket.

   Make a note of the name you enter. You will need it when you create an instance for your Oracle Platform Service later.

6. Click Create Bucket.

Set up credentials to use with Object Storage

For Big Data Cloud, set up an API signing key:

Set up an API signing key

Follow the instructions in this topic: Required Keys and OCIDs on page 4179.

For all other services, create an auth token. Note that your service might refer to this credential as a Swift password. Use the auth token wherever you are asked to provide a Swift password.

Create an auth token

1. View the user's details:

   - If you're creating an auth token for yourself:

     Open the Profile menu ( ) and click User Settings.

   - If you're an administrator creating an auth token for another user: In the Console, click Identity, and then click Users. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click Auth tokens.

3. Click Generate Token.

4. Enter a friendly description for the token and click Generate Token.

   The new token is displayed.

5. Copy the token immediately, because you can't retrieve it again after closing the dialog box. Also, make sure you have this token available when you create your Oracle Platform Services instance.

Permit Oracle Platform Services to access resources

1. In the Console, navigate to the root compartment of your tenancy by clicking your tenancy name in the Compartment list.

2. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.

3. Click Create Policy.
4. Enter the following:
   - **Name:** A unique name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
   - **Description:** A friendly description. You can change this later if you want to.
   - **Statement:** To allow Oracle Platform Services access to use the network, enter the following policy. Click + after each statement to add another. In each statement, replace `<compartment_name>` with the name of the compartment where your VCN resides.

   ```sql
   Allow service PSM to inspect vcns in compartment <compartment_name>
   Allow service PSM to use subnets in compartment <compartment_name>
   Allow service PSM to use vnics in compartment <compartment_name>
   Allow service PSM to manage security-lists in compartment <compartment_name>
   ```

   For more information about policies, see **Policy Basics** on page 2137 and also **Policy Syntax** on page 2164.

5. (Optional) If you want to enable the use of an Autonomous Transaction Processing or Oracle Cloud Infrastructure Database instance in your compartment as the infrastructure schema database for your Oracle Java Cloud Service instance, then add the following statements:

   ```sql
   Allow service PSM to inspect autonomous-database in compartment <compartment_name>
   Allow service PSM to inspect database-family in compartment <compartment_name>
   ```

6. Click **Create**.

**Create a bucket**

1. Open the **Region** menu and select the region in which you want to create the Oracle PaaS service instance.
   
   Select a region that's within the default data region of your account. For example, if your default data region is EMEA, then select Germany Central (Frankfurt) or UK South (London).

2. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

3. Choose the compartment you want to create the bucket in.

4. Click **Create Bucket**.

5. In the **Create Bucket** dialog, enter a bucket name, for example: PaasBucket. Make a note of the name you enter. You will need it when you create an instance for your Oracle Platform Service later. Avoid entering confidential information.

6. Click **Create Bucket**.

**Set up credentials to use with Object Storage**

For Big Data Cloud, set up an API signing key:

**Set up an API signing key**

Follow the instructions in this topic: **Required Keys and OCIDs** on page 4179.

For all other services, create an auth token. Note that your service might refer to this credential as a Swift password. Use the auth token wherever you are asked to provide a Swift password.
Create an auth token

1. View the user's details:
   - If you’re creating an auth token for yourself:
     - Open the Profile menu ( ) and click User Settings.
   - If you’re an administrator creating an auth token for another user: In the Console, click Identity, and then click Users. Locate the user in the list, and then click the user’s name to view the details.

2. On the left side of the page, click Auth Tokens.
3. Click Generate Token.
4. Enter a friendly description for the token and click Generate Token.

   The new token is displayed.

5. Copy the auth token immediately, because you can't retrieve it again after closing the dialog box. Also, make sure you have this token available when you create your Oracle Platform Services instance.

Information About Supported Platform Services

The following table lists the services supported on Oracle Cloud Infrastructure and links to more information about using those services on Oracle Cloud Infrastructure:

<table>
<thead>
<tr>
<th>Service</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics Cloud</td>
<td>Getting Started with Oracle Analytics Cloud</td>
</tr>
<tr>
<td>API Platform Cloud Service</td>
<td>Get Started with Oracle API Platform Cloud Service</td>
</tr>
<tr>
<td>Autonomous Data Warehouse</td>
<td>Getting Started with Autonomous Data Warehouse</td>
</tr>
<tr>
<td>Integration</td>
<td>Oracle Integration</td>
</tr>
<tr>
<td>Autonomous Mobile Cloud Enterprise</td>
<td>About Oracle Autonomous Mobile Cloud Enterprise</td>
</tr>
<tr>
<td>NoSQL Database Cloud Service</td>
<td>Oracle NoSQL Database Cloud Service</td>
</tr>
<tr>
<td>Oracle Visual Builder</td>
<td>Administering Oracle Visual Builder</td>
</tr>
<tr>
<td>Data Hub Cloud Service</td>
<td>About Oracle Data Hub Cloud Service Clusters in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Data Integration Platform Cloud</td>
<td>What is Oracle Data Integration Platform Cloud</td>
</tr>
<tr>
<td>Database Cloud Service</td>
<td>About Database Deployments in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Developer Cloud Service</td>
<td>Using Oracle Developer Cloud Service</td>
</tr>
<tr>
<td>Event Hub Cloud Service</td>
<td>About Instances in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Java Cloud Service</td>
<td>About Java Cloud Service Instances in Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Oracle SOA Cloud Service</td>
<td>About SOA Cloud Service Instances in Oracle Cloud Infrastructure</td>
</tr>
</tbody>
</table>
Renaming a Cloud Account

This topic describes the process of changing your cloud account name. When you sign up for Oracle Cloud, you get a cloud account and an Oracle Cloud Infrastructure tenancy. Both the cloud account and tenancy have an ID and a name. Oracle assigns the same name to the cloud account and the tenancy, but they each have a unique ID. You need to specify the tenancy name when you sign in to Oracle Cloud Infrastructure Console, so that you arrive at the right account. Any programmatic access uses the tenant ID or cloud account ID, not its name. For example:

- Sample account and tenancy name: "OracleCustomer1"
- Sample cloud account ID: "cacct-7a26a4exampleuniqueID"
- Sample tenancy ID: "ocid1.tenancy.oc1..exampleuniqueID"

You can view your cloud account name in the Tenancy Details page. You might need to rename your cloud account if the name that it was initially given is no longer relevant or correct. For example:

- You created a trial account called MyTrial, and then it became the main account for your company.
- You had an acquisition that is forcing name changes.

Follow these guidelines for a successful rename:

- Plan ahead and inform others that you plan on changing the name.
- Change the name during off-hours to reduce impact on users in your tenancy.
- Notify personnel who use Oracle Cloud when the rename is complete.

Note:

Only an Oracle Identity Cloud Service (IDCS) cloud account administrator can rename the cloud account. After the account name changes, you can’t use the old name to sign in to the Console. Existing sessions keep working, but new sessions need to use the new name. You can’t change an account name back to its old name.

You can change your cloud account name in the My Oracle Services dashboard, which is accessible from the Profile menu's Service User Console option.

Important:

Two methods for signing in are available: by using the oracle.com URL, which always uses IDCS, and by using the Console URL. If you use the Console URL to navigate directly to the Console and sign in, the Service User Console menu option isn't available in the Profile menu. Choose the "oraclecloudidentityservice" option when signing in if you're unsure. For more information, see Signing In to the Console on page 41.

To change a cloud account name

1. Click the Profile icon and select Service User Console. The My Oracle Services dashboard opens in another browser window.
2. From the main menu, select Account.
3. On the Account page, select the Account Management tab.
4. Next to the Account Name field, click the Rename Account button. This button is only available if you are an IDCS cloud account administrator.
5. In the Rename Account dialog box, enter the new account name, and click OK.

After you submit the change, it takes about 15 minutes to rename the account. When the rename is complete, the account admin receives an email, which states that you need to use your existing credentials to sign in.

When you sign in to the Console, you are required to use the new account name (<new_account_name>) when prompted for a cloud account or tenant name.
When you rename an account, all references to the cloud account name and the tenancy name are updated, including the following names:

- IDCS instance name
- Amazon S3 Compatibility API Designated Compartment
- SWIFT API Designated Compartment

The API Designated Compartment names are listed on the Tenancy Information tab of the Tenancy Details page, under Object Storage Settings. The Object Storage Namespace, also shown in the Object Storage Settings area, is not updated. This name is set as the name for older accounts. Newer accounts have a short random string as the namespace.

Billing and Payment Tools Overview

Oracle Cloud Infrastructure provides various billing and payment tools that make it easy to manage your service costs.

**Budgets**

Budgets can be used to set thresholds for your Oracle Cloud Infrastructure spending. You can set alerts on your budget to let you know when you might exceed your budget, and you can view all of your budgets and spending from one single place in the Oracle Cloud Infrastructure console. See Budgets Overview on page 274 for more information.

**Cost Analysis**

Cost Analysis provides easy-to-use visualization tools to help you track and optimize your Oracle Cloud Infrastructure spending. For more information, see Checking Your Expenses and Usage on page 55.

**Cost and Usage Reports**

A cost report is a comma-separated value (CSV) file that is similar to a usage report, but also includes cost columns. The report can be used to obtain a breakdown of your invoice line items at resource-level granularity. As a result, you can optimize your Oracle Cloud Infrastructure spending, and make more informed cloud spending decisions.

A usage report is a comma-separated value (CSV) file that can be used to get a detailed breakdown of resources in Oracle Cloud Infrastructure for audit or invoice reconciliation.

For more information, see Cost and Usage Reports Overview on page 278.

**Unified Billing**

You can unify billing across multiple tenancies by sharing your subscription between tenancies. For more information, see Unified Billing Overview on page 296.

**Invoices**

You can view and download invoices for your Oracle Cloud Infrastructure usage. For more information, see Viewing Your Subscription Invoice.

**Payment Methods**

The Payment Method section of the Oracle Cloud Infrastructure Console allows you to easily manage how you pay for your Oracle Cloud Infrastructure usage. For more information, see Changing Your Payment Method on page 56.
Budgets Overview

A budget can be used to set soft limits on your Oracle Cloud Infrastructure spending. You can set alerts on your budget to let you know when you might exceed your budget, and you can view all of your budgets and spending from one single place in the Oracle Cloud Infrastructure console.

How Budgets Work

Budgets are set on cost-tracking tags or on compartments (including the root compartment) to track all spending in that cost-tracking tag or for that compartment and its children.

All budgets alerts are evaluated every hour in most regions, and every four hours in IAD. To see the last time a budget was evaluated, open the details for a budget. You will see fields that show the current spend, the forecast and the “Spent in period” field which shows you the time period over which the budget was evaluated. When a budget alert fires, the email recipients configured in the budget alert receive an email.

Budget Concepts

The following concepts are essential to working with budgets:

BUDGET

A monthly threshold you define for your Oracle Cloud Infrastructure spending. Budgets are set on cost-tracking tags or compartments and track all spending in the cost-tracking tag or compartment and any child compartments.

Note:

The budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.

ALERT

You can define email alerts that get sent out for your budget. You can send a customized email message body with these alerts. Alerts are evaluated every hour in most regions (every four hours in IAD), and can be triggered when your actual or your forecasted spending hits either a percentage of your budget or a specified set amount.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

To use budgets, you must be in a group that can use "usage-budgets” in the tenancy (which is the root compartment) or be able to use all resources in the tenancy. All budgets are created in the root compartment, regardless of the compartment they are targeting, so IAM policies that grant budget permissions outside of the root will not be meaningful.

<table>
<thead>
<tr>
<th>IAM Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow group accountants to inspect usage-budgets in tenancy</td>
<td>Accountants can inspect budgets including spend.</td>
</tr>
<tr>
<td>Allow group accountants to read usage-budgets in tenancy</td>
<td>Accountants can read budgets including spend (same as list).</td>
</tr>
<tr>
<td>IAM Policy</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow group accountants to use usage-budgets in tenancy</td>
<td>Accountants can create and edit budgets and alerts rules.</td>
</tr>
<tr>
<td>Allow group accountants to manage usage-budgets in tenancy</td>
<td>Accountants can create, edit, and delete budgets and alerts rules.</td>
</tr>
</tbody>
</table>

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Creating Automation for Budgets Using the Events Service**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

**Managing Budgets**

This topic discusses how to view and manage your budgets.

**Using the Console**

*To create a budget*

1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Budgets.
2. Click Create Budget at the top of the budgets list. The Create Budget dialog is displayed.
3. Select either Compartment or Cost-Tracking Tag to select the type of target for your budget.
4. Enter a name for your budget in the Name text field. The name can only contain alphanumeric characters, dashes, and the underscore character, and can’t begin with a number. Avoid entering confidential information.
5. Enter a description for the budget. Avoid entering confidential information.
6. Select the target for your budget:
   - For budgets targeting a compartment:
     - Select a target compartment for your budget from the Target Compartment drop-down list. Note that while the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.
   - For budgets targeting a cost-tracking tag:
     - Select a tag namespace.
     - Select a target cost-tracking tag key.
     - Enter a value for the cost-tracking tag.
7. Enter a monthly amount for your budget in the **Monthly Budget Amount** field. The minimum allowed value for your monthly budget is 1; the maximum allowed value is 999,999,999,999.

8. From **Day of the Month to Begin Budget Processing**, select the day of the month that you want budget processing to periodically begin on each month. Setting this value allows you to create a budget that aligns with your billing cycle date, and to receive more meaningful budget alerts. Below this field, **Current Budget Processing Period Based on Selection** reflects the budget processing period, according to the day of the month you chose. When viewing or editing a budget on its details page, the **Budget Processing Period** field also displays this information.

```
Note:
If you select the 29th, 30th, or 31st as the day of the month, budget processing begins on the last day of the month, for months that have fewer than the respective days you have chosen (whether 29, 30, or 31).
```

9. You can optionally create an alert for your budget by creating a budget alert rule. In **Budget Alert Rule** on the **Create Budget** dialog, configure your alert rule:

a. Select a threshold for your alert from the **Threshold Metric** drop-down list. There are two possible values:
   - **Actual Spend** watches the actual amount you spend in your compartment per month;

   **Forecast Spend** watches your resource usage and alert you when it appears that you'll exceed your budget. The forecast algorithm is linear extrapolation and requires at least three days of consumption to trigger.

b. Select a threshold type from the **Threshold Type** drop-down list. You can select either a percentage of your monthly budget (which must be greater than 0 and no greater than 10,000) or a fixed amount.

c. The label of the next text field changes depending on what type of threshold you selected. Enter either a **Threshold %** or a **Threshold Amount**.

d. In the **Email Recipients** field, enter one or more email addresses to receive the alerts. Multiple addresses can be separated using a comma, semicolon, space, tab, or new line.

e. Enter the body of your email alert in the **Email Message** field. The text of the email message cannot exceed 1000 characters. This message will be included with metadata about your budget, including the budget name, the compartment, and the amount of your monthly budget. You can use this message to for things like providing instructions to the recipient that explain how to request a budget increase or reminding users about corporate policies.

10. **Advanced Options (optional)**: Click the **Show advanced options** link to add **Tags** to your budget. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

11. Click the **Create** button to create your budget.

**To view or edit a budget**

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Budgets**.

2. From the list of budgets, click on the budget you want to edit. The budget detail screen will appear.

3. Click the **Edit** button. The **Edit Budget** dialog will appear.

4. You can edit the name of your budget or the budget amount. Avoid entering confidential information.

5. When you are finished, click **Save Changes**.

**To delete a budget**

1. From the list of budgets, select **Delete** from the context menu, or click the **Delete** button at the top of budget detail screen. The **Confirm Delete** dialog will appear.

2. Click the **Confirm** button to delete the budget, or cancel by clicking **Cancel**.

**To manage tags for a budget**

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Budgets**.

2. From the list of budgets, click on the budget you want to tag. The budget detail screen will appear.
3. Click the **Add tag(s)** button to add a tag.
4. Click the **Tags** tab and then click on the pencil icon next to a tag you want to edit or remove.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operation to manage budgets:

- ListBudgets
- GetBudget
- CreateBudget
- DeleteBudget
- UpdateBudget

**Managing Budget Alert Rules**

You can set email alerts on your budgets. You can set alerts that are based on a percentage of your budget or an absolute amount, and on your actual spending or your forecast spending.

This topic covers how to view and manage your budget alert rules.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Using the Console**

*To create a budget alert rule*

1. Click the budget that you want to create an alert for from the budgets list.
2. In the **Budget Alert Rules** panel at the bottom of the screen, click the **Create Budget Alert Rule** button.
3. Configure your alert rule:
   a. Select a threshold for your alert from the **Threshold Metric** drop-down list. There are two possible values:
      - **Actual Spend** will watch the actual amount you spend in your compartment per month;
      - **Forecast Spend** will watch your resource usage and alert you when it appears that you'll exceed your budget. The forecast algorithm is linear extrapolation and requires at least 3 days of consumption to trigger
   b. Select a threshold type from the **Threshold Type** drop-down list. You can select either a percentage of your monthly budget (which must be greater than 0 and no greater than 10,000) or a fixed amount.
   c. The label of the next text field changes depending on what type of threshold you selected. Enter either a **Threshold %** or a **Threshold Amount**.
   d. In the **Email Recipients** field, enter one or more email addresses to receive the alerts. Multiple addresses can be separated using a comma, semicolon, space, tab, or new line.
   e. Enter the body of your email alert in the **Email Message** field. The text of the email message cannot exceed 1000 characters. This message will be included with metadata about your budget, including the budget name, the compartment, and the amount of your monthly budget. You can use this message for things like providing instructions to the recipient that explain how to request a budget increase or reminding users about corporate policies.
4. Click the **Create** button to create your alert.
**To view or edit a budget alert rule**

1. In the list of budget alert rules, click the menu icon at the right side of the list and select **View/Edit** from the context menu.
2. Edit your alert rule.
3. Confirm your changes by clicking **Save Changes**, or dismiss the dialog without saving by clicking the **Cancel** button.

**To delete a budget alert rule**

1. In the list of budget alert rules, click the menu icon at the right side of the list and select **Delete** from the context menu.
2. Confirm or cancel the delete operation in the **Confirm Delete** dialog by clicking either the **Confirm** or **Cancel** button.

**Using the API**

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use the following operations to manage budget alert rules:

- **ListAlertRules**
- **GetAlertRule**
- **CreateAlertRule**
- **DeleteAlertRule**
- **UpdateAlertRule**

**Cost and Usage Reports Overview**

A **cost report** is a comma-separated value (CSV) file that is similar to a usage report, but also includes cost columns. The report can be used to obtain a breakdown of your invoice line items at resource-level granularity. As a result, you can optimize your Oracle Cloud Infrastructure spending, and make more informed cloud spending decisions.

A **usage report** is a comma-separated value (CSV) file that can be used to get a detailed breakdown of resources in Oracle Cloud Infrastructure for audit or invoice reconciliation.

In summary, usage reports indicate the **quantity** of what is consumed, while cost reports indicate the **cost** of resource consumption.

**Note:**

Cost and usage reports do not apply to non-metered tenancies.

**How Cost Reports Work**

The cost report is automatically generated daily, and is stored in an Oracle-owned Object Storage bucket. It contains one row per each Oracle Cloud Infrastructure resource (such as instance, Object Storage bucket, VNIC) per hour along with consumption information (usage, price, cost), metadata, and tags. Cost reports generally contain 24 hours of usage data, although occasionally a cost report may contain late-arriving data that is older than 24 hours.

Cost reports may contain corrections. Corrections are added as new rows to the report, with the `lineItem/isCorrection` column set and the `referenceNo` value of the corrected line populated in the `lineItem/backReference` column.

Cost reports are retained for one year.

The file name for each cost report is appended with an automatically incrementing numerical value.

**Cost Report Schema**

The following table shows the cost report schema.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lineItem/referenceNo</td>
<td>Line identifier. Used for debugging and corrections.</td>
</tr>
<tr>
<td>lineItem/TenantId</td>
<td>The identifier (OCID) for the Oracle Cloud Infrastructure tenant.</td>
</tr>
<tr>
<td>lineItem/intervalUsageStart</td>
<td>The start time of the usage interval for the resource.</td>
</tr>
<tr>
<td>lineItem/intervalUsageEnd</td>
<td>The end time of the usage interval for the resource.</td>
</tr>
<tr>
<td>product/service</td>
<td>The service that the resource is in.</td>
</tr>
<tr>
<td>product/compartmentId</td>
<td>The ID of the compartment that contains the resource.</td>
</tr>
<tr>
<td>product/compartmentName</td>
<td>The name of the compartment that contains the resource.</td>
</tr>
<tr>
<td>product/region</td>
<td>The region that contains the resource.</td>
</tr>
<tr>
<td>product/availabilityDomain</td>
<td>The availability domain that contains the resource.</td>
</tr>
<tr>
<td>product/resourceId</td>
<td>The identifier for the resource.</td>
</tr>
<tr>
<td>usage/billedQuantity</td>
<td>The quantity of the resource that has been billed over the usage interval.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> billedQuantity, myCost, and unitPrice are inclusive of overage numbers.</td>
</tr>
<tr>
<td>cost/billingUnitReadable</td>
<td>The unit measure associated with the usage/billedQuantity.</td>
</tr>
<tr>
<td></td>
<td>Example: ONE GiB MONTH DATA_TRANSFERRED.</td>
</tr>
<tr>
<td>cost/subscriptionId</td>
<td>A unique identifier associated with your commitment or subscription.</td>
</tr>
<tr>
<td>cost/productSku</td>
<td>The Part Number for the resource in the line.</td>
</tr>
<tr>
<td>product/description</td>
<td>The product description for the resource in the line.</td>
</tr>
<tr>
<td>cost/unitPrice</td>
<td>The cost billed to you for each unit of the resource.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> billedQuantity, myCost, and unitPrice are inclusive of overage numbers.</td>
</tr>
<tr>
<td>cost/myCost</td>
<td>The cost charged for this line of usage.</td>
</tr>
<tr>
<td></td>
<td>myCost = usage/billedQuantity * unitPrice.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> billedQuantity, myCost, and unitPrice are inclusive of overage numbers.</td>
</tr>
<tr>
<td>cost/currencyCode</td>
<td>The currency code for your tenancy.</td>
</tr>
<tr>
<td>usage/billedQuantityOverage</td>
<td>The usage quantity for which you were billed.</td>
</tr>
<tr>
<td>cost/unitPriceOverage</td>
<td>The cost per unit of usage for overage usage of a resource.</td>
</tr>
<tr>
<td>cost/myCostOverage</td>
<td>The cost billed for overage usage of a resource.</td>
</tr>
<tr>
<td>lineItem/backReference</td>
<td>Data amendments and corrections reference. If a correction is needed, a new row is added with the corrected values and a reference to the original line.</td>
</tr>
</tbody>
</table>
Service Essentials

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lineItem/isCorrection</td>
<td>Used if the current line is a correction. See the lineItem/backReference</td>
</tr>
<tr>
<td></td>
<td>column for a reference to the corrected line item.</td>
</tr>
<tr>
<td>tags/</td>
<td>The report contains one column per tag definition (includes all tag</td>
</tr>
<tr>
<td></td>
<td>definitions, not just cost tracking tags).</td>
</tr>
</tbody>
</table>

**How Usage Reports Work**

The usage report is automatically generated daily, and is stored in an Oracle-owned Object Storage bucket. It contains one row per each Oracle Cloud Infrastructure resource (such as instance, Object Storage bucket, VNIC) per hour along with consumption information, metadata, and tags. Usage reports generally contain 24 hours of usage data, although occasionally a usage report may contain late-arriving data that is older than 24 hours.

**Note:**

If you change any cost tracking tags during a particular hour time slot, the last cost tracking tag that is chosen is what gets applied to that hour. For example, if you changed a tag from "AAA" to "BBB" at 10:40, the usage for 10:00-11:00 would reflect "BBB" for the tag. In addition, tags cannot be applied retroactively.

The report may contain corrections. Corrections are added as new rows to the report, with the lineItem/isCorrection column set and the referenceNo value of the corrected line populated in the lineItem/backReference column.

Usage reports are retained for one year.

The file name for each usage report is appended with an automatically incrementing numerical value.

**Usage Report Schema**

The following table shows the usage report schema.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lineItem/referenceNo</td>
<td>Line identifier. Used for debugging and corrections</td>
</tr>
<tr>
<td>lineItem/TenantId</td>
<td>The identifier (OCID) for the Oracle Cloud Infrastructure tenant.</td>
</tr>
<tr>
<td>lineItem/intervalUsageStart</td>
<td>The start time of the usage interval for the resource in UTC.</td>
</tr>
<tr>
<td>lineItem/intervalUsageEnd</td>
<td>The end time of the usage interval for the resource in UTC.</td>
</tr>
<tr>
<td>product/service</td>
<td>The service that the resource is in.</td>
</tr>
<tr>
<td>product/resource</td>
<td>The resource name used by the metering system.</td>
</tr>
<tr>
<td>product/compartmentId</td>
<td>The ID of the compartment that contains the resource.</td>
</tr>
<tr>
<td>product/compartmentName</td>
<td>The name of the compartment that contains the resource.</td>
</tr>
<tr>
<td>product/region</td>
<td>The region that contains the resource.</td>
</tr>
<tr>
<td>product/availabilityDomain</td>
<td>The availability domain that contains the resource.</td>
</tr>
<tr>
<td>product/resourceId</td>
<td>The identifier for the resource.</td>
</tr>
<tr>
<td>usage/consumedQuantity</td>
<td>The quantity of the resource that has been consumed.</td>
</tr>
<tr>
<td>usage/billedQuantity</td>
<td>The quantity of the resource that has been billed over the usage interval.</td>
</tr>
<tr>
<td>usage/consumedQuantityUnits</td>
<td>The unit for the consumed quantity and billed quantity.</td>
</tr>
</tbody>
</table>
**Accessing Cost and Usage Reports**

Cost and usage reports are comma-separated value (CSV) files that are generated daily and stored in an Object Storage bucket. This topic describes how to access these reports.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

To use cost and usage reports, the following policy statement is required:

```
define tenancy usage-report as
  ocid1.tenancy.oc1..aaaaaaaaaned4fkpksbwjl56u7cj63lf3wffbilvqknstgtvzub7vhkqggq
endorse group <group> to read objects in tenancy usage-report
```

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Using the Console**

To download a cost or usage report:

1. Open the navigation menu. Under Governance and Administration, go to Account Management and select Cost and Usage Reports.
2. Click the report you want to download from the list, and follow your browser's instructions for downloading.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Service Essentials

To download a cost or usage report, use the Object Storage APIs. The reports are stored in the tenancy's home region.
The Object Storage namespace used for the reports is bling; the bucket name is the tenancy OCID.
The following example shows how to download a cost report, usage report (or both) using a Python script:

import oci
import os
# This script downloads all of the cost, usage, (or both) reports for a
tenancy (specified in the config file).
#
# Pre-requisites: Create an IAM policy to endorse users in your tenancy to
read cost reports from the OCI tenancy.
#
# Example policy:
# define tenancy reporting as
ocid1.tenancy.oc1..aaaaaaaaned4fkpkisbwjlr56u7cj63lf3wffbilvqknstgtvzub7vhqkggq
# endorse group group_name to read objects in tenancy reporting
#
# Note - The only value you need to change is the group name. Do not change
the OCID in the first statement.
reporting_namespace = 'bling'
# Download all usage and cost files.
specific need:
prefix_file = ""
# prefix_file = "reports/cost-csv"
# prefix_file = "reports/usage-csv"

You can comment out based on the
#
#
#

For cost and usage files
For cost
For usage

# Update these values
destintation_path = 'downloaded_reports'
# Make a directory to receive reports
if not os.path.exists(destintation_path):
os.mkdir(destintation_path)
# Get the list of reports
config = oci.config.from_file(oci.config.DEFAULT_LOCATION,
oci.config.DEFAULT_PROFILE)
reporting_bucket = config['tenancy']
object_storage = oci.object_storage.ObjectStorageClient(config)
report_bucket_objects = object_storage.list_objects(reporting_namespace,
reporting_bucket, prefix=prefix_file)
for o in report_bucket_objects.data.objects:
print('Found file ' + o.name)
object_details = object_storage.get_object(reporting_namespace,
reporting_bucket, o.name)
filename = o.name.rsplit('/', 1)[-1]
with open(destintation_path + '/' + filename, 'wb') as f:
for chunk in object_details.data.raw.stream(1024 * 1024,
decode_content=False):
f.write(chunk)
print('----> File ' + o.name + ' Downloaded')

Cost Analysis Overview
Cost Analysis is an easy-to-use visualization tool to help you track and optimize your Oracle Cloud Infrastructure
spending, allows you to generate charts, and download accurate, reliable tabular reports of aggregated cost data on

Oracle Cloud Infrastructure User Guide

282


your Oracle Cloud Infrastructure consumption. Use the tool for spot checks of spending trends and for generating reports. Common scenarios you might be interested in include:

- Show monthly costs for compartment X and its children, grouped by service or by tag.
- Show daily costs for tag key A and tag key B, values X, Y and Z, grouped by service and product description (SKU).
- Show hourly costs for service = compute or database, grouped by compartment name.

You can choose the dates you’re interested in. Filter to the specific tags, compartments, services, or filter you want, and pick how you want it grouped. As a result, a chart and corresponding data table are generated, and can also be downloaded as a data table.

If you want to re-create the breakdown provided by the former Classic Version of the Cost Analysis tool, apply the SKU (Part Number) grouping dimension in the current version of Cost Analysis. To explore your costs in new ways, we recommended viewing your costs based on Service, or Service and Product Description. If you are doing cost tracking, we recommended grouping by Compartment or Tag.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>All tags, not only cost tracking tags, are supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs for tags are based on the date at which the tag was associated with a resource. It does not work retroactively for resources on which these tags are applied.</td>
</tr>
</tbody>
</table>

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

To use Cost Analysis, the following policy statement is required:

```
Allow group <group_name> to read usage-report in tenancy
```

### Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

### Cost Analysis Query Fields

The following table describes the Cost Analysis query fields.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Time Period (UTC)       | Allows you to query predefined time ranges for data available in the usage store. Other time ranges can be queried using the Classic Version. The available options in the drop-down (for example, **This Month, Last Month**) are according to the UTC time zone, and are based on the calendar year. The actual time ranges are indicated in parentheses. When changing the time period, it is also indicated just above the chart. Granularity (hourly, daily, monthly) is based on the requested date range size. The logic is the following:  
  - Hourly: 48 hours or less  
  - Daily: > 48 hours, <= 2 months  
  - Monthly: > 2 months  
  **Note:** Historical data is currently being back-filled for tenancies and may not appear immediately. As that process completes, up to twelve months of past consumption data will become available. |
| Show                    | Allows you to view the report in terms of **Cost** (the default) or **Usage**. To view **Usage** you must apply a filter for a unit, by selecting one from the **Filters** field, then via the **Show Usage Info** dialog box. Oracle Cloud Infrastructure services have unit measures that span from GBs/month to CPU/hours to API requests. When selecting **Usage**, a dialog appears, which prompts you to add a filter for a unit to view usage data.  
  **Note:** For **Usage**, unit filtering is the only possible selection, and you can only choose one value for the unit. |
| Cumulative              | Select this option to modify the values so that they’re cumulative for the selected time period selected. For example, consider if you were looking at 10 days of data, cumulatively, and the values for each day are $5. In such a case, selecting **Cumulative** displays values of 5, 10, 15, 20, 25, 30, 35, 40, 45, and 50 across the 10 days, respectively. In a non-cumulative chart, the values display as 5, 5, 5, 5, 5, 5, 5, 5, 5.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filters    | Allows filtering on the following:  
  • Availability domain  
  • Compartment  

  **Note:**  
  Filtering by compartment displays usage and costs attributed to all resources in the selected compartments, and their child compartments.  
  • By OCID  
  • By Name  
  • By Path (for example, root/compartmentname/compartmentname)  
  • Platform (Gen-1 are services which are not OCI native. Gen-2 includes all OCI native services)  
  • Tag  
  • By Tag Namespace  
  • By TagKey + Value  
  • Region  
  • Service  
  • Product description (the human-readable corresponding name)  
  • SKU - Part Number (for example, B91444)  
  • Unit  

  See Filters for more information on adding, editing, and removing filters, and filter logic. |
**Field Name** | **Description**
---|---
Grouping Dimensions | Allows visualizing the data in terms of the particular grouping. A grouping dimension by **Service** is displayed by default. You can view only one grouping dimension at a time.

- **Availability domain**
- **Compartment.** When you choose to group by compartment, you can pick the display name value, and a compartment depth. The compartment depth corresponds to the lowest level you want the compartments to be grouped by. All levels above that grouping level return just what is directly in those compartments. The grouping level returns values for all resources in those compartments, plus all resources in compartments below it.

- **Display As**
  - Display as Compartment Name
  - Display as Compartment OCID
  - Display as Compartment Path

**Note:**
If Compartment OCID or Compartment Name are chosen, you cannot view Compartment Level.

- **Compartment Level**
  - **All** (the default): Every compartment is displayed. Values would display usage/spend associated only with the resources in that specific compartment.
  - **Level 1** (root only): Only 1 column is returned (root), and values for resources contained in root and every child compartment are displayed.
  - **Level 2** (root/<value>): Displays root, with values for root equaling only those resources in root. All compartments that are direct children of root are also returned. The values for each of those compartments is the sum of all resources therein, or within any children of those compartments.
  - **Level 3** (root/<value>/<value>): Returns root, with values for root equaling only those resources in root. All Level 2 compartments are also returned, but with values only equal to the resources contained in each of those specific compartments. The first child level of the level 2 compartments are also returned. The values for the third level of compartment (root/child1/child2 <<) would be equal to the resources in those compartments, plus all the resources in all the children of those compartments.
  - **Level 4** (root/<value>/<value>/<value>)
  - **Level 5** (root/<value>/<value>/<value>/<value>)

- **Platform** (Gen-1 are services which are not Oracle Cloud Infrastructure native, while Gen-2 includes all native Oracle Cloud Infrastructure services)
- **Region**
- **Resource OCID**
- **Service**
- **Service and Product Description**
- **SKU - Part Number**
- **SKU - Product Description**
- **Tag**
- **Unit**

See Grouping Dimensions for more information on viewing and changing grouping dimensions.
**Viewing and Working with the Chart Data**

When the Cost Analysis page first loads, the default view is to show a grouping of services for the **This Month** time period, grouped by **Service**. The Cost Analysis chart is organized in terms of time (UTC) on the X-axis, and the cost amount on the Y-axis. When viewing a chart, you can hover the mouse over a data point in the chart to see more information about it. The tooltip shows the cost value summary for the particular Y-axis item at a particular time, whether you are viewing the chart as either a **Bars** (the default), **Lines**, or **Stacked Lines** chart.

To the right of the chart, the **Legend** box shows all the data by default, and each item is color-coded. You can click the eye icon next to any of the **Legend** items to toggle the chart data on or off. For example, when viewing a chart with various services and their costs, the **Legend** box includes all the impacted services related to the query. Toggling one or more of the services shows or hides them dynamically from the chart output. Toggling the **Legend** data, however, does not change the data shown in the table view, or what is downloaded.

When viewing a chart, you can also add filters or grouping dimensions (or both), to view the cost data according to one or more filters, or in terms of both filters and a single grouping dimension.

A tabular view of the chart is also provided under the chart, which is updated as you apply different time period, filtering, and grouping dimension options. When viewing the table data, you can click the column header to sort in ascending or descending order.

**Note:**

Data can take up to 48 hours to appear in Cost Analysis.

**Filters**

See the following for instructions on how to add, edit, and remove filters, as well filter logic.

**To add filters**

1. Open the navigation menu. Under **Governance and Administration**, go to **Account Management** and click **Cost Analysis**.

2. From **Time Period (UTC)**, select a time period.

3. From **Show**, select whether you want to view **Cost** or **Usage**.

4. Choose from three chart types, whether **Bars** (the default), **Lines**, or **Stacked Lines**.

5. From **Filters**, select a filter. A dialog specific to the chosen filter is displayed. For example, if you chose **Service**, select a service from the drop-down menu. You can add multiple services if preferred, or click the **X** icon to remove service filters. Click **Select** when you are finished selecting filtering criteria.

6. Click **Apply** to apply the changes and reload the chart and table with the selected filters.

**To edit a filter**

1. To edit the filter after it has already been applied to the chart, click the filter. The filter's dialog box is displayed.

2. From the filter dialog drop-down menu, select one or more filters, and click **Select**.

3. Click **Apply** to apply the changes and reload the chart and table with the selected filters.

**To remove a filter**

1. To remove the filter after it has been applied to the chart, click **Clear All Filters**, or click the filter's **X** icon under **Filters**.

2. Click **Apply** to apply the changes and reload the chart and table without the selected filters.

**Filter Logic**

Filters are ORed within each specific filter, and ANDed between filters. For example, a filter for **Service** = Compute, Block Storage, Object Storage, Database, and **Tag** = **Tag Key** "MyKey" displays data that is for (Compute OR Block Storage OR Object Storage OR Database) AND **Tag Key** "MyKey".

The Tag filter, however, is a unique case. You can add multiple Tag filters, which function as a joined OR.
Using Multiple Filters to View Costs

You can start by filtering the Cost Analysis chart data based on a single filter, and then add additional filters. For example:

1. Set your Grouping Dimensions on page 288 to Service, to view your costs by service.
2. From Filters, add a filter by Tag.
3. Select a Tag Namespace (this example uses "Financial" as the selected namespace).
4. Select a Tag Key (this example uses "Owner" as the selected key).
5. Specify whether to Match any value (AND condition), or Match any of the following (OR condition).

For example, assuming the value "alpha" is the value, and if Match any of the following is chosen, it means show all services that have "alpha" as the owner. Conversely, assuming multiple values "alpha" and "beta" are chosen, and if Match any of the following is selected, this corresponds to an OR condition (meaning, filter to show the costs from all the services from the "Financial" namespace, with the Tag Key "Owner", that matches either the "alpha" or "beta" values).

6. Click Select, then Apply to reload the Cost Analysis chart with the filtered information.

You can also add another filter by tag, to break the data down further. For example:

1. From Filters, add a filter by Tag.
2. Select a Tag Namespace (for example, the "Cost Center" namespace).
3. Select Match any of the following, and for example, filter for any "Cost Center" values of "1234" or "5678".

After clicking Select, then Apply, this filter shows the costs from all the services with the previous tag filter, plus this second tag filter ("Financial" namespace, Tag Key "Owner", "alpha" or "beta" values + "Cost Center" namespace with the values of "1234" or "5678"). The two tag filters together amount to an AND with the previous filter (the two filters are shown adjacent to the Add Filter drop-down list).

Alternatively, instead of this second tag filter ("Cost Center" namespace with the values of "1234" or "5678"), you could add a service filter (NETWORK), and that would show the costs from all the services from the "Financial" namespace, with the Tag Key "Owner", that matches both the "alpha" or "beta" values, and is filtered by the NETWORK service type.

Grouping Dimensions

See the following for instructions on how to view and change grouping dimensions. Grouping dimensions change the way data is aggregated, but does not change the sum. If a resource does not have a value for a particular field, a "no value" column is displayed, which reflects the sum of those resources. Specifically, products which are Gen-1 often do not have an Availability Domain, Compartment, or Resource ID.

To view grouping dimensions

1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Cost Analysis.
2. From Time Period (UTC), select a time period.
3. From Show, select whether you want to view Cost or Usage.
4. Choose from three chart types, whether Bars (the default), Lines, or Stacked Lines.
5. From Grouping Dimensions, select the preferred grouping dimension. If Compartment or Tag is chosen, additional Compartment or Tag selection fields appear.
6. Click Apply to apply the changes and reload the chart and table with the selected grouping dimension.

To change a grouping dimension

1. To change the grouping dimension, select it from Grouping Dimensions.
2. Click **Apply** to apply the changes and reload the chart and table with the new grouping dimension.

**Identifying a Resource that is Consuming Costs**

If you have noticed a large amount of, for example, Database service usage that has appeared in a chart, and you wanted to identify which resource was responsible, you can group by **Resource OCID** from the **Grouping Dimensions** drop-down list. Next, from **Filters**, add a filter for the service type (**Database** in this example), and click **Apply** to reload the chart.

The chart reloads to show which resource OCIDs were driving the Database cost, both when hovering over the data point in the chart, and in the **Legend** box. These resource OCIDs are also displayed in the data table below the chart. If desired, you can save this information by clicking **Download**, and then selecting **Download Table as CSV**.

**Tip:**

The **Legend** box is set to a default size when the charts first loads, but you can click and drag the box to more easily read lengthy items within it (such as OCIDs).

To find more information about the resource, copy the OCID and enter it in the Console’s Search box, to pinpoint which resource is driving costs.

**Grouping by Service and SKU, or Service and Product Description to Identify Costs**

In some instances you may see multiple SKU numbers for a service. When grouping by **Service and SKU (Part Number)**, multiple SKU numbers for the same service appear in the **Legend** box. For example, if you had multiple Compute entries in the **Legend** box but they have different SKUs, it means there is one resource using multiple underlying infrastructure components. This case is actually most common for Block Storage (where multiple Block Storage entries appear with different SKUs). Specifically, for the Block Storage case, you are charged for storage itself, but you are also charged for any data transfers out of Block Storage. As a result, you will see multiple "Block Storage" items listed with different SKU numbers in the **Legend** box. For example:

```
Block Storage / <SKU number 1>
Block Storage / <SKU number 2>
Block Storage / <SKU number 3>
Block Storage / <SKU number 4>
```

Another way of looking at this same type of data is to use the **Service and Product Description** grouping dimension. The **Legend** box is sorted in the same manner, but presents the data differently. That is, according to the actual product descriptions, versus the SKUs that these are associated with. For example:

```
Block Storage / Block Volume - Backup
Block Storage / Block Volume - Free
Block Storage / Block Volume - Performance Units
Block Storage / Block Volume - Storage
```

**Tip:**

By default, these longer descriptions may not be visible, and so you should resize the **Legend** box to view them.

The Database service is also a useful example. There could be different instances of a database and you could also be charged for Block Storage within the Database service. For example, this entry could appear in the **Legend** for such a case:

```
Database / DBaaS - Attached Block Storage Volume - Standard Performance
```

You could also be charged in the Database service for network transfer. For example:

```
Database / Oracle Autonomous Data Warehouse - Exadata Storage
```

Charges for licensing of the application version can also occur:
Cost and Usage reports are a good way to further slice such information you have noticed in the Cost Analysis charts. For example, in a cost report you might notice a SKU number that's associated with Compute, and also see the same SKU number that's associated with Block Storage. As a result, you may wonder if you were double-billed (though this is actually not the case). To investigate the actual cost, you can first filter the cost CSV spreadsheet by the SKU. Once you have applied a filter to the CSV using a particular SKU, you can see which services are consuming from the product/Description column. For example, a SKU could be using a lot of "Block Volume - Performance Units", but you also notice that "DBaaS - Attached Block Storage Volume" appears in this column.

A way to further segment the data would be to copy the resource ID from the product/resourceid column, of say the "DBaaS - Attached Block Storage Volume" entry you noticed amongst all the "Block Volume - Performance Units", and remove the SKU filter you applied previously. Next, filter the spreadsheet based on the resource ID instead. This then shows all the components (indicated in the product/Description column) that the particular resource ID is consuming.

Note:
When viewing a cost report, the cost/productSku and product/description columns map to one another, and are adjacent columns in the CSV. For more information on these fields and other fields that appear in the reports, see Cost and Usage Reports Overview on page 278.

Similarly, you can use Cost Analysis to do a Resource OCID grouping dimension, with a Product description filter, to show all the resources that are using a particular product. For example, if you choose Block Volume - Performance Units as the filter, the Cost Analysis chart shows which resources are using "Block Volume - Performance Units". See Identifying a Resource that is Consuming Costs on page 289 for more information on identifying the particular resource(s).

Download Your Data
Click the Download button to download a CSV file of the data, or a PNG file of the chart. Downloading generates a file that corresponds to the chart or table on the Cost Analysis page, inclusive of applied filters, sorting, and grouping dimensions.

Using the Usage API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage usage:
• UsageSummary
• RequestSummarizedUsages

The Usage API allows retrieval of usage and cost data. You can:
• Query based on different granularity, for example, MONTHLY or DAILY.
• Specify queryType, for example, COST, USAGE.
• Filter and group by different dimension/tags, functioning like an SQL query.
• Use up to four groupBy parameters.

The following is a sample Usage endpoint URI that conforms to the schema:
• https://usageapi.<region>.oci.oraclecloud.com/20200107/usage

For more information about the API and to view the full list of endpoints, see the Usage API.
Using granularity

The Usage API supports: MONTLY, DAILY, and HOURLY granularity. All startTime are inclusive, and endTime are exclusive, the same as a Java substring.

- For HOURLY, only a maximum 36-hour time period is supported, with no more precision than an hour. This means no minutes or seconds in the input time.
- For MONTHLY, only the first date of the month to another first date of the month is supported. For example, 2020-06-01T00:00:00Z, a maximum 12-month period.
- For DAILY, no more precision than a day is supported, with a maximum 90-day period. You must enter this as 00:00:00. For example, 2020-06-01T00:00:00Z.

Using groupBy

In an API response, dimension is only shown in terms of groupBy. For example, if "service" isn't in groupBy, the "service" field in the response will be empty.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only four groupBy parameters can be used at a time.</td>
</tr>
</tbody>
</table>

In addition:

- If a groupBy list is empty, "currency" will be added into groupBy.
- If the queryType is "Usage", "unit" will be add into groupBy.
- If the queryType is "COST" or "empty", "currency" will be add into groupBy.
- computedAmount works as expected only when "currency" is in groupBy.
- computedQuantity works as expected only when "unit" is in groupBy.

Using queryType

The API can query USAGE or COST. computedQuantity represents usage and computedAmount represents cost. For getting the expected usage, you need to set queryType to USAGE or add "unit" in groupByKey. This is due to the fact that usage is aggregated/grouped correctly when grouping by unit.

Using filtering

Nested filtering in API requests is supported. The list of filters are evaluated by the operator. In each filter, all dimensions and tags are evaluated by the operator. Simultaneous evaluation of the filter list and dimension/tags is not supported, which means dimensions or tags and the filter list can't be non-empty at the same time.

Supported operators are AND, OR. These two filters below are equal:

```
"filter": {
  "operator": "AND",
  "dimensions": [
    {
      "key": "service",
      "value": "compute"
    },
    {
      "key": "compartmentPath",
      "value": "abc/cde"
    }
  ],
  "tags": [
    {
      "namespace": "compute",
      "key": "created",
      "value": "string"
    }
  ]
```

Invalid example because dimensions and filters are non-empty at the same time:

```
"filter": {
  "operator": "AND",
  "dimensions": [{
    "key": "compartmentPath",
    "value": "abc/cde"
  }],
  "tags": [],
  "filters": [
    {
      "operator": "AND",
      "dimensions": [{
        "key": "service",
        "value": "compute"
      }],
      "tags": null,
      "filters": null
    },
    {
      "operator": "AND",
      "dimensions": [{
        "key": "compartmentPath",
        "value": "abc/cde"
      }],
      "tags": null,
      "filters": null
    },
    {
      "operator": "AND",
      "dimensions": null,
      "tags": [{
        "namespace": "compute",
        "key": "created",
        "value": "string"
      }],
      "filters": null
    }
  ]
}
```
Querying with tags

As mentioned previously, we only show the field in `groupBy`. So you need to add tag related fields in `groupBy`. For example:

```
"tagNamespace", "tagKey", "tagValue"
```

If you add `tagKey`, all items in the response will have a `tagKey`. `tagKey` also can be empty even if you add a `tagKey`. This is because some of your resources don't have a `tagKey`. We suggested adding all three of these in `groupBy`, so you can see a complete tag in the response:

```
"tagNamespace", "tagKey", "tagValue"
```

If you want to filter by tag, you need to add the tag in the filter object. This can be filtered by any `tagKey/_namespace/value` combination of any `tagKey/namespace/value`.

**Valid `groupBy` example**

```
"tagNamespace", "tagKey", "tagValue", "service", "skuName", "skuPartNumber", "unit", "compartmentName", "compartmentPath", "compartmentId", "platform", "region", "logicalAd", "resourceId", "tenantId", "tenantName"
```

**Note:**

Only up to four `groupBy` parameters can be used in an API call.

"tenantId" and "tenantName" are not currently supported.

**Valid filter dimension example**

```
"service", "skuName", "skuPartNumber", "unit", "compartmentName", "compartmentPath", "compartmentId", "platform", "region", "logicalAd", "resourceId", "tenantId", "tenantName"
```

This is case-sensitive. "tenantId" and "tenantName" are not currently supported.

**How to `groupBy` compartment?**

`groupBy` compartment-related keys ("compartmentName", "compartmentPath", "compartmentId") are different than the other `groupBy` keys.

To get an expected result, you must request with `compartmentDepth`. `compartmentDepth` is >=1 and <=6.

`groupBy` compartment means all compartments usage or costs with a higher depth will be aggregated to the compartment with the given depth. For example:

<table>
<thead>
<tr>
<th>Compartment</th>
<th>Depth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>
If the depth is 1, it means all usage or costs are grouped to the root compartment.

If the depth is 2, it means all compartments with depth 2 will contain the usage or costs with all its children. In the response, the root will contain its own usage, B will aggregate (B, D, E, F), and C will contain C.

**Why are some fields in a response empty?**

The fields will show up only when the fields are in `groupBy`. Not all fields in the response are currently available. Only the fields mentioned in [Valid groupBy example](#) on page 293 are supported.

**What is nextPageToken?**

This can be set as null. Currently not supported.

**Example request body**

The best way to understand how the API works is checking how the Console uses the API. You can find the request body in the web browser's debug mode.

```json
{
    "tenantId": "oci1.tenancy.oc1..<unique_ID>",
    "timeUsageStarted": "2020-04-01T00:00:00.000Z",
    "timeUsageEnded": "2020-07-01T00:00:00.000Z",
    "granularity": "MONTHLY",
    "queryType": "COST",
    "groupBy": [
        "tagNamespace",
        "tagKey",
        "tagValue",
        "service",
        "compartmentPath"
    ],
    "compartmentDepth": 2,
    "filter": null
}
```

After you make a request without any filter, you can see what the dimension/tags' value can be. Subsequently, you can make a request with a filter and a correct dimension value.

```json
{
    "tenantId": "oci1.tenancy.oc1..<unique_ID>",
    "timeUsageStarted": "2020-04-01T00:00:00.000Z",
    "timeUsageEnded": "2020-07-01T00:00:00.000Z",
    "granularity": "MONTHLY",
    "groupBy": ["tagNamespace","tagKey","tagValue","service","compartmentPath"],
    "compartmentDepth": 2,
    "filter": {
        "operator": "AND",
        "dimensions": [],
        "tags": [],
        "filters": [
            {
                "operator": "AND",
                "dimensions": [
                    {"key": "service",
                     "value": "compute"
                    }],
                "tags": null,
```
Using customized scripts, CLI, and SDK

If you write a customized script, Oracle does not support or assist with debugging your script. Only the CLI, SDK, and Terraform are supported. See 3. Create and Configure a Copy of oci-curl on page 2050 for more information on using customized scripts, and Command Line Interface (CLI) on page 4192 for more information. For example:

```bash
--request-body
file:///<system_path>/SimpleRequestSummarizedUsagesDetails.json
--config-file ~/Downloads/clitest.conf
```

**SimpleRequestSummarizedUsagesDetails.json:**

```json
{
    "tenantId": "oci1.tenancy.oc1..<unique_ID>",
    "timeUsageStarted": "2020-03-19T17:00:00.000000-07:00",
    "timeUsageEnded": "2020-03-21T00:00:00Z",
    "granularity": "DAILY",
    "groupBy": [],
    "compartmentDepth": null,
    "filter": null,
    "nextPageToken": "string"
}
```

**clitest.conf:**

```ini
[DEFAULT]
user=oci1.user.oc1..<unique_ID>
fingerprint=<MAC_ID>
key_file=<system_path>/oci_api_key.pem
#tenancy=oci1.tenancy.oc1..<unique_ID>
tenancy=oci1.tenancy.oc1..<unique_ID>
region=us-ashburn-1
```

Unified Billing Overview

This topic describes how you can unify billing across multiple tenancies by sharing your subscription. You should consider sharing your subscription if you want to have multiple tenancies to isolate your cloud workloads, but you want to have a single Universal Credits commitment. For example, you have a subscription with a $150,000 commitment, but you want to have three tenancies, because the credits are going to be used by three distinct groups that require strictly isolated environments.

Two types of tenancies are involved when sharing a subscription in the Console:

- The parent tenancy (the one that is associated with the primary funded subscription).
- Child tenancies (those that are consuming from a subscription that is not their own).

Notable benefits of sharing a subscription includes:

- Sharing a single commitment helps to avoid cost overages and allows consolidating your billing.
- Enabling multi-tenancy cost management. You can analyze, report, and monitor across all linked tenancies. The parent tenancy has the ability to analyze and report across each of your tenancies through Cost Analysis and Cost and usage reports, and you can receive alerts through Budgets.
- Isolation of data. Customers with strict data isolation requirements can use a multi-tenancy strategy to continue restricting resources across their tenancies.

The remainder of this topic provides an overview of how to share your subscription between tenancies, and provides best practices on how to isolate workloads, in order to help you determine if you should use a single-tenancy or multi-tenancy strategy.

Planning Considerations

Before you get additional tenancies you should evaluate your needs to make sure that a multi-tenancy approach is best for your workloads. The main reason to have multiple tenancies is for strong isolation. By default, each parent and child tenancy comes with:

- A distinct set of IAM users (which can be federated to another identity system).
- A distinct set of IAM policies (permissions).
- Its own service limits.
- Isolated Virtual Cloud Networks (VCNs).
- Separate security and governance settings.

The main point to be aware of is that multiple tenancies make it easier to isolate workloads, but that comes at the cost of needing to manage multiple tenancies. Additional tenancies, however, do create additional management overhead, so you need to ensure that the isolation is worth it. If you don't require a strong level of isolation, you should consider using compartments to separate workloads.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

To use subscription sharing, the following policy statements are required:

- Allow group linkUsers to use organizations-family in tenancy
- Allow group linkAdmins to manage organizations-family in tenancy

To accept an invitation but not create one use the following:

- allow group linkAccepters to manage organizations-recipient-invitations in tenancy
Subscription Sharing Overview

Depending on whether or not you already have multiple tenancies, there are two approaches:

If you don't already have an additional tenancy

1. Sign up for a new PAYG (pay as you go) subscription to get a new tenancy. You do not incur any charges against the PAYG subscription, as long as you link it with your existing subscription before creating any billable resource. There are two ways to get a new PAYG subscription:
   a. Self-service: Sign up for a new trial using http://signup.oracle.com, and upgrade the trial to a paid account.
   b. Through sales: Work with your Oracle sales team to book a new PAYG order.
2. Take note of the tenancy OCID in the new tenancy. You can find it on the Tenancy Details page in the Console. This page can be accessed by opening the Profile menu and then selecting Tenancy: <your_tenancy_name>. See the OCID field on the Tenancy Information tab.
3. From the tenancy that owns the primary subscription, invite the new tenancy to share the subscription (described in To Share a Subscription).

If you already have multiple tenancies

There are two paths you can take:

• If you have one primary tenancy that has a Universal Credits Flex (commitment) subscription and your subsequent tenancies have a PAYG subscription, you can follow the steps in If you don't already have an additional tenancy to get a new tenancy.
• If your tenancies have multiple Universal Credits Flex (commitment), you will need to work with your Oracle sales team to rebalance your commitment balances.

To Share a Subscription

Important:
Ensure that you understand the terms of your contract before sharing your subscription with another tenancy. Your contract specifies how your subscription can be used, and which end users are allowed to use it.

Note:
Rebalancing subscriptions is a manual process that needs to be coordinated, and rebalancing will not be available under all circumstances. Your sales team will work with you to rebalance your subscriptions and set up the parent-child billing relationship.

1. Sign in to the sender tenancy that will send the invitation, as a user that has permissions to manage subscription sharing.
2. Open the navigation menu. Under Governance and Administration, go to Account Management and click Subscription Sharing. The Subscription Sharing page is displayed.
3. Click Invite Tenancy. The Invite Tenancy panel is displayed.
4. Enter the invitation details. You will need to specify the following:
   • The invitation name in Invitation Name. For the invitation name, it can be helpful to use notation that signifies the direction and number of sending invitation attempts. For example, entering a1 to b1 v1 can
signify that tenancy a1 is sending an invitation to b1 and v1 as the first attempt. Such a convention allows the invitations to be more readable to the Console user, without having to access the Invitation Detail page to view sender and recipient details.

- The child tenancy OCID in Recipient Tenancy OCID.
- Optionally, an email address in Recipient Email, to notify that a sharing invitation has been sent.

**Note:**
The recipient needs to have the proper permissions to manage subscription sharing in the child tenancy, in order to accept the invitation. For more information, see Required IAM Policy on page 296.

- Optionally, enter tagging information.

5. Click Send Invitation. The invitation is sent to the tenancy you are inviting to share the subscription with.

**Note:**
Parent tenancies and tenancies that are not already in a sharing relationship can send invitations. Child tenancies cannot send invitations.

6. On the recipient (child) tenancy: Open the navigation menu. Under Governance and Administration, go to Account Management and click Subscription Sharing. The Subscription Sharing page is displayed.

7. The invitation from the other tenancy is displayed in the list, with the following information:

- **Invitation Name**: Click this linked name to go to the Invitation Detail page.
- **Status**: Displays the invitation status. For example, it is Active when the invitation is received but not yet accepted. From the parent tenancy, this field shows Pending for an invitation that has been sent but not yet accepted.

The possible status states for a sender and recipient invitation are the following:

<table>
<thead>
<tr>
<th>Sender Invitation</th>
<th>Recipient Invitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>PENDING</td>
<td>PENDING</td>
</tr>
<tr>
<td>CANCELED</td>
<td>CANCELED</td>
</tr>
<tr>
<td>ACCEPTED</td>
<td>ACCEPTED</td>
</tr>
<tr>
<td>EXPIRED</td>
<td>IGNORED</td>
</tr>
<tr>
<td>FAILED</td>
<td>EXPIRED</td>
</tr>
<tr>
<td></td>
<td>FAILED</td>
</tr>
</tbody>
</table>

- **Type**: The invitation type, whether Sent or Received.
- **Created**: The UTC creation date and time of the invitation.

8. Click the Actions icon (three dots) and select Accept Sharing Invitation. An confirmation acceptance message is displayed, which indicates that you are about to accept a subscription sharing invitation from tenancy <OCID>.

After clicking Accept, the invitation is processed, and the invitation's Status field changes to Updating. The tenancy then becomes a child tenancy.

After the sharing invitation is accepted, it will take one to two hours for metering to start flowing to the subscription in the parent tenancy. From that time onwards, however, all usage in the child tenancy will be metered against the parent tenancy's subscription. In addition, after linking tenancies, we recommend you wait
for a few hours before launching resources, that is, if you want to be sure all spending will accrue against the subscription of the parent tenancy.

If there is a remaining subscription balance, contact your sales representative to move it to a primary subscription in the sending tenancy.

Note:
Once the tenancy becomes a child tenancy, it cannot invite another tenancy to become a child tenancy. The Invite Tenancy button on the Subscription Sharing page becomes disabled to reflect this state.

9. Open the child tenancy's Linked Tenancies page, where you can view the linking between the child and parent tenancy. The following information is displayed:

- **Tenancy OCID**: The tenancy OCID.
- **Status**: Displays the invitation status.
- **Established**: The UTC date and time that the subscription sharing began.
- **Terminated**: The UTC date and time that the subscription sharing began. This field is empty if the sharing is still active.

Meanwhile on the parent tenancy's Linked Tenancies page, you can view the (child) tenancies that are being metered against your subscription.

**To Revoke a Subscription Sharing Invitation**

1. Sign in to the primary tenancy as a user that has permissions to manage subscription sharing.
2. Open the navigation menu. Under Governance and Administration, go to Account Management and click Subscription Sharing. The Subscription Sharing page is displayed.
3. For the invitation you want to revoke, click the Actions icon (three dots) and select Revoke Invitation. A Revoke Invitation confirmation is displayed. Click Revoke to cancel the sharing invitation.
4. On the Subscription Sharing page, the invitation’s Status changes to Canceled.

**Viewing Invitation Details**

Invitation details can be viewed from both the parent and child tenancy. To view invitation details:

1. Open the navigation menu. Under Governance and Administration, go to Account Management and click Subscription Sharing. The Subscription Sharing page is displayed.
2. Click the linked invitation name from the Invitation Name field, or click the Actions icon (three dots) and select View Invitation Details. The Invitation Detail page is displayed.
3. This page displays the invitation status, along with the following details on the Invitation Information tab:
   - Sent from Tenancy OCID
   - Type
   - Last Status Change
   - Sent to Tenancy OCID
   - Sent Date

   You can also click Add Tags to add tagging information, and view it on the Tags tab. See Resource Tags on page 211 for more information.

**Using the Organizations API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations in the Organizations API to manage subscription sharing:

- **Link**
Service Essentials

- RecipientInvitation
- SenderInvitation
- WorkRequest
- WorkRequestError
- WorkRequestLogEntry

Cost Reporting

Once a subscription is shared, the behavior of cost reporting tools changes. All spending against the subscription (in the parent and all child tenancies) is included in cost reporting in the parent tenancy, and child tenancies are limited to seeing spending in their own tenancy. Cost and usage reports are generated only in the parent tenancy, and include all usage for the parent and all of its children. Budgets are only supported in the parent tenancy. The following table describes the impact of subscription sharing on cost reporting.

<table>
<thead>
<tr>
<th></th>
<th>Parent Tenancy</th>
<th>Child Tenancies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Analysis</td>
<td>Reports on all usage and cost in the parent, and all children with the ability to group and filter by tenancy.</td>
<td>Reports on all usage and cost in the child tenancy.</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a child tenancy wants to use Cost Analysis from the Console, you must subscribe to the parent’s home region.</td>
</tr>
<tr>
<td>Cost and usage reports (CSVs)</td>
<td>Includes all usage and costs in the parent and all children.</td>
<td>Not available.</td>
</tr>
<tr>
<td>Budgets</td>
<td>Budgets can be created against compartments or tags in the primary tenancy but not against child tenancies.</td>
<td>Not supported.</td>
</tr>
</tbody>
</table>

Support

Depending on how you created your tenancy, you will either have separate CSI (Customer Support Identifier) numbers, and support accounts for each tenancy, or they will be combined. If you want to make sure that you get multiple CSI numbers, ensure that you work with your account team to create tenancies in a way that will create new CSIs.

My Services Use Cases

**Important:**
The My Services dashboard and APIs are deprecated.

To interact programmatically with My Services, you can use the Oracle Cloud My Services API. To help you get started, here are some use cases:

- Service Discovery Use Case on page 300
- Exadata Use Cases on page 303
- Managing Exadata Instances on page 314
- Using Access Token Authorization with My Services API on page 328

Service Discovery Use Case

This use case shows how you can get the list of your service entitlement IDs.
Important:
The My Services dashboard and APIs are deprecated.

Discover Current Service Entitlement IDs

Many of the My Services API operations require you to specify the `serviceEntitlementId`. To get the list of all your service entitlement IDs, use the `GET ServiceEntitlements` operation. This operation returns information that you can use to make more specific requests using the Oracle Cloud My Services API.

Example:

```
GET /itas/<domain>/myservices/api/v1/serviceEntitlements
```

**Note:**

In the examples, `<domain>` is the identity domain ID. An identity domain ID can be either the `IDCS GUID` that identifies the identity domain for the users within Identity Cloud Service (IDCS) or the `Identity Domain name` for a traditional Cloud Account.

Example payload returned for this request:

```
{
   "items": [
      {
         "id": "cesi-511202718", // Unique ServiceEntitlementId
         "purchaseEntitlement": { // Purchase Entitlement is the entity bought by a customer
            "subscriptionId": "511203590",
            "id": "511203590",
            "canonicalLink": "/itas/<domain>/myservices/api/v1/purchaseEntitlements/511203590"
         },
         "serviceDefinition": { // The customer is entitled to use the Storage Service
            "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceDefinitions/500089778",
            "id": "500089778",
            "name": "Storage"
         },
         "createdAt": "2017-12-20T16:23:23.326Z",
         "createdBy": "paul.smith@oracle.com",
         "modifiedAt": "2017-12-20T18:35:40.628Z",
         "modifiedBy": "paul.smith@oracle.com",
         "identityDomain": { // Identity Domain to which the Service Entitlement is associated
            "id": "511203592",
            "name": "myenvironment",
            "displayName": "myenvironment"
         },
         "cloudAccount": { // Cloud Account to which the Service Entitlement is associated
            "id": "cacct-be7475efc2c54995bc842d3379d35812",
            "name": "myenvironment",
            "canonicalLink": "/itas/<domain>/myservices/api/v1/cloudAccounts/cacct-be7475efc2c54995bc842d3379d35812"
         },
         "status": "ACTIVE", // Current Status
      }
   ]
}
```
"serviceConfigurations": { }

Service Essentials

"serviceConfigurations": { // Specific configuration information such as Exadata configuration
  "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/cesi-511202718/serviceConfigurations",
},
  "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/cesi-511202718"
},
{
  "id": "cesi-511202719",
  "purchaseEntitlement": {
    "subscriptionId": "511203590",
    "id": "511203590",
    "canonicalLink": "/itas/<domain>/myservices/api/v1/purchaseEntitlements/511203590"
  },
  "serviceDefinition": {
    "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceDefinitions/500123193",
    "id": "500123193",
    "name": "Compute" // The customer is entitled to use the Compute Service
  },
  "createdOn": "2017-12-20T16:23:23.326Z",
  "createdBy": "paul.smith@oracle.com",
  "modifiedOn": "2017-12-20T18:35:40.628Z",
  "modifiedBy": "paul.smith@oracle.com",
  "identityDomain": {
    "id": "511203592",
    "name": "myenvironment",
    "displayName": "myenvironment"
  },
  "cloudAccount": {
    "id": "cacct-be7475efc2c54995bc842d3379d35812",
    "name": "myenvironment",
    "canonicalLink": "/itas/<domain>/myservices/api/v1/cloudAccounts/cacct-be7475efc2c54995bc842d3379d35812"
  },
  "status": "ACTIVE",
  "serviceConfigurations": {
    "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/cesi-511202719/serviceConfigurations",
  },
  "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/cesi-511202719"
}, ...

Service Entitlements could be displayed

To obtain the IDCS GUID

Go to the Users page in My Services dashboard and click Identity Console. The URL in the browser address field displays the IDCS GUID for your identity domain. For example:

https://idcs-105bbbdfe5644611bf7ce04496073adf.identity.oraclecloud.com/ui/v1/adminconsole/?root=users
In the above URL, idcs-105bbdfe5644611bf7ce04496073adf is the IDCS GUID for your identity domain.

**Exadata Use Cases**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The My Services dashboard and APIs are deprecated.</td>
</tr>
</tbody>
</table>

The following use case examples can get you started working with the Exadata operations available in the Oracle Cloud My Services API.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>These procedures are for use with Oracle Database Exadata Cloud@Customer ONLY. For more information, see Administering Oracle Database Exadata Cloud at Customer. These procedures DO NOT apply to the Exadata Cloud Service available in Oracle Cloud Infrastructure.</td>
</tr>
</tbody>
</table>

**Exadata Firewall Allowlisting**

To enable access to your Exadata Cloud Service instance, you can configure security rules and associate them with your instance. The security rules define an allowlist of allowed network access points.

The firewall provides a system of rules and groups. By default, the firewall denies network access to the Exadata Cloud Service instance. When you enable a security rule, you enable access to the Exadata Cloud Service instance. To enable access you must:

- Create a security group and create security rules that define specific network access allowances.
- Assign the security group to your Exadata Cloud Service instance.

You can define multiple security groups, and each security group can contain multiple security rules. You can associate multiple security groups with each Exadata Cloud Service instance, and each security group can be associated with multiple Exadata Cloud Service instances. You can dynamically enable and disable security rules by modifying the security groups that are associated with each Exadata Cloud Service instance.

To enable access to an Exadata Cloud Service instance:

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the following examples, &lt;domain&gt; is the identity domain ID. An identity domain ID can be either the IDCS GUID that identifies the identity domain for the users within Identity Cloud Service (IDCS) or the Identity Domain name for a traditional Cloud Account.</td>
</tr>
</tbody>
</table>

1. Get the service instance IDs.

   **Operation:** GET ServiceInstances

   **Example**

   **Example request:**

   GET /itas/<domain>/myservices/api/v1/serviceInstances?
   serviceDefinitionNames=Exadata&statuses=ACTIVE

   **Example payload returned for this request:**

   ```json
   {
   "items": [
   {
   "id": "csi-585928949", // Unique ServiceInstanceID
   "serviceEntitlement": {
   ```
This example payload returns the service instance ID csi-585928949, which is part of the service entitlement ID cesi-585927251.

2. Get the service configuration IDs.

Operation: GET SIServiceConfigurations

Example

Example request, using the service instance ID csi-585928949:

GET /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations

Example payload returned for this request:

```json
{
  "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations",
  "items": [
    {
      "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata",
      "exadata": {
        "bursting": {
          "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/bursting"
        },
        "id": "Exadata",
        "securityGroupAssignments": {
          "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments"
        }
      }
    }
  ],
  "hasMore": false,
  "limit": 25,
  "offset": 0
}
```
This example payload shows that /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments is used for Exadata Firewall.

3. Get the current security groups for the service entitlement.

   Operation: GET SEExadataSecurityGroups

   Example

   Example request, using the service entitlement ID cesi-585927251:

   ```
   GET /itas/<domain>/myservices/api/v1/serviceEntitlements/cesi-585927251/serviceConfigurations/Exadata/securityGroups
   ```

   Example payload returned for this request:

   ```
   {
   "items": [
   {
   "id": "1",
   "customerId": "585927251",
   "name": "SecGroup 1",
   "description": "My first Security group",
   "version": 10,
   "rules": [
   {
   "direction": "ingress",
   "proto": "tcp",
   "startPort": 1159,
   "endPort": 1159,
   "ipSubnet": "0.0.0.0/0",
   "ruleInterface": "data"
   }
   ],
   "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/585927251/serviceConfigurations/Exadata/securityGroups/1"
   },
   {
   "id": "2",
   "customerId": "585927251",
   "name": "SecGroup 2",
   "description": "My second Security group",
   "version": 3,
   "rules": [
   {
   "direction": "egress",
   "proto": "tcp",
   "startPort": 8123,
   "endPort": 8123,
   "ipSubnet": "192.168.1.0/28",
   "ruleInterface": "data"
   }
   ],
   "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/585927251/serviceConfigurations/Exadata/securityGroups/2"
   }]
   ```
This example payload shows two security groups defined for the specified service entitlement ID.

4. Get the current security group assignments for the service instance

Operation: GET SIExadataSecurityGroupAssignments

Example

Example request, using the service instance ID csi-585928949:

GET /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments

Example payload returned for this request:

```
{
  "items": [
    {
      "id": "11",
      "securityGroup": {
        "id": "1",
        "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/585927251/serviceConfigurations/Exadata/securityGroups/1",
        "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments/11"
      },
      "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments"
    }
  ],
  "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments"
}
```

This example payload shows one security group assigned to the service instance csi-585928949.

5. Create a security group with security rules.

Operation: POST SExadataSecurityGroups

Example

Example request, using the service entitlement ID cesi-585927251:

POST /itas/<domain>/myservices/api/v1/serviceEntitlements/cesi-585927251/serviceConfigurations/Exadata/securityGroups
{
  "customerId": "585927251",
  "name": "SecGroup 1",
  "description": "My third Security group",
  "version": 1,
  "rules": [
    {
      "direction": "ingress",
      "proto": "tcp",
      "startPort": 30,
      "endPort": 31,
      "ipSubnet": "100.100.100.255",
      "ruleInterface": "admin"
    }
  ]
}
"direction": "egress",
"proto": "tcp",
"startPort": 32,
"endPort": 32,
"ipSubnet": "100.100.255.0/16",
"ruleInterface": "admin"
}
]

Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>customerId</td>
<td>Required: Yes&lt;br&gt;String&lt;br&gt;This must be the same as the &lt;serviceEntitlementId&gt;</td>
</tr>
<tr>
<td>direction</td>
<td>Required: Yes&lt;br&gt;String&lt;br&gt;Allowed values: [ingress</td>
</tr>
<tr>
<td>proto</td>
<td>Required: Yes&lt;br&gt;String&lt;br&gt;Allowed values: [tcp</td>
</tr>
<tr>
<td>startPort</td>
<td>Required: Yes&lt;br&gt;Integer&lt;br&gt;startPort defines the beginning of a range of ports to open/white-list [0 - 65535].</td>
</tr>
<tr>
<td>endPort</td>
<td>Required: Yes&lt;br&gt;Integer&lt;br&gt;endPort defines the ending of a range of ports to open/white-list [0 - 65535].</td>
</tr>
<tr>
<td>ipSubnet</td>
<td>Required: Yes&lt;br&gt;String&lt;br&gt;Single IP address or range specified in CIDR notation.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ruleInterface | Required: Yes  
String  
Allowed values: [admin | client | backup] where:  
• admin — specifies that the rule applies to network communications over the administration network interface. The administration network is typically used to support administration tasks by using terminal sessions, monitoring agents, and so on.  
• client — specifies that the rule applies to network communications over the client access network interface, which is typically used by Oracle Net Services connections.  
• backup — specifies that the rule applies to network communications over the backup network interface, which is typically used to transport backup information to and from network-based storage that is separate from Exadata Cloud Service. |

If successful, the POST request will return the unique ID of the newly created security group. For the next step, we'll assume that the newly created security group ID is 3.

**Note:**
A security group can also be modified or deleted. See Oracle Cloud My Services API.

6. Assign the security group to a service instance.

Operation: POST SIExadataSecurityGroupAssignments

Example

Example request, using the service instance csi-585928949 and the security group ID 3:

```json
POST /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments

{
   "securityGroup": {
      "id": "3",
      "customerId": "585927251",
      "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements/585927251/serviceConfigurations/Exadata/securityGroups/3"
   }
}
```
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| customerId | Required: Yes  
|          | String  
|          | This must be the same as the serviceEntitlementId. |

If successful, the POST request will return the unique Id of the newly created security group assignment.

**Note:**
A security group assignment can also be deleted. See [Oracle Cloud My Services API](#).

You can now verify all your security groups and assignments. See:

- Get the current security groups for the service entitlement.
- Get the current security group assignments for the service instance.

**To obtain the IDCS GUID**

Go to the Users page in My Services dashboard and click **Identity Console**. The URL in the browser address field displays the IDCS GUID for your identity domain. For example:

https://idcs-105bbbdfe5644611bf7ce04496073adf.identity.oraclecloud.com/ui/v1/adminconsole/?root=users

In the above URL, `idcs-105bbbdfe5644611bf7ce04496073adf` is the IDCS GUID for your identity domain.

**Exadata Scaling with Bursting**

You can temporarily modify the capacity of your Exadata environment by configuring bursting. Bursting is a method you can use to scale Exadata Cloud Service non-metered instances within an Exadata system.

To scale up your non-metered instances, increase the number of compute nodes by modifying the `burstOcpu` attribute of the host. When you no longer need the additional nodes, update the `burstOcpu` attribute back to its original setting.

**Note:**

In the following examples, `<domain>` is the identity domain ID. An identity domain ID can be either the IDCS GUID that identifies the identity domain for the users within Identity Cloud Service (IDCS) or the Identity Domain name for a traditional Cloud Account.
1. Get the service instance IDs.
   Operation: GET ServiceInstances
   Example
   Example request:
   ```
   GET /itas/<domain>/myservices/api/v1/serviceInstances?
   serviceDefinitionNames=Exadata&statuses=ACTIVE
   ```
   Example payload returned for this request:
   ```
   {
   "items": [
   {
   "id": "csi-585928949",              // Unique ServiceInstanceId
   "serviceEntitlement": {
   "id": "cesi-585927251",
   "canonicalLink": "/itas/<domain>/myservices/api/v1/
   serviceEntitlements/cesi-585927251"
   },
   "serviceDefinition": {
   "canonicalLink": "/itas/<domain>/myservices/api/v1/
   serviceDefinitions/502579309",
   "id": "502579309",
   "name": "Exadata"                // The customer is entitled to use
   the Exadata Service
   },
   "cloudAccount": {
   "canonicalLink": "/itas/<domain>/myservices/api/v1/cloudAccounts/
   cacct-fd7a122448aaaa",
   "id": "cacct-fd7a122448aaaa",
   "name": "myAccountName"
   },
   ...
   "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances/
   csi-585928949"
   }
   ...
   // More Service Instances
could be displayed
   },
   "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceInstances",
   "hasMore": false,
   "limit": 25,
   "offset": 0
   }
   ```
   This example payload returns the service instance ID csi-585928949.

2. Get the service configuration IDs.
   Operation: GET SIServiceConfigurations
   Example
   Example request, using the service instance ID csi-585928949:
   ```
   GET /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/
serviceConfigurations
   ```
   Example payload returned for this request:
   ```
   {
   ```
This example payload shows that `/itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/securityGroupAssignments` is used for Bursting.

3. Get the current compute node configuration.

   **Operation:** GET SIExadataBursting

   **Example**

   Example request, using the service instance ID `csi-585928949`:

   ```
   GET /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/serviceConfigurations/Exadata/bursting
   ```

   Example payload returned for this request:

   ```
   {  
     "ocpuOpInProgress": false,  
     "exaunitId": 50,  
     "ocpuAllocations": [  
       {  
         "nodeName": "host1.oraclecloud.com",  
         "subscriptionOcpu": 11,  
         "meteredOcpu": 0,  
         "burstOcpu": 0,  
         "minOcpu": 11,  
         "maxOcpu": 42,  
         "maxBurstOcpu": 11,  
         "maxSubOcpu": 38,  
         "maxMetOcpu": 0
         },  
       {  
         "nodeName": "host2.oraclecloud.com",  
         "subscriptionOcpu": 11,  
         "meteredOcpu": 0,  
         "burstOcpu": 0,  
         "minOcpu": 11,  
         "maxOcpu": 42,  
         "maxBurstOcpu": 11,  
         "maxSubOcpu": 38,  
         "maxMetOcpu": 0
         }  
     ]
   }  
   ```
4. **Modify the values for burstOcpu.**

Operation: PUT SIE\text{ExadataBursting}

You can modify \text{burstOcpu} to a value that is up to the value of \text{maxBurstOcpu}. This example adds two compute nodes to each host.

Example

Example request, using the service instance csi-585928949:

```json
PUT /itas/\text{<domain>}/myservices/api/v1/serviceInstances/csi-585928949/
    serviceConfigurations/Exadata/bursting/
{
    "ocpuOpInProgress": false,
    "exaunitId": 50,
    "ocpuAllocations": [
        {
            "hostName": "host1.oraclecloud.com",
            "subscriptionOcpu": 11,
            "meteredOcpu": 0,
            "burstOcpu": 2,
            "minOcpu": 11,
            "maxOcpu": 42,
            "maxBurstOcpu": 11,
            "maxSubOcpu": 38,
            "maxMetOcpu": 0
        },
        {
            "hostName": "host2.oraclecloud.com",
            "subscriptionOcpu": 11,
            "meteredOcpu": 0,
            "burstOcpu": 2,
            "minOcpu": 11,
            "maxOcpu": 42,
            "maxBurstOcpu": 11,
            "maxSubOcpu": 38,
            "maxMetOcpu": 0
        }
    ]
}
```
Attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| burstOcpu | Required: Yes  
|          | Type: Integer, Minimum Value: 0, Maximum Value:       |
|          | maxBurstOcpu                                         |
|          | Number of additional cores                           |

Note:  
This action may take a few minutes to complete.

5. Verify the new compute node configuration.

Operation: GET SIExadataBursting

Example

Example request, using the service instance ID csi-585928949:

```
GET /itas/<domain>/myservices/api/v1/serviceInstances/csi-585928949/
    serviceConfigurations/Exadata/bursting
```

Example payload returned for this request:

```
{
    "ocpuOpInProgress": false,
    "exaunitId": 50,
    "ocpuAllocations": [
        {
            "hostName": "host1.oraclecloud.com",
            "subscriptionOcpu": 11,
            "meteredOcpu": 0,
            "burstOcpu": 2, // New Burst value
            "minOcpu": 11,
            "maxOcpu": 42,
            "maxBurstOcpu": 11,
            "maxSubOcpu": 38,
            "maxMetOcpu": 0
        },
        {
            "hostName": "host2.oraclecloud.com",
            "subscriptionOcpu": 11,
            "meteredOcpu": 0,
            "burstOcpu": 2, // New Burst value
            "minOcpu": 11,
            "maxOcpu": 42,
            "maxBurstOcpu": 11,
            "maxSubOcpu": 38,
            "maxMetOcpu": 0
        }
    ],
    "status": 200,
    "op": "exaunit_coreinfo",
    "additionalNumOfCores": "0",
    "additionalNumOfCoresHourly": "0",
    "coreBursting": "Y"
}
```
To obtain the IDCS GUID

Go to the Users page in My Services dashboard and click Identity Console. The URL in the browser address field displays the IDCS GUID for your identity domain. For example:

https://idcs-105bbbdfe5644611bf7ce04496073adf.identity.oraclecloud.com/ui/v1/adminconsole/?root=users

In the above URL, idcs-105bbbdfe5644611bf7ce04496073adf is the IDCS GUID for your identity domain.

Managing Exadata Instances

Important:
The My Services dashboard and APIs are deprecated.

The following procedures walk you through creating, modifying, and deleting Exadata instances used with the Oracle Cloud My Services API.

Important:
These procedures are for use with Oracle Database Exadata Cloud@Customer ONLY. For more information, see Administering Oracle Database Exadata Cloud at Customer. These procedures DO NOT apply to the Exadata Cloud Service available in Oracle Cloud Infrastructure.

Prerequisites

Before you can manage Exadata instances, you need to:

- Subscribe to an Oracle Cloud service
- Obtain account credentials with required roles assigned
- Determine your API endpoint

To subscribe to an Oracle Cloud service

To access Oracle Cloud My Services API, you must request a trial or paid subscription to an Oracle Cloud service.

To obtain account credentials and role assignments

Ask your account administrator for the following items to access Oracle Cloud My Services API:

- Account credentials:
  - User name and password
  - Identity domain ID

  An identity domain ID can be either the IDCS GUID that identifies the identity domain for the users within Identity Cloud Service (IDCS) or the Identity Domain name for a traditional Cloud Account.

- Required roles assigned to above user name

To determine your API endpoint

Insert the identity domain ID provided by the account administrator (<domain>) between /itas/ and /myservices/.

Example:

https://itra.oraclecloud.com/itas/<domain>/myservices/api/v1/serviceEntitlements
Creating Exadata Instances

This section covers how to create a basic Exadata instance, an instance with custom IP network configuration, and an instance with multi-VM support.

To create a basic Exadata instance

Post a request with the required payload to create a new instance for a given service entitlement (Exadata in our case). In the following example, `<domain>` is the identity domain ID.

```json
POST /itas/<domain>/myservices/api/v1/operations
{
    "operationItems": [
    {
        "attributes": [
        {
            "name": "requestPayload.name",
            "value": "newinstanceName"
        },
        {
            "name": "requestPayload.serviceEntitlementId",
            "value": "500073421"
        },
        {
            "name": "requestPayload.size",
            "value": "CUSTOM"
        },
        {
            "name": "requestPayload.serviceType",
            "value": "Exadata"
        },
        {
            "name": "requestPayload.adminUserName",
            "value": "john.smith@example.com"
        },
        {
            "name": "requestPayload.adminEmail",
            "value": "john.smith@example.com"
        },
        {
            "name": "requestPayload.adminFirstName",
            "value": "John"
        },
        {
            "name": "requestPayload.adminLastName",
            "value": "Smith"
        },
        {
            "name": "requestPayload.invokerAdminUserName",
            "value": "john.smith@example.com"
        },
        {
            "name": "requestPayload.invokerAdminEmail",
            "value": "john.smith@example.com"
        },
        {
            "name": "requestPayload.invokerAdminFirstName",
            "value": "John"
        },
        {
            "name": "requestPayload.invokerAdminLastName",
            "value": "Smith"
        }
    ],
}
```
Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requestPayload.name</td>
<td>Required: Yes&lt;br&gt;Type: String&lt;br&gt;Name of the Exadata instance. This name:&lt;br&gt;• Must not exceed 25 characters.&lt;br&gt;• Must start with a letter.&lt;br&gt;• Must contain only lower case letters and numbers.&lt;br&gt;• Must not contain spaces or any other special characters.&lt;br&gt;• Must be unique within the identity domain.</td>
</tr>
<tr>
<td>requestPayload.serviceEntitlementId</td>
<td>Required: Yes&lt;br&gt;Type: String&lt;br&gt;Service Entitlement for the Exadata instance. See “Exadata Service Entitlement discovery”. Note that any “cesi-“ or “sub-“ prefix should not be included.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>requestPayload.</td>
<td></td>
</tr>
<tr>
<td>customAttributes.</td>
<td></td>
</tr>
<tr>
<td>ExaUnitName</td>
<td>Required: Yes Type: String A name for your Exadata Database Machine environment. This name is also used as the cluster name for the Oracle Grid Infrastructure installation.</td>
</tr>
<tr>
<td>requestPayload.</td>
<td></td>
</tr>
<tr>
<td>customAttributes.</td>
<td></td>
</tr>
<tr>
<td>CreateSparse</td>
<td>Required: Yes Type: String &quot;Y&quot; to create a disk group that is based on sparse grid disks, else &quot;N&quot;. You must select this option to enable Exadata Cloud Service snapshots. Exadata snapshots enable space-efficient clones of Oracle databases that can be created and destroyed very quickly and easily.</td>
</tr>
<tr>
<td>requestPayload.</td>
<td></td>
</tr>
<tr>
<td>customAttributes.</td>
<td></td>
</tr>
<tr>
<td>BackupToDisk</td>
<td>Required: Yes Type: String &quot;Y&quot; to use &quot;Database backups on Exadata Storage&quot;, else &quot;N&quot;. This option configures the Exadata storage to enable local database backups on Exadata storage.</td>
</tr>
<tr>
<td>requestPayload.</td>
<td></td>
</tr>
<tr>
<td>customAttributes.</td>
<td></td>
</tr>
<tr>
<td>isBYOL</td>
<td>Required: Yes Type: String &quot;Y&quot; to indicate that the Exadata Cloud Service instance uses Oracle Database licenses that are provided by you rather than licenses that are provided are part of the service subscription, else &quot;N&quot;. This option only affects the billing that is associated with the service instance. It has no effect on the technical configuration of the Exadata Cloud Service instance.</td>
</tr>
<tr>
<td>requestPayload.</td>
<td></td>
</tr>
<tr>
<td>customAttributes.</td>
<td></td>
</tr>
<tr>
<td>PickRackSize</td>
<td>Required: Yes Type: String Specify the rack configuration for your service instance. Exact allowed values depend on your purchase. Typical values are like &quot;Full Rack&quot;, &quot;Half Rack&quot;, &quot;Quarter Rack&quot; or &quot;Eighth Rack&quot;.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
requestPayload. | Required: Yes  
Type: String  
Data center that will host your Exadata Cloud Service instance. See “Exadata Service Entitlement discovery” to obtain the Eligible Data Center IDs.
customAttributes. |  
SELECTED_DC_ID |  

**To create an Exadata instance with custom IP network configuration**

Post a request with the attributes ClientNetwork and BackupNetwork as part of the payload. The following example includes these optional attributes as well as required attributes.

In the following example, `<domain>` is the identity domain ID.

```json
POST /itas/<domain>/myservices/api/v1/operations
{
   "operationItems": [
   {
      "attributes": [
      {
         "name": "requestPayload.name",
         "value": "newinstanceName"
      },
      {
         "name": "requestPayload.serviceEntitlementId",
         "value": "500073421"
      },
      {
         "name": "requestPayload.size",
         "value": "CUSTOM"
      },
      {
         "name": "requestPayload.serviceType",
         "value": "Exadata"
      },
      {
         "name": "requestPayload.adminUserName",
         "value": "john.smith@example.com"
      },
      {
         "name": "requestPayload.adminEmail",
         "value": "john.smith@example.com"
      },
      {
         "name": "requestPayload.adminFirstName",
         "value": "John"
      },
      {
         "name": "requestPayload.adminLastName",
         "value": "Smith"
      },
      {
         "name": "requestPayload.invokerAdminUserName",
         "value": "john.smith@example.com"
      },
      {
         "name": "requestPayload.invokerAdminEmail",
         "value": "john.smith@example.com"
      }
   ]
}
Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| requestPayload.customAttributes.ClientNetwork     | Required: Yes  
Type: Url  
IP network definitions for the network that is primarily used for client access to the database servers. Applications typically access databases on Exadata Cloud Service through this network using Oracle Net Services in conjunction with Single Client Access Name (SCAN) and Oracle RAC Virtual IP (VIP) interfaces. |
| requestPayload.customAttributes.SELECTED_DC_ID    | US001                                                                 |
| requestPayload.customAttributes.BackupNetwork     | /root/root/1/ipnetwork2                                                   |
| requestPayload.customAttributes.CreateSparse       | N                                                                     |
| requestPayload.customAttributes.BackupToDisk       | N                                                                     |
| requestPayload.customAttributes.isBYOL             | N                                                                     |
| requestPayload.customAttributes.PickRackSize       | Quarter Rack                                                            |
| requestPayload.invokerAdminFirstName               | John                                                                    |
| requestPayload.invokerAdminLastName                | Smith                                                                   |
| requestPayload.customAttributes.ExaUnitName        | systemname                                                              |
### Service Essentials

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requestPayload.</td>
<td>Required: Yes Type: Url</td>
</tr>
<tr>
<td>customAttributes.</td>
<td>IP network definitions for the network that is typically used to access the database servers for various purposes, including backups and bulk data transfers.</td>
</tr>
<tr>
<td>BackupNetwork</td>
<td></td>
</tr>
</tbody>
</table>

#### To create an Exadata instance with multi-VM support

If your Exadata system environment is enabled to support multiple virtual machine (VM) clusters, then you can define up to eight clusters and specify how the overall Exadata system resources are allocated to them.

In a configuration with multiple VM clusters, each VM cluster is allocated a dedicated portion of the overall Exadata system resources, with no over-provisioning or resource sharing. On the compute nodes, a separate VM is defined for each VM cluster, and each VM is allocated a dedicated portion of the available compute node CPU, memory, and local disk resources. Each VM cluster is also allocated a dedicated portion of the overall Exadata storage.

Post a request with the attributes EXAUNIT_ALLOCATIONS and MULTIVM_ENABLED as part of the payload. The following example includes these optional attributes as well as required attributes.

In the following example, <domain> is the identity domain ID and <base64_encoded_string> is a base64 encoding of the payload following the example.

**Example payload for request:**

```json
POST /itas/<domain>/myservices/api/v1/operations
{
  "operationItems": [
    {
      "attributes": [
        {
          "name": "requestPayload.name",
          "value": "newinstanceName"
        },
        {
          "name": "requestPayload.serviceEntitlementId",
          "value": "500073421"
        },
        {
          "name": "requestPayload.size",
          "value": "CUSTOM"
        },
        {
          "name": "requestPayload.serviceType",
          "value": "Exadata"
        },
        {
          "name": "requestPayload.adminUserName",
          "value": "john.smith@example.com"
        },
        {
          "name": "requestPayload.adminEmail",
          "value": "john.smith@example.com"
        },
        {
          "name": "requestPayload.adminFirstName",
          "value": "John"
        },
        {
          "name": "requestPayload.adminLastName",
          "value": "Smith"
        }
      ]
    }
  ]
}
Payload for <base64_encoded_string>:

```
{
  ExaunitProperties: [
    {name:requestId, value:27ac0ee3-0c72-4493-b02b-40038f07d2a0},
    ...
  ]
}
```
Service Essentials

```javascript
{name:Operation, value:AddCluster},
{name:TotalNumOfCoresForCluster, value:4},
{name:TotalMemoryInGb, value:30},
{name:StorageInTb, value:3},
{name:OracleHomeDiskSizeInGb, value:60},
{name:ClientNetwork, value:/root/root/1/ipnetwork1},  // Only if Higgs is also required
{name:BackupNetwork, value:/root/root/1/ipnetwork2},  // Only if Higgs is also required
{name:ExaUnitName, value:systemname},
{name:CreateSparse, value:N},
{name:BackupToDisk, value:N}
```

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| requestId             | Required: Optional  
|                       | Type: String  
|                       | Unique UUID  |
| TotalNumOfCoresForCluster | Required: Yes  
|                       | Type: String  
|                       | The number of CPU cores that are allocated to the VM cluster. This is the total number of CPU cores that are allocated evenly across all of the compute nodes in the VM cluster. Must be a multiple of numComputes as returned by a call to ecra/endpoint/clustershapes.  |
| TotalMemoryInGb       | Required: Yes  
|                       | Type: String  
|                       | The amount of memory (in GB) that is allocated to the VM cluster. This is the total amount of memory that is allocated evenly across all of the compute nodes in the VM cluster. Must be a multiple of numComputes as returned by a call to ecra/endpoint/clustershapes.  |
| StorageInTb           | Required: Yes  
|                       | Type: String  
|                       | The total amount of Exadata storage (in TB) that is allocated to the VM cluster. This storage is allocated evenly from all of the Exadata Storage Servers.  |
| OracleHomeDiskSizeInGb | Required: Yes  
|                       | Type: String  
|                       | The amount of local disk storage (in GB) that is allocated to each database server in the first VM cluster.  |
Modifying Exadata Instances

This section covers how to add a cluster to an existing instance, reshape a cluster, and delete a cluster.

To add a cluster to an existing instance

Post a request with the operationItemDefinition of CIM-Exadata-CUSTOM-PRODUCTION-UPDATE and a base64 encoding of a payload that includes the Operation value of AddCluster.

In the following example, <domain> is the identity domain ID, <instanceId> and <serviceEntitlementId> are returned from iTAS serviceInstances, and <base64_encoded_string> is a base64 encoding of the payload following the example.

Example payload for request:

```json
POST /itas/<domain>/myservices/api/v1/operations HTTP/1.1
{
    "operationItems": [
        {
            "attributes": [
                {
                    "name": "instanceId",
                    "value": "<instanceId>"
                },
                {
                    "name": "requestPayload.serviceEntitlementId",
                    "value": "<serviceEntitlementId>"
                },
                {
                    "name": "requestPayload.size",
                    "value": "CUSTOM"
                },
                {
                    "name": "requestPayload.serviceType",
                    "value": "Exadata"
                },
                {
                    "name": "requestPayload.customAttributes.EXAUNIT_ALLOCATIONS",
                    "value": "<base64_encoded_string>"
                },
                {
                    "name": "requestPayload.customAttributes.MULTIVM_ENABLED",
                    "value": "true"
                }
            ],
            "operationItemDefinition": {
                "id": "CIM-Exadata-CUSTOM-PRODUCTION-UPDATE"
            }
        }
    ]
}
```

Payload for <base64_encoded_string>:

```json
{
    "ExaunitProperties": {
        {name:requestId, value:27ac0ee3-0c72-4493-b02b-40038f07d2a0},
        {name:Operation, value:AddCluster},
        {name:TotalNumOfCoresPerCluster, value:4},
        {name:TotalMemoryInGb, value:30},
        {name:StorageInTb, value:3},
        {name:OracleHomeDiskSizeInGb, value:60},
        {name:ClientNetwork, value:/root/root/1/ipnetwork1}, // Only if Higgs is also required
```
To reshape a cluster

Post a request with the operationItemDefinition of CIM-Exadata-CUSTOM-PRODUCTION-UPDATE and a base64 encoding of a payload that includes the Operation value of ReshapeCluster.

In the following example, <domain> is the identity domain ID and <base64_encoded_string> is a base64 encoding of the payload following the example.

Example payload for request:

```json
POST /itas/<domain>/myservices/api/v1/operations HTTP/1.1
{
  "operationItems": [
    {
      "attributes": [
        {
          "name": "instanceId",
          "value": "500076173"
        },
        {
          "name": "requestPayload.serviceEntitlementId",
          "value": "500073421"
        },
        {
          "name": "requestPayload.size",
          "value": "CUSTOM"
        },
        {
          "name": "requestPayload.serviceType",
          "value": "Exadata"
        },
        {
          "name": "requestPayload.customAttributes.EXAUNIT_ALLOCATIONS",
          "value": "<base64_encoded_string>"
        },
        {
          "name": "requestPayload.customAttributes.MULTIVM_ENABLED",
          "value": "true"
        }]
    },
    "operationItemDefinition": {
      "id": "CIM-Exadata-CUSTOM-PRODUCTION-UPDATE"
    }
  ]
}
```

Payload for <base64_encoded_string>:

```json
{
  "ExaunitProperties": [
    {
      "name": "requestId",
      "value": "27ac0ee3-0c72-4493-b02b-40038f07d2a0"
    },
    {
      "name": "ExaunitID",
      "value": "1" // From ecra/endpoint/exaservice/serviceInstance/resourceinfo
    },
    {
      "name": "Operation",
      "value": "ReshapeCluster"
    }
  ]
}
```
Important:

- Only one attribute can be modified per Reshape request. The payload should contain only the modified attribute. Example:

```json
{ExaunitProperties :
 [{name:Operation,value :
 ReshapeCluster),
 { name:ExaunitID,value:5
 },
 name:TotalNumOfCoresForCluster
 ,
 value:6}]
}
```

- When doing a Reshape with the OracleHomeDiskSizeInGb attribute, use the name OhomePartitionInGB.
- The value for TotalNumOfCoresForCluster must be a multiple of numComputes as returned by a call to ecra/endpoint/clustershapes.
- The value for TotalMemoryInGb must be a multiple of numComputes as returned by a call to ecra/endpoint/clustershapes.

To delete a cluster

Post a request with the operationItemDefinition of CIM-Exadata-CUSTOM-PRODUCTION-UPDATE and a base64 encoding of a payload that includes the Operation value of DeleteCluster.

In the following example, `<domain>` is the identity domain ID and `<base64_encoded_string>` is a base64 encoding of the payload following the example.

Example payload for request:

```
POST /itas/<domain>/myservices/api/v1/operations HTTP/1.1
{
```
"operationItems": [
  {
    "attributes": [
      {
        "name": "instanceId",
        "value": "500076173"
      },
      {
        "name": "requestPayload.serviceEntitlementId",
        "value": "500073421"
      },
      {
        "name": "requestPayload.size",
        "value": "CUSTOM"
      },
      {
        "name": "requestPayload.serviceType",
        "value": "Exadata"
      },
      {
        "name": "requestPayload.customAttributes.EXAUNIT_ALLOCATIONS",
        "value": "<base64_encoded_string>"
      },
      {
        "name": "requestPayload.customAttributes.MULTIVM_ENABLED",
        "value": "true"
      }
    ],
    "operationItemDefinition": {
      "id": "CIM-Exadata-CUSTOM-PRODUCTION-UPDATE"
    }
  }
],
"Payload for <base64_encoded_string>:"
{
  "ExaunitProperties": [
    {name:requestId, value:27ac0ee3-0c72-4493-b02b-40038f07d202},  // Optional
    {name:ExaunitID, value:2},
    {name:Operation, value:DeleteCluster}
  ]
}

**Deleting Exadata Instances**

This section covers how to delete Exadata instances.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete all existing multi-VM clusters before deleting the Exadata instance. Following this guidance prevents the instance ending up in an invalid state.</td>
</tr>
</tbody>
</table>

**To delete an instance**

Post a request with the operationItemDefinition of CIM-Exadata-CUSTOM-PRODUCTION-DELETE.

In the following example, `<domain>` is the identity domain ID.

Example payload for request:

```
POST /itas/<domain>/myservices/api/v1/operations HTTP/1.1
```
Discovering Entitlements and Instances

This section describes how to discover service entitlements and service instances.

To discover service entitlements

Send the following request:

```
GET /itas/<domain>/myservices/api/v1/serviceEntitlements?
serviceDefinitionNames=Exadata
```

Example payload returned for this request:

```
{
   "items": [
      {
         "id": "cesi-585927251", // Unique ServiceEntitlementId
         "serviceDefinition": {
            "canonicalLink": "/itas/a517289/myservices/api/v1/
            serviceDefinitions/502579309",
            "id": "502579309",
            "name": "Exadata" // The customer is entitled to
            use the Exadata Service
         },
         "status": "ACTIVE",
         "canonicalLink": "/itas/a517289/myservices/api/v1/serviceInstances/
            csi-585928949"
      } // More Service
   Entitlements could be displayed
   ]
```

Eligible Data Centers:
Use:

/itas/<domain>/myservices/api/v1/serviceEntitlements/{ServiceEntitlementId}?expands=serviceInstancesEligibleDataCenters

where `{ServiceEntitlementId}` is a service entitlement ID such as cesi-500074601. This will provide additional information such as:

```
"serviceInstancesEligibleDataCenters": [  
  {  
    "id": "US001"
  }  
],
```

To discover service instances

Send the following request:

GET /<domain>/myservices/api/v1/serviceInstances?

serviceDefinitionNames=Exadata

Example payload returned for this request:

```json
{
  "items": [  
    {  
      "id": "csi-585928949",             // Unique ServiceInstanceId
      "serviceEntitlement": {  
        "id": "cesi-585927251",         // Related ServiceEntitlementId
        "canonicalLink": "/itas/a517289/myservices/api/v1/serviceEntitlements/cesi-585927251"
      },  
      "serviceDefinition": {  
        "canonicalLink": "/itas/a517289/myservices/api/v1/serviceDefinitions/502579309",
        "id": "502579309",
        "name": "Exadata"                 // The customer is entitled to use the Exadata Service
      },
      "canonicalLink": "/itas/a517289/myservices/api/v1/serviceInstances/csi-585928949"
    }
  ],
  "canonicalLink": "/itas/<domain>/myservices/api/v1/serviceEntitlements",
  "hasMore": false,
  "limit": 25,
  "offset": 0
}
```

Using Access Token Authorization with My Services API

**Important:**

The My Services dashboard and APIs are deprecated.
This topic explains how to set up and use access token authorization with the Oracle Cloud My Services API. Access token authorization allows a developer to access programmatic endpoints (APIs) to obtain some information (for example, entitlements, instances, or metering data) for your cloud account.

**About Access Tokens**

An access token contains the information required to allow a developer to access information on your cloud account. A developer presents the token when making API calls. The allowed actions and endpoints depend on the scopes (permissions) that you select when you generate the token. An access token is valid for about an hour.

A refresh token allows the developer to generate a new access token without having to contact an administrator. A refresh token is valid for about one year.

**Process Overview**

**Setup steps for the Administrator:**

1. Create an Identity Cloud Service client application with the specific privileges you want to grant to developers.
2. Generate an access token that contains the required privileges for the intended developer.
3. Provide the access token and required information to the developer.
4. Configure Identity Cloud Service for access token validation.

**Steps for developer to use the token:**

1. Issue requests against My Services API endpoints. Include the access token for the authorization parameter.
2. When the access token expires, refresh the access token without administrator intervention until the privilege is terminated.

**Administrator Tasks to Set Up Token Validation**

Perform the following tasks to enable developer access with an access token:

**Create the IDCS client application**

1. Sign in to Identity Cloud Services as an Administrator and go to the administration console. See How to Access Oracle Identity Cloud Service if you need help signing in.
2. Click the Applications tile. A list of the applications is displayed.
3. Click + Add to create a new application.
4. Click Confidential Application as the type of application.
5. In the App Details section, enter a Name and Description. Avoid entering confidential information.
6. Click Next.
7. In the Client section:
   a. Select Configure this application as a client now.
   b. Under Authorization, for Allowed Grant Types, select the following options:
      - JWT Assertion
      - Refresh Token
9. In the Select Scope dialog, select CloudPortalResourceApp and click the arrow to select scopes for the resource.
10. Select the box next to each authorization that you might want to give the developers to whom you will provide an Access Token. (The permissions are assigned in another step.)
11. Click Add to close the dialog. Your selections are displayed.
12. Click Next.
13. In the Resources section, accept the default and click Next.
14. In the Web Tier Policy section, accept the default and click Next.
15. In the **Authorization** section, click **Finish**.

The **Application Added** notification displays the new Client ID and Client Secret for the application.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy and store the Client ID and Client Secret in a safe place and then click <strong>Close</strong>. The Client ID and Client Secret are credentials that are specific to the application that you just created. You will need these credentials later.</td>
</tr>
</tbody>
</table>

16. To complete the creation process, click **Activate** at the top of the page.

**Generate an access token**

1. Navigate to the IDCS application that you created in the preceding task and select the **Details** tab.
2. Click **Generate Access Token**.
3. On the **Generate Token** dialog, select **Customized Scopes**, then select **Invokes Other APIs**.
4. Select the scopes that you want to give to the developer who will receive this access token.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle recommends that you provide only the minimum required privileges.</td>
</tr>
</tbody>
</table>

5. Select **Include Refresh Token**.
6. Click **Download Token**. Your browser will prompt you to download a token file (.tok). The token file contains an access token and a refresh token.
7. Provide this file to the developer.

**Send the access information to a developer**

To call API endpoints, the developer needs:

- A token file that you generated.
- The Client ID and Client Secret for the IDCS application used to generate the token file. The Client ID and Secret are required for the developer to generate a new access token from the refresh token.
- The endpoints for the APIs.
  - End points related to the itas:myservices scopes are: https://itra.oraclecloud.com/itas/<tenant-IDCS-ID>/myservices/api/v1
  - End points related to the itas:metering scopes are: https://itra.oraclecloud.com/metering/api/v1

Make sure that you send the above information in a secure way. If you think that this information has been compromised, see Revoking a Developer's Ability to Refresh Access Tokens on page 331.

**Configure Identity Cloud Service for access token validation**

To allow clients to access the tenant signing certificate without logging in to Oracle Identity Cloud Service:

1. Sign in to the Oracle Identity Cloud Services admin console. See How to Access Oracle Identity Cloud Service if you need help signing in.
2. Open the navigation menu. Under **Settings** select **Default Settings**.
3. Set the **Access Signing Certificate** toggle button to on.

**Using the Access Token**

The token file has a .tok extension. The file contains the access token and the refresh token. The content looks like:

```json
{"app_access_token":"eyJ4N...aabb...CpNwA","refresh_token":"AQID...9NCA"}
```

To use the token with the My Services API:
1. Open the token file.
2. Issue a request to a valid endpoint, inserting the access token for the Authorization parameter.

For example:

```sh
```

### Requesting a New Access Token from a Refresh Token

An access token is valid for about one hour. When the token is no longer valid you will get a 401 response code and an Error Message (“errorMessage”) value containing “Expired”.

You can generate a new short-lived access token from the refresh token. You'll need the Client ID and Client Secret to generate the new token. You can only generate tokens with the same or lower access (scopes) as your original token.

Example using the curl command:

```sh
```

Using the sample token file from the previous section, the value for `<refresh-token>` would be AQID...9NCA=.

Sample response:

```
{ "access_token": "eyJraWQiO....2nqA", "token_type": "Bearer", "expires_in": 3600, "refresh_token": "AQIDBAUn...VkxNCB7djF9NCA=" }`
```

**Note:**

When a developer generates a new access token and refresh token, the previous refresh token becomes invalid.

### Revoking a Developer's Ability to Refresh Access Tokens

If you need to revoke a developer's ability to refresh access tokens, you can either invalidate the existing refresh token by generating a new Client Secret for the token; or, you can temporarily revoke access by deactivating the application.

**Important:**

Taking either of these actions will terminate or suspend the ability of all developers using the current Client Secret or application. When generating tokens for multiple developers, consider creating more than one IDCS application to isolate developers from each other.

**To terminate a developer's ability to refresh their access token**

1. Sign in to Identity Cloud Services as an Administrator and go to the administration console. See [How to Access Oracle Identity Cloud Service](#) if you need help signing in.
2. Click the Applications tile. A list of the applications is displayed.
3. Click the application used to generate the token to view its details.
4. Click Configuration.
5. Under General Information, next to Client Secret, click Regenerate to generate a new Client Secret.

To restore the ability for the developer to generate an access token from a refresh token, generate a new access token. Then provide the token along with the new Client Secret to the developer.
To temporarily suspend a developer's ability to refresh their access token

1. Sign in to Identity Cloud Services as an Administrator and go to the administration console. See How to Access Oracle Identity Cloud Service if you need help signing in.
2. Click the Applications tile. A list of the applications is displayed.
3. Click the application used to generate the token to view its details.
4. In the upper right corner of the page, click Deactivate.
5. At the prompt, click Deactivate Application.

To re-enable developers to use the same tokens, click Activate.
Chapter 6

API Gateway

This chapter explains how to use the API Gateway service to create protected RESTful API endpoints for Oracle Functions, Container Engine for Kubernetes, and other services running on Oracle Cloud Infrastructure and beyond.

Overview of API Gateway

The API Gateway service enables you to publish APIs with private endpoints that are accessible from within your network, and which you can expose with public IP addresses if you want them to accept internet traffic. The endpoints support API validation, request and response transformation, CORS, authentication and authorization, and request limiting.

Using the API Gateway service, you create one or more API gateways in a regional subnet to process traffic from API clients and route it to back-end services. You can use a single API gateway to link multiple back-end services (such as load balancers, compute instances, and Oracle Functions) into a single consolidated API endpoint.

You can access the API Gateway service to define API gateways and API deployments using the Console and the REST API.

The API Gateway service is integrated with Oracle Cloud Infrastructure Identity and Access Management (IAM), which provides easy authentication with native Oracle Cloud Infrastructure identity functionality.

To get set up and running quickly with the API Gateway service, see the Quick Start Guide. A number of related Developer Tutorials are also available.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

• Google Chrome 69 or later
• Safari 12.1 or later
• Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.
API Gateway

Authentication and Authorization
Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

API Gateway Capabilities and Limits
The number of API gateways, API resources, and certificate resources you can define in a region is controlled by API Gateway service limits (see API Gateway Limits on page 218). The default service limits vary according to your payment method. If you need more capacity, you can submit a request to increase the default service limits (see Requesting a Service Limit Increase on page 217).

Some other API Gateway capabilities and limits are also fixed. However, there are also a number that you can change. See API Gateway capabilities and limits on page 476.

Required IAM Service Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re new to policies, see Getting Started with Policies and Common Policies.

For more details about policies for the API Gateway service, see:

- Create Policies to Control Access to Network and API Gateway-Related Resources on page 342
- Details for API Gateway on page 2173

API Gateway Concepts
This topic describes key concepts you need to understand when using the API Gateway service.

API Gateways
In the API Gateway service, an API gateway is a virtual network appliance in a regional subnet. Private API gateways can only be accessed by resources in the same subnet. Public API gateways are publicly accessible, including from the internet.

An API gateway routes inbound traffic to back-end services including public, private, and partner HTTP APIs, as well as Oracle Functions. Each API gateway is a private endpoint that you can optionally expose over a public IP address as a public API gateway.

To ensure high availability, you can only create API gateways in regional subnets (not AD-specific subnets). You can create private API gateways in private or public subnets, but you can only create public API gateways in public subnets.

An API gateway is bound to a specific VNIC.

You create an API gateway within a compartment in your tenancy. Each API gateway has a single front end, zero or more back ends, and has zero or more APIs deployed on it as API deployments.
APIs

In the API Gateway service, an API is a set of back-end resources, and the methods (for example, GET, PUT) that can be performed on each back-end resource in response to requests sent by an API client.

To enable an API gateway to process API requests, you must deploy the API on the API gateway by creating an API deployment.

To deploy an API on an API gateway, you have the option to create an API resource in the API Gateway service. An API resource includes an API description that defines the API resource. Note that creating an API resource is optional. You can deploy an API on an API gateway without creating an API resource in the API Gateway service.

API Deployments

In the API Gateway service, an API deployment is the means by which you deploy an API on an API gateway. Before the API gateway can handle requests to the API, you must create an API deployment.

When you create an API deployment, you set properties for the API deployment, including an API deployment specification. Every API deployment has an API deployment specification.

You can deploy multiple APIs on the same API gateway, so a single API gateway can host multiple API deployments.

API Deployment Specifications

In the API Gateway service, an API deployment specification describes some aspects of an API deployment.

When you create the API deployment, you set properties for the API deployment, including an API deployment specification. Every API deployment has an API deployment specification. You can create an API deployment specification:

- by using dialogs in the Console
- by using your preferred JSON editor to create a JSON file
- by using an API description that you've uploaded from an API description file written in a supported language (for example, OpenAPI Specification version 3.0)

Each API deployment specification describes one or more back-end resources, the route to each back-end resource, and the methods (for example, GET, PUT) that can be performed on each resource. The API deployment specification describes how the API gateway integrates with the back end to execute those methods. The API deployment specification can also include request and response policies.

API Resources and API Descriptions

In the API Gateway service, you have the option to create an API resource. An API resource is the design-time representation of an API. You can use an API resource to deploy an API on an API gateway.

An API description defines an API resource, including:

- available endpoints
- available operations on each endpoint
- parameters that can be input and output for each operation
- authentication methods

If you use an API resource to deploy an API on an API gateway, its API description pre-populates some of the properties of the API deployment specification.

You import the API description from a file (sometimes called an 'API specification', or 'API spec') written in a supported language. Currently, OpenAPI Specification version 2.0 (formerly Swagger Specification 2.0) and version 3.0 are supported.

Note that creating an API resource in the API Gateway service is optional. You can deploy an API on an API gateway without creating an API resource in the API Gateway service. Note also that you can create an API resource that doesn't have an API description initially, and then add an API description later.
Front ends
In the API Gateway service, a front end is the means by which requests flow into an API gateway. An API gateway can have either a public front end or a private front end:

- A public front end exposes the APIs deployed on an API gateway via a public IP address.
- A private front end exposes the APIs deployed on an API gateway to a VCN via a private endpoint.

Back ends
In the API Gateway service, a back end is the means by which a gateway routes requests to the back-end services that implement APIs. If you add a private endpoint back end to an API gateway, you give the API gateway access to the VCN associated with that private endpoint.

You can also grant an API gateway access to other Oracle Cloud Infrastructure services as back ends. For example, you could grant an API gateway access to Oracle Functions, so you can create and deploy an API that is backed by a serverless function.

API Providers, API Consumers, API Clients, and End Users
An API provider is a person or team who designs, implements, delivers, and operates APIs. These users interact with interfaces such as the Oracle Cloud Infrastructure Console, SDK, CLI, and Terraform provider. They use API Gateway to deploy, monitor, and operate APIs. Some organizations segment the API provider role further, for example into:

- API developers, with responsibility for building APIs and deploying them on API gateways
- API Gateway managers, with responsibility for monitoring and managing API gateways, typically in production

An API consumer is a person or team who builds apps and services (API clients) and wants to leverage one or more APIs offered by an API provider. The API consumer is typically not sharing an Oracle Cloud Infrastructure tenancy with the API provider. The API consumer is a customer of the API provider.

An API client is an application or device created by an API consumer. The API client invokes the API at runtime by sending requests to the API gateway on which the API is deployed. API clients typically authenticate with the API using OAuth, Basic Auth, mTLS and might use some other token such as an API key for metering and monetization.

An end user is a user of an API client, and is sometimes referred to as the "resource-owner" in terms of authorization. The end user only ever interacts with an API using the API client, and is typically unaware of the API itself. The end user is a customer of the API consumer.

Routes
In the API Gateway service, a route is the mapping between a path, one or more methods, and a back-end service. Routes are defined in API deployment specifications.

Policies
In the API Gateway service, there are different types of policy:

- a request policy describes actions to be performed on an incoming request from an API client before it is sent to a back end
- a response policy describes actions to be performed on a response returned from a back end before it is sent to an API client
- a logging policy describes how to store information about requests and responses going through an API gateway, and information about processing within an API gateway

You can use request policies and/or response policies to:

- limit the number of requests sent to back-end services
- enable CORS (Cross-Origin Resource Sharing) support
- provide authentication and authorization
• modify incoming requests and outgoing responses

You can add policies to an API deployment specification that apply globally to all routes in the API deployment specification, as well as policies that apply only to particular routes.

Note that API Gateway policies are different to IAM policies, which control access to Oracle Cloud Infrastructure resources.

Preparing for API Gateway

Before you can use the API Gateway service to create API gateways and deploy APIs on them as API deployments:

• You must have access to an Oracle Cloud Infrastructure tenancy. The tenancy must be subscribed to one or more of the regions in which API Gateway is available (see Availability by Region on page 338).
• Your tenancy must have sufficient quota on API Gateway-related resources (see Service Limits on page 215).
• Within your tenancy, there must already be a compartment to own the necessary network resources. If such a compartment does not exist already, you will have to create it. See Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don't exist already on page 340.
• The compartment that owns network resources must contain a VCN, a public or private regional subnet, and other resources (such as an internet gateway, a route table, security lists). To ensure high availability, API gateways can only be created in regional subnets (not AD-specific subnets). Note that an API gateway must be able to reach the back ends defined in the API deployment specification. For example, if the back end is on the public internet, the VCN must have an internet gateway to enable the API gateway to route requests to the back end.
• The VCN must have a set of DHCP options that includes an appropriate DNS resolver to map host names defined in an API deployment specification to IP addresses. If such a DHCP options set does not exist in the VCN already, you will have to create it. Select the DHCP options set for the API gateway's subnet as follows:
  • If the host name is publicly published on the internet, or if the host name belongs to an instance in the same VCN, select a DHCP options set that has the Oracle-provided Internet and VCN Resolver as the DNS Type. This is the default if you do not explicitly select a DHCP options set.
  • If the host name is on your own private or internal network (for example, connected to the VCN by FastConnect), select a DHCP options set that has Custom Resolver as the DNS Type, and has the URL of a suitable DNS server that can resolve the host name to an IP address.

Note that you can change the DNS server details in the DHCP options set specified for an API gateway's subnet. The API gateway will be reconfigured to use the updated DNS server details within two hours. For more information about resolving host names to IP addresses, see DNS in Your Virtual Cloud Network on page 2910 and DHCP Options on page 2917.
• Within your tenancy, there must already be a compartment to own API Gateway-related resources (API gateways, API deployments). This compartment can be, but need not be, the same compartment that contains the network resources. See Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don't exist already on page 340. Note that the API Gateway-related resources can reside in the root compartment. However, if you expect multiple teams to create API gateways, best practice is to create a separate compartment for each team.
• To create API gateways and deploy APIs on them, you must belong to one of the following:
  • The tenancy's Administrators group.
  • A group to which policies grant the appropriate permissions on network and API Gateway-related resources. See Create Policies to Control Access to Network and API Gateway-Related Resources on page 342.
  • Policies must be defined to give the API gateways you create access to additional resources, if necessary. See Create a Policy to Give API Gateways Access to Functions on page 345.

Availability by Region

The API Gateway service is available in the Oracle Cloud Infrastructure regions listed at Regions and Availability Domains on page 180. Refer to that topic to see region identifiers, region keys, and availability domain names.
Configuring Your Tenancy for API Gateway Development

Before you can start using the API Gateway service to create API gateways and deploy APIs on them, you have to set up your tenancy for API gateway development.

When a tenancy is created, an Administrators group is automatically created for the tenancy. Users that are members of the Administrators group can perform any operation on resources in the tenancy. API Gateway service users are typically not members of the Administrators group, and do not have to be. However, a member of the Administrators group does need to perform a number of administrative tasks to enable users to use the API Gateway service.

To set up your tenancy for API gateway development, you have to complete the following tasks in the order shown in this checklist (the instructions in the topics below assume that you are a tenancy administrator):

<table>
<thead>
<tr>
<th>Task #</th>
<th>Tenancy Configuration Task</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create Groups and Users to Use API Gateway, if these don't exist already on page 339</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don't exist already on page 340</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Create a VCN to Use with API Gateway, if one doesn't exist already on page 340 See Example Network Resource Configurations on page 346 for details of typical network configurations.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Create Policies to Control Access to Network and API Gateway-Related Resources on page 342, and more specifically: • Create a Policy to Give API Gateway Users Access to API Gateway-Related Resources on page 342 • Create a Policy to Give API Gateway Users Access to Network Resources on page 343 • Create a Policy to Give API Gateway Users Access to Functions on page 344 • Create a Policy to Give API Gateways Access to Functions on page 345</td>
<td></td>
</tr>
</tbody>
</table>

Click each of the links in turn, and follow the instructions.

Create Groups and Users to Use API Gateway, if these don't exist already

Before users can start using the API Gateway service to create API gateways and deploy APIs on them, as a tenancy administrator you have to create Oracle Cloud Infrastructure user accounts, along with a group to which the user accounts belong. Later on, you'll define policies to give the group (and the user accounts that belong to it) access to API Gateway-related resources. If a suitable group and user accounts already exist, there's no need to create new ones.

To create groups and users to use the API Gateway service:

1. Log in to the Console as a tenancy administrator.
2. If a suitable group for API Gateway users doesn't exist already, create such a group as follows:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups. A list of
      the groups in your tenancy is displayed.
   b. Click Create Group and create a new group (see To create a group on page 2420). Give the group a
      meaningful name (for example, api-gateway-developers) and description. Avoid entering confidential
      information.
3. If suitable user accounts for API Gateway users don't exist already, create users as follows:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of
      the users in your tenancy is displayed.
   b. Click Create User and create one or more new users (see To create a user on page 2417).
4. If they haven't been added already, add users to the group to use the API Gateway service as follows:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of
      the users in your tenancy is displayed.
   b. Select one or more users and add them to the group authorized to use the API Gateway service (see To add a
      user to a group on page 2417).

Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don't exist already

Before users can start using the API Gateway service to create API gateways and deploy APIs on them, as a tenancy
administrator you have to create:

- a compartment to own network resources (a VCN, a public or private regional subnet, and other resources such as
  an internet gateway, a route table, security lists)
- a compartment to own API Gateway resources (API gateways, API deployments)

Note that the same compartment can own both network resources and API Gateway-related resources. Alternatively,
you can create two separate compartments for network resources and API Gateway-related resources.

If suitable compartments already exist, there's no need to create new ones.

To create a compartment to own network resources and/or API Gateway-related resources in the tenancy:

1. Log in to the Console as a tenancy administrator.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A
   list of the compartments in your tenancy is displayed.
3. Click Create Compartment and create a new compartment (see To create a compartment on page 2442). Give
   the compartment a meaningful name (for example, acme-network, acme-api-gateway-compartment,) and
   description. Avoid entering confidential information.

Tip:

Normally, API gateways and API deployments are created in the same compartment. However, in large development teams with many API
developers, you might find it useful to create separate compartments for
API gateways and for API deployments. Doing so will enable you to give
different groups of users appropriate access to those resources.

Create a VCN to Use with API Gateway, if one doesn't exist already

Before users can start using the API Gateway service to create API gateways and deploy APIs on them, as a tenancy
administrator you have to create one or more VCNs containing a public or private regional subnet in which to create
API gateways.

The VCN can be, but need not be, owned by the same compartment to which other API Gateway-related resources
will belong. To ensure high availability, API gateways can only be created in regional subnets (not AD-specific
subnets). Note that an API gateway must be able to reach the back ends defined in the API deployment specification.
For example, if the back end is on the public internet, the VCN must have an internet gateway to enable the API...
gateway to route requests to the back end. The VCN must have a set of DHCP options that includes an appropriate DNS resolver to map host names defined in an API deployment specification to IP addresses.

The public or private regional subnet in which to create API gateways must have a CIDR block that provides a minimum of 32 free IP addresses. Note that Oracle strongly recommends the CIDR block provides more than the minimum.

To support the largest possible number of concurrent connections, Oracle also strongly recommends that the security lists used by the subnet only have stateless rules.

If a suitable VCN already exists, there's no need to create a new one.

If you do decide to create a new VCN, you have several options, including the following:

- You can create just the VCN initially, and then create the regional subnets and other related resources later (as described in this topic). In this case, you can choose whether to create a public regional subnet and an internet gateway (see Internet Gateway on page 3243), or a private regional subnet and a service gateway (see Access to Oracle Services: Service Gateway on page 3256). For example, if you don't want to expose traffic over the public internet, create a private regional subnet and a service gateway.
- You can create the new VCN and have related resources created automatically at the same time by selecting the Start VCN Wizard option. In this case, a public regional subnet and a private regional subnet are created, along with an internet gateway, a NAT gateway, and a service gateway. Although a default security list is also created, you have to add a new stateful ingress rule for the regional subnet to allow traffic on port 443. That's because API Gateway communicates on port 443, and port 443 is not open by default (see the corresponding step in this topic).

See Example Network Resource Configurations on page 346 for details of typical network configurations.

To create a VCN to use with API Gateway:

1. Log in to the Console as a tenancy administrator.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
3. Choose the compartment that will own the network resources (on the left side of the page). For example, acme-network.
   
   The VCN can be, but need not be, owned by the same compartment to which API Gateway-related resources will belong. The page updates to display only the resources in the compartment you select.

4. Click Create Virtual Cloud Network to create a new VCN.

5. In the Create Virtual Cloud Network dialog box, enter the following:

   - Name: A meaningful name for the VCN, such as acme-api-gw-vcn. The name doesn't have to be unique, but you cannot change it later using the Console (although you can change it using the API). Avoid entering confidential information.
   - Other details for the VCN (see To create a VCN on page 2825).

6. Click Create Virtual Cloud Network to create the VCN.

   The VCN is created and displayed on the Virtual Cloud Networks page in the compartment you chose.

7. On the Virtual Cloud Networks page, click Create Subnet.

8. In the Create Subnet dialog box, enter the following:

   - Name: A meaningful name for the subnet, such as acme-api-gw-subnet. The name doesn't have to be unique, but you cannot change it later using the Console (although you can change it using the API). Avoid entering confidential information.
   - Subnet Type: Select Regional (Recommended). To ensure high availability, API gateways can only be created in regional subnets (not AD-specific subnets).
   - CIDR Block: A CIDR block that provides a minimum of 32 free IP addresses.
   - DHCP Options: (Optional) Select a set of DHCP options that includes an appropriate DNS resolver to map host names defined in an API deployment specification to IP addresses. If you do not explicitly specify a DHCP options set, the default DHCP options set uses the Oracle-provided Internet and VCN Resolver to
API Gateway communicates on port 443, which is not open by default. You have to add a new stateful ingress rule for the regional subnet to allow traffic on port 443.

10. Click the name of the regional subnet, then the name of the default security list, and then click Add Ingress Rules and enter the following:

- **Source Type:** CIDR
- **Source CIDR:** 0.0.0.0/0
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 443

11. Click Add Ingress Rules to add the new rule to the default security list.

### Create Policies to Control Access to Network and API Gateway-Related Resources

Before users can start using the API Gateway service to create API gateways and deploy APIs on them, as a tenancy administrator you have to create a number of Oracle Cloud Infrastructure policies to grant access to API Gateway-related and network resources.

To grant access to API Gateway-related and network resources, you have to:

- Grant users access to API Gateway-related resources, network resources, and (optionally) function resources. More specifically, you have to:
  - Create a Policy to Give API Gateway Users Access to API Gateway-Related Resources on page 342
  - Create a Policy to Give API Gateway Users Access to Network Resources on page 343
  - Create a Policy to Give API Gateway Users Access to Functions on page 344

- Grant API gateways access to functions defined in Oracle Functions, if required. If API Gateway users define a new API gateway with a serverless function in Oracle Functions as an API back end, the API Gateway service verifies that the new API gateway will have access to the specified function. To provide access, you have to create a policy that grants API gateways access to functions defined in Oracle Functions. See Create a Policy to Give API Gateway Users Access to Functions on page 345.

See Details for API Gateway on page 2173 for more information about policies.

### Create a Policy to Give API Gateway Users Access to API Gateway-Related Resources

When API Gateway users define a new API gateway and new API deployments, they have to specify a compartment for those API Gateway-related resources. Users can only specify a compartment that the groups to which they belong have been granted access. To enable users to specify a compartment, you must create an identity policy to grant the groups access.

To create a policy to give users access to API Gateway-related resources in the compartment that will own those resources:

1. Log in to the Console as a tenancy administrator.
2. In the Console, open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed.
3. Select the compartment that will own API Gateway-related resources from the list on the left.
4. Click Create Policy.
5. Enter the following:

- **Name:** A meaningful name for the policy (for example, acme-apigw-developers-manage-access). The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
- **Description:** A meaningful description (for example, Gives api-gateway developers access to all resources in the acme-apigw-compartment). You can change this later if you want to.
- **Statement:** The following policy statement to give the group access to all API Gateway-related resources in the compartment:

As **Statement 1:** enter the following policy statement to give the group access to all API Gateway-related resources in the compartment:

```
Allow group <group-name> to manage api-gateway-family in compartment <compartment-name>
```

For example:

```
Allow group acme-apigw-developers to manage api-gateway-family in compartment acme-apigw-compartment
```

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. Click **Create** to create the policy giving API Gateway users access to API Gateway-related resources in the compartment.

**Tip:**

Normally, API gateways and API deployments are created in the same compartment. However, in large development teams with many API developers, you might find it useful to create separate compartments for API gateways and for API deployments. Doing so will enable you to give different groups of users appropriate access to those resources.

**Create a Policy to Give API Gateway Users Access to Network Resources**

When API Gateway users define a new API gateway, they have to specify a VCN and a subnet in which to create the API gateway. Users can only specify VCNs and subnets that the groups to which they belong have been granted access. To enable users to specify a VCN and subnet, you must create an identity policy to grant the groups access. In addition, if you want to enable users to create public API gateways, the identity policy must allow the groups to manage public IP addresses in the compartment that owns the network resources.

To create a policy to give API Gateway users access to network resources:

1. Log in to the Console as a tenancy administrator.
2. In the Console, open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**. A list of the policies in the compartment you’re viewing is displayed.
3. Select the compartment that owns the network resources from the list on the left.
4. Click **Create Policy**.
5. Enter the following:

- **Name**: A meaningful name for the policy (for example, `acme-apigw-developers-network-access`). The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.

- **Description**: A meaningful description (for example, `Gives api-gateway developers access to all network resources in the acme-network compartment`). You can change this later if you want to.

- **Statement**: The following policy statement to give the group access to network resources in the compartment (including the ability to manage public IP addresses):

  ```
  Allow group <group-name> to manage virtual-network-family in compartment <compartment-name>
  ```

  For example:

  ```
  Allow group acme-apigw-developers to manage virtual-network-family in compartment acme-network
  ```

- **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. Click **Create** to create the policy giving API Gateway users access to network resources and public IP addresses in the compartment.

---

### Create a Policy to Give API Gateway Users Access to Functions

When API Gateway users define a new API gateway, one option is to specify a serverless function defined in Oracle Functions as the API back end. Users can only specify functions that the groups to which they belong have been granted access. If you want to enable users to specify functions as API back ends, you must create an identity policy to grant the groups access. Note that in addition to this policy for the user group, to enable users to specify functions as API back ends you also have to create a policy to give API gateways access to Oracle Functions (see [Create a Policy to Give API Gateways Access to Functions](#) on page 345).

Another reason to create an identity policy that grants groups access to Oracle Functions is if you want to enable users to use the Console (rather than a JSON file) to define an authentication request policy and specify an authorizer function defined in Oracle Functions (see [Using Authorizer Functions to Add Authentication and Authorization to API Deployments](#) on page 431).

To create a policy to give API Gateway users access to functions defined in Oracle Functions:

1. Log in to the Console as a tenancy administrator.
2. In the Console, open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**. A list of the policies in the compartment you're viewing is displayed.
3. Select the compartment that owns the functions from the list on the left.
4. Click **Create Policy**.
5. Enter the following:
   - **Name:** A meaningful name for the policy (for example, acme-apigw-developers-functions-access). The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
   - **Description:** A meaningful description (for example, Gives api-gateway developers access to all functions in the acme-functions-compartment). You can change this later if you want to.
   - **Statement:** The following policy statement to give the group access to the functions in the compartment:

   ```plaintext
   Allow group <group-name> to use functions-family in compartment <compartment-name>
   ```

   For example:

   ```plaintext
   Allow group acme-apigw-developers to use functions-family in compartment acme-functions-compartment
   ```

   - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. Click **Create** to create the policy giving API Gateway users access to functions in the compartment.

   **Create a Policy to Give API Gateways Access to Functions**

   When API Gateway users define a new API gateway, one option is to specify a serverless function defined in Oracle Functions as the API back end. Before creating the API gateway, the API Gateway service verifies that the new API gateway will have access to the specified function through an IAM policy.

   Note that in addition to this policy for API gateways, to enable users to specify functions as API back ends you also have to create a policy to give users access to Oracle Functions (see **Create a Policy to Give API Gateway Users Access to Functions** on page 344).

   To create a policy to give API gateways access to functions defined in Oracle Functions:

   1. Log in to the Console as a tenancy administrator.
2. Create a new policy to give API gateways access to functions defined in Oracle Functions:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
   b. Select the compartment containing the function-related resources to which you want to grant access. If the resources are in different compartments, select a common parent compartment (for example, the tenancy's root compartment).
   c. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acme-apigw-gateways-functions-policy).
   d. Enter a policy statement to give API gateways access to the compartment containing functions defined in Oracle Functions:

   ```allow any-user to use functions-family in compartment <functions-compartment-name> where ALL {request.principal.type='ApiGateway', request.resource.compartment.id='<api-gateway-compartment-OCID>'}`

   where:
   • `<functions-compartment-name>` is the name of the compartment containing the functions you want to use as back ends for API gateways.
   • `<api-gateway-compartment-OCID>` is the OCID of the compartment containing the API gateways that you want to have access to the functions.

   For example:

   ```allow any-user to use functions-family in compartment acme-functions-compartment where ALL {request.principal.type='ApiGateway', request.resource.compartment.id='ocid1.compartment.oc1..aaaaaaaa7______ysq'}`

   e. Click Create to create the policy giving API gateways access to functions defined in Oracle Functions.

Example Network Resource Configurations

Before you can use the API Gateway service to create API gateways and deploy APIs on them as API deployments:
   • You must have access to an Oracle Cloud Infrastructure tenancy. The tenancy must be subscribed to one or more of the regions in which API Gateway is available (see Availability by Region on page 338).
   • Your tenancy must have sufficient quota on API Gateway-related resources (see Service Limits on page 215).
   • Within your tenancy, there must already be a compartment to own the necessary network resources. If such a compartment does not exist already, you will have to create it. See Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don't exist already on page 340.
   • The compartment that owns network resources must contain a VCN, a public or private regional subnet, and other resources (such as an internet gateway, a route table, security lists). To ensure high availability, API gateways can only be created in regional subnets (not AD-specific subnets). Note that an API gateway must be able to reach the back ends defined in the API deployment specification. For example, if the back end is on the public internet, the VCN must have an internet gateway to enable the API gateway to route requests to the back end.
   • The VCN must have a set of DHCP options that includes an appropriate DNS resolver to map host names defined in an API deployment specification to IP addresses. If such a DHCP options set does not exist in the VCN already, you will have to create it. Select the DHCP options set for the API gateway's subnet as follows:
     • If the host name is publicly published on the internet, or if the host name belongs to an instance in the same VCN, select a DHCP options set that has the Oracle-provided Internet and VCN Resolver as the DNS Type. This is the default if you do not explicitly select a DHCP options set.
     • If the host name is on your own private or internal network (for example, connected to the VCN by FastConnect), select a DHCP options set that has Custom Resolver as the DNS Type, and has the URL of a suitable DNS server that can resolve the host name to an IP address.

   Note that you can change the DNS server details in the DHCP options set specified for an API gateway's subnet. The API gateway will be reconfigured to use the updated DNS server details within two hours. For more
information about resolving host names to IP addresses, see DNS in Your Virtual Cloud Network on page 2910 and DHCP Options on page 2917.

- Within your tenancy, there must already be a compartment to own API Gateway-related resources (API gateways, API deployments). This compartment can be, but need not be, the same compartment that contains the network resources. See Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don’t exist already on page 340. Note that the API Gateway-related resources can reside in the root compartment. However, if you expect multiple teams to create API gateways, best practice is to create a separate compartment for each team.

- To create API gateways and deploy APIs on them, you must belong to one of the following:
  - The tenancy’s Administrators group.
  - A group to which policies grant the appropriate permissions on network and API Gateway-related resources. See Create Policies to Control Access to Network and API Gateway-Related Resources on page 342.
  - Policies must be defined to give the API gateways you create access to additional resources, if necessary. See Create a Policy to Give API Gateways Access to Functions on page 345.

This topic gives examples of how you might configure network resources for API gateways with a serverless function as a back end:

- for a public API gateway in a public subnet (see Example 1: Example Network Resource Configuration for a Public API Gateway in a Public Subnet with a Serverless Function as an HTTP Back End on page 347)
- for a private API gateway in a private subnet (see Example 2: Network Resource Configuration for a Private API Gateway in a Private Subnet with a Serverless Function as an HTTP Back End on page 350)

These examples assume the default helloworld function has been created and deployed in Oracle Functions with the name helloworld-func and belonging to the helloworld-app application (see Creating, Deploying, and Invoking a Helloworld Function on page 2059).

**Example 1: Example Network Resource Configuration for a Public API Gateway in a Public Subnet with a Serverless Function as an HTTP Back End**

This example assumes you want a public API gateway that can be accessed directly from the internet, with a serverless function as an HTTP back end.
To achieve this example configuration, you create the following resources in the sequence shown, with the properties shown in the Example Resource Configuration table below:

1. A VCN named 'acme-vcn1'.
2. An internet gateway named 'acme-internet-gateway'.
3. A route table named 'acme-routetable-public'.
4. A security list named 'acme-security-list-public', with an ingress rule that allows public access to the API gateway and an egress rule that allows access to Oracle Functions.
5. A public subnet named 'acme-public-subnet'.
6. An API gateway named 'acme-public-gateway', with an API deployment named 'acme-public-deployment'.

Issuing a curl command from the public internet against the API deployment returns the response shown:

```
[user@machinename ~]$ curl -X GET https://lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com/marketing/hello
Hello, world!
```

### Example Network Resource Configuration

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCN</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: acme-vcn1</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td>Internet Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: acme-internet-gateway</td>
</tr>
<tr>
<td>Route Table</td>
<td>One route table created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: acme-routetable-public, with a route rule defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Destination CIDR block: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• Target Type: Internet Gateway</td>
</tr>
<tr>
<td></td>
<td>• Target Internet Gateway: acme-internet-gateway</td>
</tr>
<tr>
<td>DHCP Options</td>
<td>Created automatically and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• DNS Type set to Internet and VCN Resolver</td>
</tr>
<tr>
<td>Resource</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security List</td>
<td>One security list created manually (in addition to the default security list), named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List Name</strong>: acme-security-list-public, with a ingress rule that allows public access to the API gateway, and an egress rule that allows access to Oracle Functions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ingress Rule 1</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>: Stateful</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source Type</strong>: CIDR</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source CIDR</strong>: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Protocol</strong>: TCP</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source Port Range</strong>: All</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination Port Range</strong>: 443</td>
</tr>
<tr>
<td></td>
<td>• <strong>Egress Rule 1</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>: Stateful</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination Type</strong>: CIDR</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination CIDR</strong>: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Protocol</strong>: All Protocols</td>
</tr>
<tr>
<td>Subnet</td>
<td>One regional public subnet created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: acme-public-subnet with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block</strong>: 10.0.0.0/24</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route Table</strong>: acme-routetable-public</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet access</strong>: Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution</strong>: Selected</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP Options</strong>: Default</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List</strong>: acme-security-list-public</td>
</tr>
<tr>
<td>API Gateway</td>
<td>One public API gateway created and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: acme-public-gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>VCN</strong>: acme-vcn1</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet</strong>: acme-public-subnet</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hostname</strong>: (for the purpose of this example, the hostname is lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com)</td>
</tr>
</tbody>
</table>
One API deployment created and defined as follows:

- **Name**: acme-public-deployment
- **Path Prefix**: /marketing
- **API Request Policies**: None specified
- **API Logging**: None specified
- **Route**:
  - **Path**: /hello
  - **Methods**: GET
  - **Type**: Oracle Functions
  - **Application**: helloworld-app
  - **Function Name**: helloworld-func

**Example 2: Network Resource Configuration for a Private API Gateway in a Private Subnet with a Serverless Function as an HTTP Back End**

This example assumes you want a private API gateway that can only be accessed via a bastion host (rather than accessed directly from the internet), with a serverless function as an HTTP back end.

To achieve this example configuration, you create the following resources in the sequence shown, with the properties shown in the Example Resource Configuration table below:

1. A VCN named acme-vcn2
2. An internet gateway named acme-internet-gateway
3. A service gateway named acme-service-gateway. (In this example, you only need to create a service gateway, because the API gateway only has an Oracle Functions back end. However, if the API gateway has both an Oracle Functions back end and also an HTTP back end on the public internet, you could create a NAT gateway instead to access both back ends.)

4. A route table named acme-routetable-private

5. A security list named acme-security-list-private, with an ingress rule that allows the bastion host to access the API gateway and an egress rule that allows access to Oracle Functions.

6. A private subnet named acme-private-subnet

7. An API gateway named acme-private-gateway, with an API deployment named acme-private-deployment

8. A route table named acme-routetable-bastion

9. A security list named acme-security-list-bastion, with an ingress rule that allows public SSH access to the bastion host and an egress rule that allows the bastion host to access the API gateway.

10. A public subnet named acme-bastion-public-subnet

11. A compute instance with a public IP address to act as the bastion host, called acme-bastion-instance

Having SSH'd into the bastion host, issuing a curl command against the API deployment returns the response shown:

```
[user@machinename ~]$ ssh opc@198.51.100.254
[opc@acme-bastion-instance ~]$ curl -X GET https://pwa...djt.apigateway.us-phoenix-1.oci.customer-oci.com/marketing-private/hello
Hello, world!
```

**Example Resource Configuration**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCN</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: acme-vcn2</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block</strong>: 10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution</strong>: Selected</td>
</tr>
<tr>
<td>Internet Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: acme-internet-gateway</td>
</tr>
<tr>
<td>Service Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: acme-service-gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Services</strong>: All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
<tr>
<td>Resource</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Route Tables</td>
<td>Two route tables created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> acme-routetable-bastion, with a route rule defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination CIDR block:</strong> 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type:</strong> Internet Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Internet Gateway:</strong> acme-internet-gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> acme-routetable-private, with a route rule defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination CIDR block:</strong> 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type:</strong> Service Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination Service:</strong> All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Service Gateway:</strong> acme-service-gateway</td>
</tr>
<tr>
<td>DHCP Options</td>
<td>Created automatically and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Type</strong> set to Internet and VCN Resolver</td>
</tr>
<tr>
<td>Resource</td>
<td>Example</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security List</td>
<td>Two security lists created manually (in addition to the default security list), named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List Name</strong>: acme-security-list-bastion, with an ingress rule that allows public SSH access to the bastion host and an egress rule that allows the bastion host to access the API gateway:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ingress Rule 1</strong>:</td>
</tr>
<tr>
<td></td>
<td>• State: Stateful</td>
</tr>
<tr>
<td></td>
<td>• Source Type: CIDR</td>
</tr>
<tr>
<td></td>
<td>• Source CIDR: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• IP Protocol: TCP</td>
</tr>
<tr>
<td></td>
<td>• Destination Port Range: 22</td>
</tr>
<tr>
<td></td>
<td>• <strong>Egress Rule 1</strong>:</td>
</tr>
<tr>
<td></td>
<td>• State: Stateful</td>
</tr>
<tr>
<td></td>
<td>• Destination Type: CIDR</td>
</tr>
<tr>
<td></td>
<td>• Destination CIDR: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• IP Protocol: All Protocols</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List Name</strong>: acme-security-list-private, with an ingress rule that allows the bastion host to access the API gateway and an egress rule that allows access to Oracle Functions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ingress Rule 1</strong>:</td>
</tr>
<tr>
<td></td>
<td>• State: Stateful</td>
</tr>
<tr>
<td></td>
<td>• Source Type: CIDR</td>
</tr>
<tr>
<td></td>
<td>• Source CIDR: 10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• IP Protocol: TCP</td>
</tr>
<tr>
<td></td>
<td>• Destination Port Range: All</td>
</tr>
<tr>
<td></td>
<td>• Destination Port Range: 443</td>
</tr>
<tr>
<td></td>
<td>• <strong>Egress Rule 1</strong>:</td>
</tr>
<tr>
<td></td>
<td>• State: Stateful</td>
</tr>
<tr>
<td></td>
<td>• Destination Type: CIDR</td>
</tr>
<tr>
<td></td>
<td>• Destination CIDR: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• IP Protocol: All Protocols</td>
</tr>
<tr>
<td>Resource</td>
<td>Example</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subnet</td>
<td>Two regional subnets created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>- Name: acme-bastion-public-subnet, with the following properties:</td>
</tr>
<tr>
<td></td>
<td>- CIDR Block: 10.0.1.0/24</td>
</tr>
<tr>
<td></td>
<td>- Route Table: acme-routetable-bastion</td>
</tr>
<tr>
<td></td>
<td>- Subnet access: Public</td>
</tr>
<tr>
<td></td>
<td>- DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>- DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>- Security List: acme-security-list-bastion</td>
</tr>
<tr>
<td></td>
<td>- Name: acme-private-subnet, with the following properties:</td>
</tr>
<tr>
<td></td>
<td>- CIDR Block: 10.0.2.0/24</td>
</tr>
<tr>
<td></td>
<td>- Route Table: acme-routetable-private</td>
</tr>
<tr>
<td></td>
<td>- Subnet access: Private</td>
</tr>
<tr>
<td></td>
<td>- DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>- DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>- Security List: acme-security-list-private</td>
</tr>
<tr>
<td>API Gateway</td>
<td>One private API gateway created and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>- Name: acme-private-gateway</td>
</tr>
<tr>
<td></td>
<td>- Type: Private</td>
</tr>
<tr>
<td></td>
<td>- VCN: acme-vcn2</td>
</tr>
<tr>
<td></td>
<td>- Subnet: acme-private-subnet</td>
</tr>
<tr>
<td></td>
<td>- Hostname: (for the purpose of this example, the hostname is pwa...djt.apigateway.us-phoenix-1.oci.customer-oci.com)</td>
</tr>
<tr>
<td>API Deployment</td>
<td>One API deployment created and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>- Name: acme-private-deployment</td>
</tr>
<tr>
<td></td>
<td>- Path Prefix: /marketing-private</td>
</tr>
<tr>
<td></td>
<td>- API Request Policies: None specified</td>
</tr>
<tr>
<td></td>
<td>- API Logging: None specified</td>
</tr>
<tr>
<td></td>
<td>- Route:</td>
</tr>
<tr>
<td></td>
<td>- Path: /hello</td>
</tr>
<tr>
<td></td>
<td>- Methods: GET</td>
</tr>
<tr>
<td></td>
<td>- Type: Oracle Functions</td>
</tr>
<tr>
<td></td>
<td>- Application: helloworld-app</td>
</tr>
<tr>
<td></td>
<td>- Function Name: helloworld-func</td>
</tr>
<tr>
<td>Resource</td>
<td>Example</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>Instance</td>
<td>One compute instance created and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> acme-bastion-instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>Availability Domain:</strong> AD1</td>
</tr>
<tr>
<td></td>
<td>• <strong>Instance Type:</strong> Virtual Machine</td>
</tr>
<tr>
<td></td>
<td>• <strong>VCN:</strong> acme-vcn2</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet:</strong> acme-bastion-public-subnet</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assign a public IP address:</strong> Selected (for the purpose of this example, the instance is given the IP address 198.51.100.254)</td>
</tr>
</tbody>
</table>

**Configuring Your Client Environment for API Gateway Development**

When using the API Gateway service to create API gateways and API deployments, you can perform many operations using the Console. However, as well as using the Console, you'll typically also want to create and manage API gateways and API deployments programmatically using the API Gateway service's REST API.

You can use the API Gateway REST API using the Oracle Cloud Infrastructure CLI (for more information and configuration instructions, see Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).

**Configuring Your Client Environment to use the CLI for API Gateway Development**

In addition to using the Console to create API gateways and API deployments, you'll typically also want to create and manage API gateways and API deployments programmatically using the API Gateway service's REST API.

One way to use the API Gateway REST API is to use the Oracle Cloud Infrastructure CLI.

Before you can start using the Oracle Cloud Infrastructure CLI to create and manage API gateways and API deployments programmatically using the API Gateway REST API, you have to set up your client environment appropriately. Note that prior to setting up your client environment, you must already have set up your tenancy (see Configuring Your Tenancy for API Gateway Development on page 339).

To set up your client environment for API development using the Oracle Cloud Infrastructure CLI, you have to complete the following tasks in the order shown in this checklist:

<table>
<thead>
<tr>
<th>Task #</th>
<th>Development Environment Configuration Task</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Installing the CLI on page 4195</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Setting up the Config File on page 4197</td>
<td></td>
</tr>
</tbody>
</table>

Click each of the links in the checklist in turn, and follow the instructions.

**Creating an API Gateway**

You can create one or more API gateways to process traffic from API clients and route it to back-end services. Having created an API gateway, you then deploy an API on the API gateway by creating an API deployment.

You can use a single API gateway as the front end for multiple back-end services by:

- Creating a single API deployment on the API gateway, with an API deployment specification that defines multiple back-end services.
- Creating multiple API deployments on the same API gateway, each with an API deployment specification that defines one (or more) back-end services.
Having a single API gateway as a front end enables you to present a single cohesive API to API consumers and API clients, even if the API is actually comprised of smaller microservices written by different software teams using different programming languages or technologies.

**Using the Console**

To create an API gateway:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **API Gateway**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Gateways** page, click **Create Gateway** and specify:
   - **Name**: The name of the new API gateway. Avoid entering confidential information.
   - **Type**: The type of API gateway to create. Select Private if you want the API gateway (and the APIs deployed on it) to be accessible only from the same subnet in which the API gateway is created. Select Public if you want the API gateway (and the APIs deployed on it) to be accessible from the internet. In the case of a public API gateway, an internet gateway must exist to give access to the VCN.
   - **Compartment**: The compartment to which the new API gateway is to belong.
   - **Custom DNS**: Use this option to determine the TLS certificate (and associated domain name) that the API gateway uses.

   Do not select this option if you want the domain name to be generated automatically for you, and you want the API gateway to use a TLS certificate obtained by the API Gateway service (the default behavior). The auto-generated domain name will comprise a random string of characters followed by \`apigateway.<region-identifier>.oci.customer-oci.com\`. For example, `laksjd.apigateway.us-phoenix-1.oci.customer-oci.com`.

   Do select this option if you want the API gateway to use a custom TLS certificate (and associated custom domain name). In this case, specify the name of the default API Gateway certificate resource containing details of the custom TLS certificate (and associated custom domain name) that you want the API gateway to use.

   Note that for public or production systems, Oracle recommends using custom TLS certificates. Oracle recommends only using TLS certificates obtained by the API Gateway service for private or non-production systems (for example, for development and testing).

   See [Setting Up Custom Domains and TLS Certificates](#) on page 371.
   - **VCN in `<compartment-name>`**: The VCN in which to create the API gateway. The VCN can belong to the same compartment as the new API gateway, but does not have to.
   - **Subnet in `<compartment-name>`**: The name of a public or private regional subnet in which to create the API gateway. If you want to create a public API gateway, you must specify a public regional subnet.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

4. Click **Create** to create the new API gateway.

   Note that it can take a few minutes to create the new API gateway. While it is being created, the API gateway is shown with a state of Creating on the **Gateways** page. When it has been created successfully, the new API gateway is shown with a state of Active.

5. If you have waited more than a few minutes for the API gateway to be shown with an Active state (or if the API gateway creation operation has failed):
   a. Click the name of the API gateway, and click **Work Requests** to see an overview of the API gateway creation operation.
   b. Click the **Create Gateway** operation to see more information about the operation (including error messages, log messages, and the status of associated resources).
   c. If the API gateway creation operation has failed and you cannot diagnose the cause of the problem from the work request information, see [Troubleshooting API Gateway](#) on page 474.
Having successfully created an API gateway, you can deploy an API on it (see Deploying an API on an API Gateway by Creating an API Deployment on page 363).

**Using the CLI**

To create a new API gateway using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).
2. Open a command prompt and run `oci api-gateway gateway create` to create the API gateway:

   ```
   oci api-gateway gateway create --display-name "<gateway-name>" --compartment-id <compartment-ocid> --endpoint-type "<gateway-type>" --subnet-id <subnet-ocid> --certificate-id <certificate-ocid>
   ```

   where:
   - `<gateway-name>` is the name of the new API gateway. Avoid entering confidential information.
   - `<compartment-ocid>` is the OCID of the compartment to which the new API gateway will belong.
   - `<gateway-type>` is the type of API gateway to create. Specify `PRIVATE` if you want the API gateway (and the APIs deployed on it) to be accessible only from the same subnet in which the API gateway is created. Specify `PUBLIC` if you want the API gateway (and the APIs deployed on it) to be accessible from the internet.
   - `<subnet-ocid>` is the OCID of a public or private regional subnet in which to create the API gateway. If you want to create a public API gateway, you must specify a public regional subnet.
   - `<certificate-ocid>` (optional) is the OCID of the API Gateway certificate resource created for the API gateway's custom TLS certificate. See Setting Up Custom Domains and TLS Certificates on page 371.

   For example:

   ```
   oci api-gateway gateway create --display-name "Hello World Gateway" --compartment-id ocid1.compartment.oc1..aaaaaaaa7_____ysq --endpoint-type "PRIVATE" --subnet-id ocid1.subnet.oc1.iad.aaaaaaaaz______rca
   ```

   The response to the command includes:
   - The API gateway's OCID.
   - The host name, as the domain name to use when calling an API deployed on the API gateway. If you didn't specify an API Gateway certificate resource when creating the API gateway, a domain name is automatically generated in the format `<gateway-identifier>.apigateway.<region-identifier>.oci.customer-oci.com`, where:
     - `<gateway-identifier>` is a string of characters that identifies the API gateway. For example, lak...sjd (abbreviated for readability).
     - `<region-identifier>` is the identifier of the region in which the API gateway has been created. See Availability by Region on page 338.
   - For example, lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com.
   - The lifecycle state (for example, ACTIVE, FAILED).
   - The id of the work request to create the API gateway (details of work requests are available for seven days after completion, cancellation, or failure).

   If you want the command to wait to return control until the API gateway is active (or the request has failed), include either or both the following parameters:
   - `--wait-for-state ACTIVE`
   - `--wait-for-state FAILED`

   For example:

   ```
   oci api-gateway gateway create --display-name "Hello World Gateway" --compartment-id ocid1.compartment.oc1..aaaaaaaa7_____ysq --endpoint-type
   ```
Note that you cannot use the API gateway until the work request has successfully created it and the API gateway is active.

3. (Optional) To see the status of the API gateway, enter:

```
oci api-gateway gateway get --gateway-id <gateway-ocid>
```

4. (Optional) To see the status of the work request that is creating the API gateway, enter:

```
oci api-gateway work-request get --work-request-id <work-request-ocid>
```

5. (Optional) To view the logs of the work request that is creating the API gateway, enter:

```
oci api-gateway work-request-log list --work-request-id <work-request-ocid>
```

6. (Optional) If the work request that is creating the API gateway fails and you want to review the error logs, enter:

```
oci api-gateway work-request-error --work-request-id <work-request-ocid>
```

For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the CreateGateway operation to create an API gateway.

**Creating an API Resource with an API Description**

When using the API Gateway service, you have the option to create an API resource. You can use the API resource to deploy an API on an API gateway. The API resource has an API description that describes the API.

If you use an API resource to deploy an API on an API gateway, its API description pre-populates some of the properties of the API deployment specification.

You import the API description from a file (sometimes called an 'API specification', or 'API spec') written in a supported language. Currently, OpenAPI Specification version 2.0 (formerly Swagger Specification 2.0) and version 3.0 are supported.

Note that creating an API resource in the API Gateway service is optional. You can deploy an API on an API gateway without creating an API resource in the API Gateway service. Note also that you can create an API resource that doesn't have an API description initially, and then add an API description later.

**Using the Console**

To create an API resource, optionally with an API description created from an uploaded API description file, using the Console:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click API Gateway.
2. Choose a Compartment you have permission to work in.
3. On the APIs page, click **Create API Resource** and specify:
   - **Name**: The name of the new API resource. Avoid entering confidential information.
   - **Compartment**: The compartment to which the new API resource is to belong.
   - **Upload API Description File**: (optional) A file containing an API description (in a supported language) to upload and from which to create the API description. The file can be up to 1MB in size. The file is parsed to confirm that it is in a supported language and correctly formatted. Currently, OpenAPI Specification version 2.0 (formerly Swagger Specification 2.0) and version 3.0 files are supported.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

4. Click **Create** to create the new API resource.
   
   If you uploaded an API description file, an API description is created and validated. Note that it can take a few minutes to validate the API description. While it is being validated, the API description is shown with a state of Validating on the Validations page. When the API description has been validated successfully:
   - The Validations page shows successful validation.
   - The API description page shows the API description created from the API description file.
   - The API Deployment Specification page shows any additional information about the default API deployment specification created from the API description.

5. If you have waited more than a few minutes for the API description to be shown as Valid (or if the API description validation operation has failed):
   
   a. Click **Work Requests** to see an overview of the API description validation operation.
   b. Click the **Validate API** operation to see more information about the operation (including error messages, log messages, and the status of associated resources).
   c. If the API description validation operation has failed and you cannot diagnose the cause of the problem from the work request information, see Troubleshooting API Gateway on page 474.

6. If you don't upload an API description file when you first create an API resource, or if you subsequently want to upload a different API description file:
   
   a. On the APIs page, select **Edit** from the Actions menu beside the API resource.
   b. Provide details of the API description file from which to create the API description.

Having successfully created an API resource with an API description, you can deploy it on an API gateway (see Using the Console to Create an API Deployment from an API Resource on page 366).

**Using the CLI**

To create an API resource, optionally with an API description created from an uploaded API description file, using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).
2. Open a command prompt and run `oci api-gateway api create` to create the API resource:

```
oci api-gateway api create --display-name "<api-name>" --compartment-id <compartment-ocid> --content "<api-description>"
```

where:

- `<api-name>` is the name of the new API resource. Avoid entering confidential information.
- `<compartment-ocid>` is the OCID of the compartment to which the new API resource will belong.
- `<api-description>` is optionally an API description (in a supported language). The value you specify for `<api-description>` can be:
  - The entire API description, enclosed within double quotes. Inside the description, each double quote must be escaped with a backslash (`\`) character. For example (and abbreviated for readability), `--content "swagger:2.0",title:"Sample API",..."`
  - The name and location of an API description file, enclosed within double quotes and in the format `"$<path>/<filename>.yaml"`. For example, `--content "$<path>/api.yaml"`

The description is parsed to confirm that it is in a supported language and correctly formatted. Currently, OpenAPI Specification version 2.0 (formerly Swagger Specification 2.0) and version 3.0 files are supported.

For example:

```
oci api-gateway api create --display-name "Hello World API Resource" --compartment-id ocid1.compartment.oc1..aaaaaaa7____ysq --content "swagger:2.0",title:"Sample API",..."
```

The response to the command includes:

- The API resource's OCID.
- The lifecycle state (for example, SUCCEEDED, FAILED).
- The id of the work request to create the API resource (details of work requests are available for seven days after completion, cancellation, or failure).

If you want the command to wait to return control until the API resource has been created (or the request has failed), include either or both the following parameters:

- `--wait-for-state SUCCEEDED`
- `--wait-for-state FAILED`

For example:

```
oci api-gateway api create --display-name "Hello World API Resource" --compartment-id ocid1.compartment.oc1..aaaaaaa7____ysq --content "swagger:2.0",title:"Sample API",..." --wait-for-state SUCCEEDED
```

Note that you cannot use the API resource until the work request has successfully created it.

3. (Optional) To see the status of the work request that is creating the API resource, enter:

```
oci api-gateway work-request get --work-request-id <work-request-ocid>
```

4. (Optional) To view the logs of the work request that is creating the API resource, enter:

```
oci api-gateway work-request-log list --work-request-id <work-request-ocid>
```

5. (Optional) If the work request that is creating the API resource fails and you want to review the error logs, enter:

```
oci api-gateway work-request-error --work-request-id <work-request-ocid>
```
For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the CreateAPI operation to create an API resource.

### Creating an API Deployment Specification

Before you can deploy an API on an API gateway, you have to create an API deployment specification. Every API deployment has an API deployment specification.

Each API deployment specification describes a set of resources, and the methods (for example, GET, PUT) that can be performed on each resource.

You can use a single API gateway as the front end for multiple back-end services by:

- Creating a single API deployment on the API gateway, with an API deployment specification that defines multiple back-end services.
- Creating multiple API deployments on the same API gateway, each with an API deployment specification that defines one (or more) back-end services.

Typically, back-end services will be in the same VCN as the API gateway on which you deploy an API. However, they don't have to be. In the API deployment specification, you can describe back-end services that are on a private or public subnet in your tenancy, as well as services outside your tenancy (including on the public internet). Wherever they are located, the back-end services must be routable from the subnet containing the API gateway on which the API is deployed. For example, if the back-end service is on the public internet, the VCN must have an internet gateway to enable the API gateway to route requests to the back-end service.

You can create an API deployment specification:

- Using dialogs in the Console whilst creating an API deployment.
- Using your preferred JSON editor to create a separate JSON file. You can then specify the JSON file when using the Console, the CLI, or the API to create an API deployment.
- Using an API description file you upload for an API resource. The API description file provides some initial values for the API deployment specification, which you can modify and extend when deploying the API resource on an API gateway. See Creating an API Resource with an API Description on page 358.

The instructions in this topic show a basic API deployment specification with a single backend, only one route, and no request or response policies. See Example API Deployment Specification with Multiple Back Ends on page 363 for a more typical API deployment specification that includes multiple back ends, each with one or more routes.

In addition, you can add request and response policies that apply to routes in an API deployment specification (see Adding Request Policies and Response Policies to API Deployment Specifications on page 417).

### Using the Console to Create an API Deployment Specification

To create an API deployment specification whilst creating an API deployment using dialogs in the Console, see Using the Console to Create an API Deployment from Scratch on page 364.

### Using a JSON Editor to Create an API Deployment Specification in a Separate JSON File

To create an API deployment specification in a JSON file:

1. Using your preferred JSON editor, create the API deployment specification in a JSON file in the format:

   ```json
   {
     "requestPolicies": {},
   }
   ```
"routes": [
  {
    "path": "<api-route-path>",
    "methods": ["<method-list>"],
    "backend": {
      "type": "<backend-type>",
      "<backend-target>": "<identifier>"
    },
    "requestPolicies": {}
  }
]

where:

- "requestPolicies" specifies optional policies to control the behavior of an API deployment. If you want to apply policies to all routes in an API deployment specification, place the policies outside the routes section. If you want to apply the policies just to a particular route, place the policies inside the routes section. See Adding Request Policies and Response Policies to API Deployment Specifications on page 417.

- <api-route-path> specifies a path for API calls using the listed methods to the back-end service. Note that the route path you specify:
  - is relative to the deployment path prefix (see Deploying an API on an API Gateway by Creating an API Deployment on page 363)
  - must be preceded by a forward slash (/), and can be just that single forward slash
  - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters \$ - _ . + ! * ' ( ) , % ; : @ & =
  - can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)

- <method-list> specifies one or more methods accepted by the back-end service, separated by commas. For example, "GET, PUT".

- <backend-type> specifies the type of the back-end service. Valid values are ORACLE_FUNCTIONS_BACKEND, HTTP_BACKEND, and STOCK_RESPONSE_BACKEND.

- <backend-target> and <identifier> specify the back-end service. Valid values for <backend-target> and <identifier> depend on the value of <backend-type>, as follows:
  - If you set <backend-type> to ORACLE_FUNCTIONS_BACKEND, then replace <backend-target> with functionId, and replace <identifier> with the OCID of the function. For example, "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab5b...". See Adding a Function in Oracle Functions as an API Gateway Back End on page 410.
  - If you set <backend-type> to HTTP_BACKEND, then replace <backend-target> with url, and replace <identifier> with the URL of the back-end service. For example, "url": "https://api.weather.gov". See Adding an HTTP or HTTPS URL as an API Gateway Back End on page 406.
  - If you set <backend-type> to STOCK_RESPONSE_BACKEND, then replace <backend-target> and <identifier> with appropriate key-value pairs. See Adding Stock Responses as an API Gateway Back End on page 413.

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
```
For a more complex example that defines multiple back ends, see Example API Deployment Specification with Multiple Back Ends on page 363.

2. Save the JSON file containing the API deployment specification.

3. Use the API deployment specification when you create or update an API deployment in the following ways:
   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363.

Using an API Description File to Create an API Deployment Specification

To create an API deployment specification based on an API description file you upload for an API resource, see Creating an API Resource with an API Description on page 358

The API description file provides some initial values for the API deployment specification, which you can modify and extend when deploying the API resource on an API gateway.

Example API Deployment Specification with Multiple Back Ends

You can create a single API deployment on an API gateway, with an API deployment specification that defines multiple back-end services.

For example, the following API deployment specification defines a simple Hello World serverless function in Oracle Functions as one back end, and the National Weather Service API as a second back end.

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab________xmq"
            }
        },
        {
            "path": "/weather",
            "methods": ["GET"],
            "backend": {
                "type": "HTTP_BACKEND",
                "url": "https://api.weather.gov"
            }
        }
    ]
}
```

Deploying an API on an API Gateway by Creating an API Deployment

Having created an API gateway, you deploy an API on the API gateway by creating an API deployment. When you create an API deployment, you include an API deployment specification that defines the API. The API Gateway service inspects the API deployment specification to confirm that it is valid.

You can use a single API gateway as the front end for multiple back-end services by:
• Creating a single API deployment on the API gateway, with an API deployment specification that defines multiple back-end services.
• Creating multiple API deployments on the same API gateway, each with an API deployment specification that defines one (or more) back-end services.

**Using the Console to Create an API Deployment from Scratch**

To use the Console to create an API deployment, entering the API deployment specification in dialogs in the Console as you go:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **API Gateway**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Gateways** page, click the name of the API gateway on which you want to deploy the API to show the **Gateway Details** page.
4. On the **Gateway Details** page, select **Deployments** from the **Resources** list, and then click **Create Deployment**.
5. Click **From Scratch** and in the **Basic Information** section, specify:
   - **Name**: The name of the new API deployment. Avoid entering confidential information.
   - **Path Prefix**: A path on which to deploy all routes contained in the API deployment specification. For example:
     - /v1
     - /v2
     - /test/20191122
     Note that the deployment path prefix you specify:
     - must be preceded by a forward slash ( / )
     - can contain multiple forward slashes (provided they are not adjacent), but must not end with a forward slash
     - can include alphanumeric uppercase and lowercase characters
     - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
     - cannot include parameters and wildcards
   - **Compartment**: The compartment in which to create the new API deployment.
6. (Optional) In the **API Request Policies** section, optionally specify request policy details to provide support for:
   - **Authentication**: Click **Add** and enter details for an authentication request policy (see **Adding Authentication and Authorization to API Deployments** on page 431).
   - **CORS**: Click **Add** and enter details for a CORS request policy (see **Adding CORS support to API Deployments** on page 424).
   - **Rate Limiting**: Click **Add** and enter details for a rate limiting request policy (see **Limiting the Number of Requests to API Gateway Back Ends** on page 421).
7. (Optional) In the **API Logging Policies** section, optionally specify an execution log level to record information about processing within the API gateway. See **Adding Logging to API Deployments** on page 397.
8. (Optional) Click **Show Advanced Options** and optionally specify:
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
9. Click **Next** to enter details of the routes in the API deployment.
10. In the **Route 1** section, specify the first route in the API deployment that maps a path and one or more methods to a back-end service:

- **Path:** A path for API calls using the listed methods to the back-end service. Note that the route path you specify:
  - is relative to the deployment path prefix
  - must be preceded by a forward slash (/), and can be just that single forward slash
  - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)
- **Methods:** One or more methods accepted by the back-end service, separated by commas. For example, GET, PUT.
- **Type:** The type of the back-end service, as one of:
  - **HTTP:** For an HTTP back end, you also need to specify a URL, timeout details, and whether to disable SSL verification (see Adding an HTTP or HTTPS URL as an API Gateway Back End on page 406).
  - **Oracle Functions:** For an Oracle Functions back end, you also need to specify the application and function (see Adding a Function in Oracle Functions as an API Gateway Back End on page 410).
  - **Stock Response:** For a stock response back end, you also need to specify the HTTP status code, the content in the body of the response, and one or more HTTP header fields (see Adding Stock Responses as an API Gateway Back End on page 413).

11. (Optional) Click **Another Route** to enter details of additional routes.

12. Click **Next** to review the details you entered for the new API deployment.

13. Click **Create** to create the new API deployment.

   Note that it can take a few minutes to create the new API deployment. While it is being created, the API deployment is shown with a state of Creating on the **Gateway Details** page. When it has been created successfully, the new API deployment is shown with a state of Active.

14. If you have waited more than a few minutes for the API deployment to be shown with an Active state (or if the API deployment creation operation has failed):

   a. Click the name of the API deployment, and click **Work Requests** to see an overview of the API deployment creation operation.
   b. Click the **Create Deployment** operation to see more information about the operation (including error messages, log messages, and the status of associated resources).
   c. If the API deployment creation operation has failed and you cannot diagnose the cause of the problem from the work request information, see Troubleshooting API Gateway on page 474.

15. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

### Using the Console to Create an API Deployment from a JSON File

To use the Console to create an API deployment, uploading the API deployment specification from a JSON file:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **API Gateway**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Gateways** page, click the name of the API gateway on which you want to deploy the API to show the **Gateway Details** page.
4. On the **Gateway Details** page, select **Deployments** from the **Resources** list, and then click **Create Deployment**.
5. Click **Upload an existing API**.
6. In the **Upload Information** section, specify:
   - **Name**: The name of the new API deployment. Avoid entering confidential information.
   - **Path Prefix**: A path on which to deploy all routes contained in the API deployment specification. For example:
     - `/v1`
     - `/v2`
     - `/test/20191122`

   Note that the deployment path prefix you specify:
   - must be preceded by a forward slash (`/`)  
   - can contain multiple forward slashes (provided they are not adjacent), but must not end with a forward slash
   - can include alphanumeric uppercase and lowercase characters
   - can include the special characters `$_+!*()%,@&=`
   - cannot include parameters and wildcards

   - **Compartment**: The compartment in which to create the new API deployment.
   - **Specification**: The JSON file containing the API deployment specification, either by dragging and dropping the file, or by clicking **select one**. See **Creating an API Deployment Specification** on page 361.

7. (Optional) Click **Show Advanced Options** and optionally specify:
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

8. Click **Next** to review the details you entered for the new API deployment.

9. Click **Create** to create the new API deployment.

   Note that it can take a few minutes to create the new API deployment. While it is being created, the API deployment is shown with a state of Creating on the **Gateway Details** page. When it has been created successfully, the new API deployment is shown with a state of Active.

10. If you have waited more than a few minutes for the API deployment to be shown with an Active state (or if the API deployment creation operation has failed):
    a. Click the name of the API deployment, and click **Work Requests** to see an overview of the API deployment creation operation.
    b. Click the **Create Deployment** operation to see more information about the operation (including error messages, log messages, and the status of associated resources).
    c. If the API deployment creation operation has failed and you cannot diagnose the cause of the problem from the work request information, see **Troubleshooting API Gateway** on page 474.

11. (Optional) Confirm the API has been deployed successfully by calling it (see **Calling an API Deployed on an API Gateway** on page 384).

### Using the Console to Create an API Deployment from an API Resource

You can create an API deployment from an existing API resource, using the API resource's API description. In this case, the API description is based on an API description file you've uploaded for the API resource (see **Creating an API Resource with an API Description** on page 358). The API description file provides some initial values for the API deployment specification, which you can modify and extend when creating the API deployment. In particular, a default route is created for each path and associated method in the API description.

To use the Console to create an API deployment from an existing API resource, using an API deployment specification derived from an API description file:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **API Gateway**.
2. Choose a **Compartment** you have permission to work in.
3. On the **APIs** page, click the name of the API resource that you want to deploy.

4. (Optional) On the **API Details** page, select **API Deployment Specification** from the **Resources** list to confirm that a valid API deployment specification has been created for the API resource from an uploaded API description file. If no API deployment specification is available, see **Creating an API Resource with an API Description** on page 358.

5. On the **API Details** page, click **Deploy API Gateway** to use the Console dialogs for creating an API deployment.

Some of the initial values for the API deployment specification properties shown in the Console dialogs are derived from the API description file.

The **API Information** section shows details about the API resource from which to create the API deployment.

6. In the **Gateway** section, select the API gateway on which to create the API deployment. If a suitable API gateway does not already exist, click **Create Gateway** to create one (see **Creating an API Gateway** on page 355).

7. In the **Basic Information** section, specify:
   - **Name**: The name of the new API deployment. Avoid entering confidential information.
   - **Path Prefix**: A path on which to deploy all routes contained in the API deployment specification.
     
     For example:
     - `/v1`
     - `/v2`
     - `/test/20191122`
     
     Note that the deployment path prefix you specify:
     - must be preceded by a forward slash (`/`)
     - can contain multiple forward slashes (provided they are not adjacent), but must not end with a forward slash
     - can include alphanumeric uppercase and lowercase characters
     - can include the special characters `$_.+!*()%,@&=`
     - cannot include parameters and wildcards
   - **Compartment**: The compartment in which to create the new API deployment.

8. (Optional) In the **API Request Policies** section, optionally specify request policy details to provide support for:
   - **Authentication**: Click **Add** and enter details for an authentication request policy (see **Adding Authentication and Authorization to API Deployments** on page 431).
   - **CORS**: Click **Add** and enter details for a CORS request policy (see **Adding CORS support to API Deployments** on page 424).
   - **Rate Limiting**: Click **Add** and enter details for a rate limiting request policy (see **Limiting the Number of Requests to API Gateway Back Ends** on page 421).

9. (Optional) In the **API Logging Policies** section, optionally specify an execution log level to record information about processing within the API gateway. See **Adding Logging to API Deployments** on page 397.

10. (Optional) Click **Show Advanced Options** and optionally specify:
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

11. Click **Next** to review and enter details of the routes in the API deployment.

    By default, a route is created for every path and associated method that is present in the API description. Initially, each of these default routes is created with a stock response back end. The HTTP status code, the content in the body of the response body content, and the header are obtained from the details in the API description. If the API description does not include response information for a particular path and associated method, a default stock response back end is created for that route with 501 as the HTTP status code.
12. Review each default route in turn, modifying its configuration if necessary to meet your requirements, and adding request, response, and logging policies:

- **Path**: A path for API calls using the listed methods to the back-end service. Note that the route path you specify:
  - is relative to the deployment path prefix
  - must be preceded by a forward slash (\/), and can be just that single forward slash
  - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)

- **Methods**: One or more methods accepted by the back-end service, separated by commas. For example, GET, PUT.

- **Type**: The type of the back-end service, as one of:
  - **HTTP**: For an HTTP back end, you also need to specify a URL, timeout details, and whether to disable SSL verification (see Adding an HTTP or HTTPS URL as an API Gateway Back End on page 406).
  - **Oracle Functions**: For an Oracle Functions back end, you also need to specify the application and function (see Adding a Function in Oracle Functions as an API Gateway Back End on page 410).
  - **Stock Response**: For a stock response back end, you also need to specify the HTTP status code, the content in the body of the response, and one or more HTTP header fields (see Adding Stock Responses as an API Gateway Back End on page 413).

- **Show Route Request Policies**: and **Show Route Response Policies**: Review and optionally update the request policies and response policies that apply to the route. See Adding Request Policies and Response Policies to API Deployment Specifications on page 417.

- **Show Route Logging Policies**: Review and optionally update the logging policy that applies to the route. See Adding Logging to API Deployments on page 397.

13. (Optional) Click **Another Route** to enter details of more routes, in addition to those created by default from the API description.

14. Click **Next** to review the details you entered for the new API deployment.

15. Click **Create** to create the new API deployment.

Note that it can take a few minutes to create the new API deployment. While it is being created, the API deployment is shown with a state of Creating on the Gateway Details page. When it has been created successfully, the new API deployment is shown with a state of Active.

16. If you have waited more than a few minutes for the API deployment to be shown with an Active state (or if the API deployment creation operation has failed):
   a. Click the name of the API deployment, and click **Work Requests** to see an overview of the API deployment creation operation.
   b. Click the **Create Deployment** operation to see more information about the operation (including error messages, log messages, and the status of associated resources).
   c. If the API deployment creation operation has failed and you cannot diagnose the cause of the problem from the work request information, see Troubleshooting API Gateway on page 474.

17. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

**Using the CLI**

To create a new API deployment using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).
2. Open a command prompt and run `oci api-gateway deployment create` to create the deployment:

```
oci api-gateway deployment create --compartment-id <compartment-ocid>
--display-name <api-name> --gateway-id <gateway-ocid> --path-prefix "/<deployment-path-prefix>"
--specification file:///<filename>
```

where:

- `<compartment-ocid>` is the OCID of the compartment in which to create the new API deployment.
- `<api-name>` is the name of the new API deployment. Avoid entering confidential information.
- `<gateway-ocid>` is the OCID of the existing gateway on which to deploy the API. To find out the API gateway's OCID, see Listing API Gateways and API Deployments on page 386.
- `/<deployment-path-prefix>` is a path on which to deploy all routes contained in the API deployment specification.

Note that the deployment path prefix you specify:

- must be preceded by a forward slash (`/`) in the JSON file
- can contain multiple forward slashes (provided they are not adjacent), but must not end with a forward slash
- can include alphanumeric uppercase and lowercase characters
- can include the special characters `$ - _ . + ! * ' ( ) , % ; : @ & =`
- cannot include parameters and wildcards
- `<filename>` is the API deployment specification, including a path, one or more methods, and a back end definition. See Creating an API Deployment Specification on page 361.

For example:

```
oci api-gateway deployment create --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq --display-name "Marketing Deployment" --gateway-id ocid1.apigateway.oc1..aaaaaaaab_____hga
```
The response to the command includes:

- The API deployment's OCID.
- The host name on which the API deployment has been created, as a domain name in the format `<gateway-identifier>.apigateway.<region-identifier>.oci.customer-oci.com`, where:
  - `<gateway-identifier>` is the string of characters that identifies the API gateway. For example, lak...sja (abbreviated for readability).
  - `<region-identifier>` is the identifier of the region in which the API deployment has been created. See Availability by Region on page 338.

For example, lak...sja.apigateway.us-phoenix-1.oci.customer-oci.com.

- The lifecycle state (for example, ACTIVE, FAILED).
- The id of the work request to create the API deployment (details of work requests are available for seven days after completion, cancellation, or failure).

If you want the command to wait to return control until the API deployment is active (or the request has failed), include either or both the following parameters:

- `--wait-for-state ACTIVE`
- `--wait-for-state FAILED`

For example:

```bash
oci api-gateway deployment create --compartment-id ocid1.compartment.oc1..aaaaaaaa7_____ysq --display-name "Marketing Deployment" --gateway-id ocid1.apigateway.oc1..aaaaaaaab_____hga --path-prefix "/marketing" --specification file:///Users/jdoe/work/deployment.json --wait-for-state ACTIVE
```

Note that you cannot use the API deployment until the work request has successfully created it and the API deployment is active.

3. (Optional) To see the status of the API deployment, enter:

```bash
oci api-gateway deployment get --deployment-id <deployment-ocid>
```

4. (Optional) To see the status of the work request that is creating the API deployment, enter:

```bash
oci api-gateway work-request get --work-request-id <work-request-ocid>
```

5. (Optional) To view the logs of the work request that is creating the API deployment, enter:

```bash
oci api-gateway work-request-log list --work-request-id <work-request-ocid>
```

6. (Optional) If the work request that is creating the API deployment fails and you want to review the error logs, enter:

```bash
oci api-gateway work-request-error --work-request-id <work-request-ocid>
```

For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use the `CreateDeployment` operation to create an API deployment.

### Setting Up Custom Domains and TLS Certificates

The API gateways you create with the API Gateway service are TLS-enabled, and therefore require TLS certificates (formerly SSL certificates) issued by a Certificate Authority to secure them. To specify a particular custom domain name for an API gateway, you must obtain a custom TLS certificate from a Certificate Authority yourself, rather than have the API Gateway service obtain a TLS certificate for you.

When you create an API gateway, you specify that the API gateway uses one of the following:

- A TLS certificate that the API Gateway service obtains for you (the default behavior). In this case, the API Gateway service requests a TLS certificate from an Oracle-designated Certificate Authority.
- A custom TLS certificate that you obtain from your chosen Certificate Authority yourself. Your request to the Certificate Authority includes the custom domain name. The Certificate Authority returns a file containing the custom TLS certificate, and typically one or more files containing intermediate certificates forming a certificate chain from the TLS certificate back to the Certificate Authority.

To enable API gateways to use a custom TLS certificate, you create an API Gateway certificate resource comprising the custom TLS certificate, any intermediate certificates, and the private key used to generate the TLS certificate. You then specify that API Gateway certificate resource when creating a new API gateway.

The way in which the TLS certificate is obtained determines how much control you have over the API gateway's domain name:

- If the API Gateway service obtains a TLS certificate for you, the API Gateway service gives the API gateway an auto-generated domain name. The auto-generated domain name comprises a random string of characters followed by `.apigateway.<region-identifier>.oci.customer-oci.com`. For example, `lakjsd.apigateway.us-phoenix-1.oci.customer-oci.com`.
- If you obtain a custom TLS certificate yourself, the API Gateway service gives the API gateway the custom domain name you specified in your request to the Certificate Authority.

The way in which the TLS certificate is obtained also determines responsibility for recording the mapping between the API gateway's domain name and its public IP address with a DNS provider:

- If the API Gateway service obtains a TLS certificate for you, the API Gateway service takes responsibility for recording the mapping between the API gateway's auto-generated domain name and its public IP address with the Oracle Cloud Infrastructure DNS service.
- If you obtain a custom TLS certificate yourself, you are responsible for recording the mapping between the API gateway's custom domain name and its public IP address with your chosen DNS provider as an A record.

Similarly, the handling of TLS certificate expiry and renewal is determined by how the TLS certificate is originally obtained:

- If the API Gateway service obtains a TLS certificate for you, the API Gateway service automatically renews the TLS certificate with the Oracle-designated Certificate Authority before it expires.
- If you obtain a custom TLS certificate yourself, you are responsible for renewing the TLS certificate with your chosen Certificate Authority before it expires. Having received a new custom TLS certificate from the Certificate Authority, you create a new API Gateway certificate resource with the details of the new custom TLS certificate. You then update any API gateways that used the original API Gateway certificate resource to use the new certificate resource instead.

For some customers, use of custom domains and custom TLS certificates is obligatory. For example, if you are using Oracle Cloud Infrastructure Government Cloud, you are required to:

- only obtain a TLS certificate from a particular, approved Certificate Authority
- only use a particular, approved DNS provider

For other customers, use of custom domains is likely to be driven by commercial requirements. For example, typically you'll want to include your company name in the API gateway's domain name, rather than using the auto-generated random string of characters followed by `.apigateway.<region-identifier>.oci.customer-oci.co`. 
Note the following:

- You cannot delete an API Gateway certificate resource that is currently being used by an API gateway. To delete the API Gateway certificate resource, you must first remove it from any API gateway that is using it.
- You can only specify one API Gateway certificate resource for an API gateway.
- You cannot update an API Gateway certificate resource after you have created it.
- You can change the API Gateway certificate resource for an existing API gateway if you originally specified one when you first created the API gateway.

**Important:**
For public or production systems, Oracle recommends using custom TLS certificates. Oracle recommends only using TLS certificates obtained by the API Gateway service for private or non-production systems (for example, for development and testing).

**Setting up a Custom Domain Name and TLS Certificate for an API Gateway**

To set up a custom domain name and TLS certificate for an API gateway:

**Step 1: Obtain a TLS Certificate from your Chosen Certificate Authority**

The precise steps to obtain a TLS certificate will be different, according to the Certificate Authority you choose to use. At a high level, the steps will probably be somewhat similar to the following, but always refer to the Certificate Authority documentation for more detailed information:

1. Create a certificate signing request for your chosen Certificate Authority.
   Typically, you'll include information like the organization name, locality, and country in the certificate signing request.
   You'll also include a common name in the certificate signing request as the fully qualified domain name of the site you want to secure. The common name usually connects the TLS certificate with a particular domain. This domain name is used as the custom domain name for API gateways.
   When you create a certificate signing request, a public key is added to the request, and a corresponding private key is also generated and stored in a local file. You'll use this private key when you set up an API Gateway certificate resource, so make a note of its location. The private key you use to obtain a TLS certificate:
   - must be an RSA key
   - must be in PEM-encoded X.509 format
   - must start with -----BEGIN RSA PRIVATE KEY-----
   - must end with -----END RSA PRIVATE KEY-----
   - must not be protected by a passphrase
   - must have a minimum length of 2048 bits and must not exceed 4096 bits

2. Submit the certificate signing request to the Certificate Authority.
   The Certificate Authority returns:
   - a file containing the custom TLS certificate for the API gateway itself (known as the 'leaf certificate' or 'end-entity certificate')
   - typically one or more files containing intermediate certificates that form a certificate chain from the leaf certificate back to the Certificate Authority

You can now use these certificate files to create an API Gateway certificate resource.

**Step 2: Create an API Gateway Certificate Resource**

An API Gateway certificate resource is a named definition of a TLS certificate that you can use when creating or updating an API gateway using the API Gateway service.
An API Gateway certificate resource comprises:

- a name of your choice for the certificate resource itself
- the custom TLS certificate for the API gateway (the 'leaf certificate' or 'end-entity certificate') returned by the Certificate Authority
- any intermediate certificates forming a certificate chain from the leaf certificate back to the Certificate Authority
- the private key paired with the public key that was included in the original certificate signing request

Note that you cannot update an API Gateway certificate resource after you have created it.

You can create an API Gateway certificate resource using the Console or the CLI.

**Using the Console**

To create an API Gateway certificate resource using the Console:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **API Gateway**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Certificates** page, click **Add Certificate** and specify:
   - **Name**: The name of the new API Gateway certificate resource. Avoid entering confidential information.
   - **Certificate**: The custom TLS certificate returned by the Certificate Authority (the 'leaf certificate' or 'end-entity certificate'). Drag and drop, select, or paste a valid TLS certificate. Note that the TLS certificate you specify:
     - must be in PEM-encoded X.509 format
     - must start with `-----BEGIN CERTIFICATE-----`
     - must end with `-----END CERTIFICATE-----`
     - must not exceed 4096 bits in length
   - **Intermediate Certificates**: (Optional) If there is one or more intermediate certificates forming a certificate chain from the TLS certificate back to the Certificate Authority, include the contents of the intermediate certificate files in the correct order. The correct order begins with the certificate directly signed by the Trusted Root Certificate Authority at the bottom, with any additional certificate directly above the Certificate Authority that signed it. For example:

```
-----BEGIN CERTIFICATE-----
<PEM_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<PEM_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<PEM_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<PEM_encoded_certificate>
```

If you have concatenated the contents of intermediate certificate files into a single certificate chain file in the correct order, drag and drop that file, or select that file, or paste that file's content.

If you don't have a concatenated certificate chain file, paste the contents of the individual certificate files, in the correct order.

The combined length of any intermediate certificates you specify must not exceed 10240 bits.

- **Private Key:** The private key used to obtain the TLS certificate from the Certificate Authority. Drag and drop, select, or paste a valid private key in this field. Note that the key you specify:
  - must be an RSA key
  - must be in PEM-encoded X.509 format
  - must start with `-----BEGIN RSA PRIVATE KEY-----`
  - must end with `-----END RSA PRIVATE KEY-----`
  - must not be protected by a passphrase
  - must have a minimum length of 2048 bits and must not exceed 4096 bits

4. Click **Create** to create the API Gateway certificate resource.

**Using the CLI**

To create an API Gateway certificate resource using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).

2. Open a command prompt and run `oci api-gateway certificate create` to create the API Gateway certificate resource:

   ```bash
   oci api-gateway certificate create --display-name "<certificate-name>" --compartment-id <compartment-ocid> --certificate-file <certificate-file-path> --intermediate-certificates-file <intermediate-certificates-file-path> --private-key-file <private-key-file-path>
   ```

   where:
   - `<certificate-name>` is the name of the new API Gateway certificate resource. Avoid entering confidential information.
   - `<compartment-ocid>` is the OCID of the compartment to which the new API Gateway certificate resource will belong.
   - `<certificate-file-path>` is the path and name of the file containing the leaf certificate returned by the Certificate Authority. For example, `~/.certs/cert.pem`. Note that the leaf certificate in the file you specify:
     - must be in PEM-encoded X.509 format
     - must start with `-----BEGIN CERTIFICATE-----`
     - must end with `-----END CERTIFICATE-----`
     - must not exceed 4096 bits in length
   - `<intermediate-certificates-file-path>` is optionally the path and name of a file containing one or more intermediate certificates forming a certificate chain from the leaf certificate back to the Certificate Authority. For example, `~/.certs/int_cert.pem`. If the file contains multiple intermediate certificates, the intermediate certificates must be in the correct order. The correct order ends with the certificate directly signed by the Trusted Root Certificate Authority, with any additional certificate directly preceding the Certificate Authority that signed it. For example:

     ```
     -----BEGIN CERTIFICATE-----
     <PEM_encoded_certificate>-----
     END CERTIFICATE-------------BEGIN CERTIFICATE-----
     <PEM_encoded_certificate>-----END CERTIFICATE-------------BEGIN
     ```
The combined length of any intermediate certificates you specify must not exceed 10240 bits.

- `<private-key-file-path>` is the path and name of the file containing the private key used to obtain the TLS certificate from the Certificate Authority. For example, `~/.certs/key.pem`. Note that the private key in the file you specify:
  - must be an RSA key
  - must be in PEM-encoded X.509 format
  - must start with `-----BEGIN RSA PRIVATE KEY-----`
  - must end with `-----END RSA PRIVATE KEY-----`
  - must not be protected by a passphrase
  - must have a minimum length of 2048 bits and must not exceed 4096 bits

For example:

```bash
oci api-gateway certificate create --display-name "Acme gateway certificate" --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq --certificate-file ~/.certs/cert.pem --private-key-file ~/.certs/key.pem
```

The response to the command includes:

- The OCID of the new API Gateway certificate resource.
- The lifecycle state (for example, ACTIVE, FAILED).
- The id of the work request to create the API Gateway certificate resource (details of work requests are available for seven days after completion, cancellation, or failure).

If you want the command to wait to return control until the API Gateway certificate resource is active (or the request has failed), include either or both of the following parameters:

- `--wait-for-state ACTIVE`
- `--wait-for-state FAILED`

For example:

```bash
oci api-gateway certificate create --display-name "Acme gateway certificate" --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq --certificate-file ~/.certs/cert.pem --private-key-file ~/.certs/key.pem --wait-for-state ACTIVE
```

For more information about using the CLI, see [Command Line Interface (CLI)](https://docs.oracle.com/en-us/iaas/Content/API/Concepts/iaas-index.htm). For a complete list of flags and options available for CLI commands, see [Command Line Reference](https://docs.oracle.com/en-us/iaas/Content/API/Concepts/iaas-index.htm).

**Step 3: Specify the API Gateway certificate resource when creating an API gateway**

To specify the API Gateway certificate resource when creating an API gateway:

1. Follow the instructions in [Creating an API Gateway](https://docs.oracle.com/en-us/iaas/Content/API/Concepts/iaas-index.htm#Create) on page 355 to create an API gateway using either the Console or the CLI.
2. Specify the API Gateway certificate resource as described in the instructions:
   - If using the Console: Use the **Certificate** field.
   - If using the CLI: Set the `--certificate-id <certificate-ocid>` property.

   The API Gateway service creates the new API gateway, and installs the custom TLS certificate and private key.
3. Obtain the public IP address of the API gateway.
Step 4: Record the Mapping Between the API Gateway's Custom Domain Name and Public IP Address With Your Chosen DNS Provider

The precise steps to record the mapping between an API gateway's custom domain name and its public IP address depend on the DNS provider you choose to use. Typically, you will create a new record (specifically a new A record) in the DNS provider's configuration. The record associates the domain name you configured when requesting the TLS certificate from your chosen Certificate Authority with the public IP address that the API Gateway service assigns to the new API gateway. Refer to your chosen DNS provider's documentation for more detailed information.

Renewing Custom TLS Certificates Used by API Gateways

TLS certificates are valid for a limited period of time (typically one or two years) before they expire. If the TLS certificate used by an API gateway expires, calls to an API deployed on the API gateway return warning messages. To avoid warning messages, you have to renew TLS certificates before they expire (sometime referred to as 'rotating' certificates)

If the API Gateway service obtained the original TLS certificate for you, the API Gateway service automatically renews the TLS certificate with the Oracle-designated Certificate Authority before it expires. However, if you obtained a custom TLS certificate yourself, you are responsible for renewing the custom TLS certificate with your chosen Certificate Authority before it expires (although the Console does show a warning if the TLS certificate is due to expire shortly).

When you request the renewal of a TLS certificate, the Certificate Authority returns a completely new TLS certificate. You cannot simply update the existing API Gateway certificate resource with the new TLS certificate. Instead, you create a new API Gateway certificate resource, add the new TLS certificate to the new certificate resource, and then update any API gateways that used the previous certificate resource to use the new certificate resource.

To renew the custom TLS certificate used by an API gateway:

1. Submit a TLS certificate renewal request to the Certificate Authority from which you originally obtained the TLS certificate. The exact steps to renew a TLS certificate depend on the Certificate Authority you use, so always refer to the Certificate Authority documentation for more detailed information.

When you create the certificate renewal request, a public key is added to the request, and a corresponding private key is also generated and stored in a local file. You'll use this private key when you set up the new API Gateway certificate resource, so make a note of its location.

The Certificate Authority returns a file containing the new custom TLS certificate, and typically one or more files containing intermediate certificates forming a certificate chain from the TLS certificate back to the Certificate Authority.

2. Create a new API Gateway certificate resource and add to it the new TLS certificate, any intermediate certificates, and the new private key (see Step 2: Create an API Gateway Certificate Resource on page 372).

3. Update all the existing API gateways that used the original API Gateway certificate resource to use the new API Gateway certificate resource (see Updating API Gateways and API Deployments on page 387).

4. When there are no API gateways still using the original API Gateway certificate resource, delete the original certificate resource:
   - If using the Console: On the Certificates page, click the Actions icon (three dots) beside the original API Gateway certificate resource you want to delete, and then click Delete.
   - If using the CLI: Use the following command to delete the original API Gateway certificate resource:

   ```sql
   oci api-gateway certificate delete --certificate-id <certificate-ocid>
   ```

   Note that you cannot delete an API Gateway certificate resource if there are API gateways still using it.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use the:

- **CreateCertificate** operation to create a new API Gateway certificate resource
- **DeleteCertificate** operation to delete an existing API Gateway certificate resource
- **UpdateCertificate** operation to change the details of an existing API Gateway certificate resource
- **GetCertificate** operation to see details of an existing API Gateway certificate resource
- **ListCertificates** operation to list all the certificates in a compartment
- **ChangeCertificateCompartment** operation to change the compartment to which an existing API Gateway certificate resource belongs

### Adding Path Parameters and Wildcards to Route Paths

You might want different API requests routed to the same backend, even when the request URLs vary to a greater or lesser extent from the route path definition in the API deployment specification.

When defining a route path in an API deployment specification, you can include a path parameter to exactly replace an individual segment of the path. If necessary, you can include multiple path parameters in the route path. You can also append the asterisk (*) wildcard to a path parameter in the route path to provide even more flexibility when identifying requests to send to the same backend.

The examples in this topic assume you are adding route paths to an API deployment specification in a JSON file. Note the examples also apply when you're defining an API deployment specification using dialogs in the Console.

#### Example: Adding Path Parameters to Match Similar URLs

You might have a requirement to route requests with similar URLs to the same backend. For example:

- `https://<gateway-hostname>/marketing/hello/apac/index.html`
- `https://<gateway-hostname>/marketing/hello/emea/index.html`

To enable calls to these similar URLs to resolve to the same backend, add a path parameter name enclosed within curly brackets as the segment of the route path that will vary between API calls. For example, `{region}` as shown below:

```json
{
  "routes": [
    {
      "path": "/hello/{region}/index.html",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaabb_xmq"
      }
    }
  ]
}
```

Note that path parameter names:

- Can include alphanumeric uppercase and lowercase characters.
- Can include the underscore `_` special character.
- Cannot include other special characters. In particular, note that you cannot include spaces, forward slashes, and curly brackets in path parameter names.

#### Example: Adding Path Parameters with a Wildcard to Match Dissimilar URLs

You might have a requirement to route requests to the same backend, even though the request URLs are significantly different. For example:


```json
{
  "routes": [
    {
      "path": "/hello/*index.html",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaabb_xmq"
      }
    }
  ]
}
```
To enable calls to these significantly different URLs to resolve to the same backend:

- add a path parameter name enclosed within curly brackets as the first segment of the route path that will differ between the various API calls
- add the asterisk (*) wildcard to the end of the path parameter name

For example, \{generic_welcome\*\} as shown below:

```json
{
   "routes": [
      {
         "path": "/hello/{generic_welcome*}",
         "methods": ["GET"],
         "backend": {
            "type": "ORACLE_FUNCTIONS_BACKEND",
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
      }
   ]
}
```

Note that a path parameter name with an asterisk wildcard will match:

- no path segment
- a single path segment
- multiple path segments

### Adding Context Variables to Policies and HTTP Back End Definitions

Calls to APIs deployed on an API gateway typically include parameters that you’ll want to use when defining the following in API deployment specifications:

- request policies and response policies
- HTTP and HTTPS back ends

To enable you to use parameters included in API calls, the API Gateway service saves the values of the following types of parameter in temporary ‘context tables’:

- Path parameters you define in the API deployment specification (see Adding Path Parameters and Wildcards to Route Paths on page 377) are saved in records in the request.path table.
- Query parameters included in the call to the API are saved in records in the request.query table.
- Header parameters included in the call to the API are saved in records in the request.headers table.
- Authentication parameters returned by an authorizer function or contained in a JSON Web Token (JWT) are saved in records in the request.auth table (see Using Authorizer Functions to Add Authentication and Authorization to API Deployments on page 431 and Using JSON Web Tokens (JWTs) to Add Authentication and Authorization to API Deployments on page 440 respectively).

Each record in a context table is identified by a unique key.

When defining request and response policies, and HTTP and HTTPS back ends, you can reference the value of a parameter in a context table using a ‘context variable’. A context variable has the format `<context-table-name>[<key>]` where:

- `<context-table-name>` is one of request.path, request.query, request.headers, or request.auth
• `<key>` is one of:
  • a path parameter name defined in the API deployment specification
  • a query parameter name included in the request to the API
  • a header name included in the request to the API
  • an authentication parameter name returned by an authorizer function or contained in a JWT token

If you want to include the context variable within a string in the API deployment specification (for example, in the `url` property of an HTTP back end definition), use the format `${<context-table-name>[<key>]}`.

For example, the `request.path[region]` context variable in the example below returns the value of the record identified by the `region` key in the `request.path` context table.

```
{
  "routes": [
    {
      "path": "/weather/{region}"
      "methods": ["GET"],
      "backend": {
        "type": "HTTP_BACKEND",
        "url": "https://api.weather.gov/${request.path[region]}"
      }
    }
  ]
}
```

Note the following:

• A single record is created in the context table for each discrete parameter in an HTTP request. If the HTTP request includes two (or more) parameters of the same type and with the same name, the value of each parameter with that name is saved in the same record in the context table and identified by the same key. However, only the first value in the context table record can be substituted in place of a context variable. When adding a context variable for which multiple values can exist in the context table record and you want the first value in the context table record to be substituted in place of the context variable, add the context variable to the API deployment specification in the format `${<context-table-name>[<key>]}`

• If a parameter value includes special characters that have been encoded, the encoding is preserved when the value is saved in the context table. When the value is substituted for a context variable, the encoded value is substituted in place of the context variable. For example, if San José is included in a query parameter as `San+José`, the encoded version is what will be substituted in place of the context variable for that query parameter.

• If a context variable key does not exist in the specified context table, an empty string is substituted in place of the context variable.

• If a context variable key contains a dot, the dot is treated as any other character. It is not treated as an indicator of a parent-child relationship between the strings either side of it.

• If a path parameter includes a wildcard (for example, `generic_welcome*`), the path parameter without the wildcard is used as the key.

• You can include a context variable as a path segment in the `url` property of an HTTP back end definition, but not as a query parameter. For example:
  
  • You can use the `request.query[state]` context variable as a path segment in the `url` property, as shown in the following valid HTTP back end definition:

```
{
  "path": "/weather/{region}"
  "methods": ["GET"],
  "backend": {
    "type": "HTTP_BACKEND",
    "url": "https://api.weather.gov/${request.path[region]}/
    ${request.query[state]}"
  }
}
```
You cannot use the `request.query[state]` context variable as a query parameter in the URL property, as shown in the following invalid HTTP back end definition:

```
{
  "path": "/weather/{region}",
  "methods": ["GET"],
  "backend": {
    "type": "HTTP_BACKEND",
    "url": "https://api.weather.gov/${request.path[region]}?state=${request.query[state]}"
  }
}
```

**Examples**

The examples in this section assume the following API deployment definition and basic API deployment specification in a JSON file:

```
{
  "displayName": "Marketing Deployment",
  "gatewayId": "ocid1.apigateway.oc1..aaaaaaaab______hga",
  "compartmentId": "ocid1.compartment.oc1..aaaaaaa7______ysq",
  "pathPrefix": "/marketing",
  "specification": {
    "routes": [
      {
        "path": "/weather",
        "methods": ["GET"],
        "backend": {
          "type": "HTTP_BACKEND",
          "url": "https://api.weather.gov"
        }
      }
    ],
    "freeformTags": {},
    "definedTags": {}
  }
}
```

Note the examples also apply when you're defining an API deployment specification using dialogs in the Console.

**Example 1: Query path parameter in a definition**

You can define a path parameter in the API deployment specification, and then use it elsewhere in the API deployment specification as a context variable.

This example creates a path parameter, `region`, and uses it in a context variable `request.path[region]` in the HTTP back end definition.

```
{
  "path": "/weather/{region}",
  "methods": ["GET"],
  "backend": {
    "type": "HTTP_BACKEND",
    "url": "https://api.weather.gov/${request.path[region]}"
  }
}
```
In this example, a request like \texttt{https://<gateway-hostname>/marketing/weather/west} resolves to \texttt{https://api.weather.gov/west}.

**Example 2: Different types of context variable in the same definition**

You can include different types of context variable in the same definition in the API deployment specification.

This example uses the following in the HTTP back end definition:

- a path parameter context variable, \texttt{request.path[region]}
- a query parameter context variable, \texttt{request.query[state]}

```json
{
  "path": "/weather/{region}",
  "methods": ["GET"],
  "backend": {
    "type": "HTTP_BACKEND",
    "url": "https://api.weather.gov/${request.path[region]}/
             ${request.query[state]}"
  }
}
```

In this example, a request like \texttt{https://<gateway-hostname>/marketing/weather/west?state=california} resolves to \texttt{https://api.weather.gov/west/california}.

**Example 3: Multiple context variables of the same type in the same definition**

You can include the same type of context variable multiple times in the same definition.

This example uses the following in the HTTP back end definition:

- a path parameter context variable, \texttt{request.path[region]}
- two query parameter context variables, \texttt{request.query[state]} and \texttt{request.query[city]}

```json
{
  "path": "/weather/{region}",
  "methods": ["GET"],
  "backend": {
    "type": "HTTP_BACKEND",
    "url": "https://api.weather.gov/${request.path[region]}/
             ${request.query[state]}/${request.query[city]}"
  }
}
```

In this example, a request like \texttt{https://<gateway-hostname>/marketing/weather/west?state=california&city=fremont} resolves to \texttt{https://api.weather.gov/west/california/fremont}.

**Example 4: Multiple values for the same parameter**

It is often valid for an HTTP request to include the same query parameter multiple times. The API Gateway service saves the value of each parameter with the same name to the same record in the context table. However, in the API deployment specification, it’s typically the case that only a single value can be substituted for a context variable. In these situations, you can indicate that only the first value recorded in the context table for a key is substituted in place of a context variable by enclosing the context variable within \texttt{{...}}.

For example, a valid request like \texttt{https://<gateway-hostname>/marketing/weather/west?state=california&city=fremont&city=belmont} has two occurrences of the \texttt{city} query parameter. On receipt of the HTTP request, the API Gateway service writes both values of the \texttt{city} query parameter \texttt{(fremont and belmont)} to the same record in the \texttt{request.query} table. When the definition of an HTTP back
end includes \${request.query[city]}, only the first value in the record is substituted in place of the context variable.

This example uses the following in the HTTP back end definition:

- a path parameter context variable, request.path[region]
- two query parameter context variables, request.query[state] and request.query[city]

```json
{
    "path": "/weather/{region}",
    "methods": ["GET"],
    "backend": {
        "type": "HTTP_BACKEND",
        "url": "https://api.weather.gov/${request.path[region]}/\${request.query[state]}/${request.query[city]}"
    }
}
```

In this example, a request like https://<gateway-hostname>/marketing/weather/west?state=california&city=fremont&city=belmont resolves to https://api.weather.gov/west/california/fremont. Note that only fremont (as the first value in the request.query context table record identified by the city key) is substituted for the request.query[city] context variable.

**Example 5: Parameter value includes encoded special characters**

If an HTTP request includes special characters (for example, the character é, the space character) that have been encoded, the value is stored in the context table in its encoded form. When the value from the context table is substituted for a context variable, the encoding is preserved.

This example uses the following in the HTTP back end definition:

- a path parameter context variable, request.path[region]
- a query parameter context variable, request.query[city]

```json
{
    "path": "/weather/{region}",
    "methods": ["GET"],
    "backend": {
        "type": "HTTP_BACKEND",
        "url": "https://api.weather.gov/${request.path[region]}/\${request.query[state]}/${request.query[city]}"
    }
}
```

In this example, a request like https://<gateway-hostname>/marketing/weather/west?city=San+José resolves to https://api.weather.gov/west/california/San+José.

**Example 6: Header parameters in a definition**

You can include values passed in the headers of a request as context variables in a definition. If the request includes a header, the value of the header is stored in the request.headers table, and the name of the header is used as the key.

This example uses the following in the HTTP back end definition:

- a path parameter context variable, request.path[region]
- a header parameter context variable, request.headers[X-Api-Key]

```json
{
    "path": "/weather/{region}",
    "methods": ["GET"],
    "backend": {
```
In this example, a request like `https://<gateway-hostname>/marketing/weather/west` included an `X-Api-Key` header with the value `abc123def456fhi789`. The request resolves to `https://api.weather.gov/west/abc123def456fhi789`.

**Example 7: Authentication parameters in a definition**

You can include values returned from an authorizer function or contained in a JWT token as context variables in a definition:

- An authorizer function validates the token passed by an API client when calling the API Gateway service. The authorizer function returns a response that includes information such as the validity of the authorization, information about the end user, access scope, and a number of claims in key-value pairs. Depending on the authorization token, the information might be contained within the token, or the authorizer function might invoke end-points provided by the authorization server to validate the token and to retrieve information about the end user. When the API Gateway service receives a key-value pair from the authorizer function, it saves the key-value pair in the `request.auth` table as an authentication parameter.

- A JWT token can optionally include a custom claim named `scope`, comprising a key-value pair. When the JWT token has been validated, the API Gateway service saves the key-value pair in the `request.auth` table as an authentication parameter.

This example uses the key-value pair returned by an authorizer function as the authentication parameter context variable `request.auth[region]` in the HTTP back end definition.

Assume an authorizer function `ocid1.fnfunc.oc1.phx.aaaaaaaaac2______kg6fq` validates the token passed by an API client in a call to the API Gateway service. The authorizer function returns a response to the API Gateway service that includes the region associated with the end user as a key-value pair, and also the authenticated end user's access scope. When the API Gateway service receives the key-value pair, it saves the key-value pair in the `request.auth` table as an authentication parameter.
In this example, a request like https://<gateway-hostname>/marketing/weather is made by an end user jdoe using an API client. The authorizer function validates the token passed by the API client in the request, and also determines that jdoe has the "weatherwatcher" access scope. The authorizer function identifies that jdoe is associated with the west region. The authorizer function returns jdoe's access scope to the API Gateway service, along with the region associated with jdoe. The API Gateway service saves the region associated with jdoe as an authentication parameter. The HTTP back end definition specifies that end users with the "weatherwatcher" access scope are allowed to access the HTTP back end. The API Gateway service uses the value of the authentication parameter context variable `request.auth[region]` in the request. The request resolves to https://api.weather.gov/west.

**Calling an API Deployed on an API Gateway**

Having deployed an API on an API gateway, you can call the deployed API.

**Tip:**

When assembling the curl command described in this topic, you can quickly get the value of the `https://<gateway-hostname>/<deployment-path-prefix>` string as the API deployment's endpoint using:

- The Console, by going to the **Gateway Details** page and clicking **Copy** beside the endpoint of the API deployment.
- The API, by using the **GetDeployments** operation.
Using curl

To call an API deployed on an API gateway:

1. Open a terminal window and type a cURL command similar to the following that is appropriate for the deployed API:

```
curl -k -X <method> https://<gateway-hostname>/<deployment-path-prefix>/<api-route-path>
```

where:

- `<method>` is a valid method for the deployed API (for example, GET, PUT).
- `<gateway-hostname>` is an automatically generated domain name in the format `<gateway-identifier>.apigateway.<region-identifier>.oci.customer-oci.com`, where:
  - `<gateway-identifier>` is the string of characters that identifies the API gateway. For example, lak...sjd (abbreviated for readability).
  - `<region-identifier>` is the identifier of the region in which the API gateway has been created. See Availability by Region on page 338.

For example, lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com.

Use the Console or the API to find out the domain name to use as the value of `<gateway-hostname>`.

- `<deployment-path-prefix>` is the prefix added to the path of every route in the API deployment. Note that the deployment path prefix in the request:
  - can contain multiple forward slashes (provided they are not adjacent)
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - cannot include parameters and wildcards
  - must match exactly the deployment path prefix defined for the API deployment (see Deploying an API on an API Gateway by Creating an API Deployment on page 363)

Use the Console or the API to find out the path prefix to use as the value of `<deployment-path-prefix>`.

- `<api-route-path>` is the path to a particular route defined in the API deployment specification. Note that the route path in the request:
  - is relative to the deployment path prefix
  - can be a single forward slash
  - can include multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - need not match exactly the route path defined in the API deployment specification, provided the route path in the API deployment specification includes a path parameter with or without a wildcard (see Adding Path Parameters and Wildcards to Route Paths on page 377)

Use the Console or the API to find out the path to use as the value of `<api-route-path>`.

For example:

```
curl -k -X GET https://lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com/marketing/hello/
```

If the API gateway back end is a serverless function that accepts parameters, include those parameters in the call to the API. For example:

```
curl -k -X POST https://lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com/marketing/hello/ -d "name=John"
```
Listing API Gateways and API Deployments

Having created API gateways, and deployed APIs on API gateways by creating API deployments, you might need to list the existing API gateways or API deployments. For example, you might want to see whether there are any API gateways that are no longer required, quickly locate an API gateway by its OCID, or obtain the OCID of an API deployment.

Using the Console

To list API gateways or API deployments using the Console:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click API Gateway.
2. Choose a Compartment you have permission to work in.
3. To see a list of all existing API gateways in the current region and compartment (including their OCIDs), use the Gateways page.
4. To see more detail about an individual API gateway, click the name of the API gateway on the Gateways page to show the Gateway Details page.
5. To see a list of API deployments on an API gateway (including their endpoint, state, and OCID), click the name of the API gateway on the Gateways page and select Deployments from the Resources list.

Using the CLI

To list the API gateways and API deployments in a compartment using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).
2. To list all the API gateways in a compartment, open a command prompt and run oci api-gateway gateway list to list the API gateways:

   `oci api-gateway gateway list --compartment-id <compartment-ocid>

where:

- `<compartment-ocid>` is the OCID of the compartment containing the API gateway.

For example:

   `oci api-gateway gateway list --compartment-id ocid1.compartment.oc1..aaaaaaaa7_____ysq`

If you want to list just those API gateways with a status of Active, include the --lifecycle-state ACTIVE parameter in the request. For example:

   `oci api-gateway gateway list --compartment-id ocid1.compartment.oc1..aaaaaaaa7_____ysq --lifecycle-state ACTIVE`
To list all the API deployments in a compartment, open a command prompt and run `oci api-gateway deployment list` to list the API deployments:

```
oci api-gateway deployment list --compartment-id <compartment-ocid>
```

where:

- `<compartment-ocid>` is the OCID of the compartment containing the API deployments.

For example:

```
oci api-gateway deployment list --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq
```

If you want to list just those API deployments with a status of Active, include the `--lifecycle-state ACTIVE` parameter in the request. For example:

```
oci api-gateway deployment list --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq --lifecycle-state ACTIVE
```

If you want to list all the API deployments on a particular API gateway in a compartment, include the `--gateway-id` parameter in the request and specify the API gateway's OCID. For example:

```
oci api-gateway deployment list --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq --gateway-id ocid1.apigateway.oc1..aaaaaaaab______hga
```

For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the:

- `ListGateways` operation to list API gateways
- `ListDeployments` operation to list API deployments

**Updating API Gateways and API Deployments**

Having created an API gateway, and deployed an API on the API gateway by creating an API deployment, you might decide to change either or both. For example, to change the API gateway's name or the tags applied to it, or to change an API deployment specification to add additional back ends to the API deployment.

Note that there are some properties of API gateways and API deployments for which you cannot change the original values.

You can update API gateways and API deployments using the Console, the CLI, and the API.

You can update an API deployment specification by:

- using dialogs in the Console
- editing a JSON file

**Using the Console**

To update an existing API gateway or an API deployment using the Console:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click API Gateway.
2. Choose a **Compartment** you have permission to work in.

3. On the **Gateways** page, click the name of the API gateway that you want to update (or that contains the API deployment you want to update) to show the **Gateway Details** page.

4. To update an API gateway:
   - Click **Edit** to change the API gateway's name. If you have set up a custom TLS certificate (and associated custom domain name), you can also change the API Gateway certificate resource used by the API gateway (see Setting Up Custom Domains and TLS Certificates on page 371). Avoid entering confidential information.
   - Click **Move Resource** to move the API gateway to a different compartment.
   - Click **Add Tag(s)** and **View Tag(s)** to change and view the tags applied to the API gateway.

5. To update an API deployment, on the **Gateway Details** page, select **Deployments** from the **Resources** list and click the Actions icon (three dots) beside the API deployment you want to update:
   - Click **Edit** to change the API deployment's name, or to replace the original API deployment specification. You can change the original API deployment specification by selecting one of two options:
     - **From Scratch**: Select to change API deployment specification properties using dialogs in the Console.
     - **Upload an existing API**: Select to change API deployment specification properties by uploading a replacement JSON file.
   - Click **Move Resource** to move the API deployment to a different compartment.
   - Click **Add Tag(s)** and **View Tag(s)** to change and view the tags applied to the API deployment.

**Using the CLI**

To update existing API gateways and API deployments using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).

2. To update an existing API gateway:
   - Open a command prompt and run `oci api-gateway gateway update` to update the API gateway:
     ```
     oci api-gateway gateway update --gateway-id <gateway-ocid> --<property-to-update> <property-value>
     ```
     where:
     - `<gateway-ocid>` is the OCID of the API gateway to update. To find out the API gateway's OCID, see Listing API Gateways and API Deployments on page 386.
     - `<property-to-update>` is the property to update. Note that you can only change the values for **display-name**, **freeform-tags** and **defined-tags** (and **certificate-id** if this was
originally set for the API gateway). All other values must be identical to values in the original gateway definition.

- `<property-value>` is the new value of the property you want to change.

For example:

```bash
oci api-gateway gateway update --gateway-id ocid1.apigateway.oc1..aaaaaaab______hga --display-name "Hello World Gateway - version 2"
```

The response to the command includes:

- The lifecycle state (for example, ACTIVE, FAILED).
- The id of the work request to update the API gateway (details of work requests are available for seven days after completion, cancellation, or failure).

If you want the command to wait to return control until the API gateway is active (or the request has failed), include either or both the following parameters:

- `--wait-for-state ACTIVE`
- `--wait-for-state FAILED`

For example:

```bash
oci api-gateway gateway update --gateway-id ocid1.apigateway.oc1..aaaaaaab______hga --display-name "Hello World Gateway - version 2" --wait-for-state ACTIVE
```

b. (Optional) To see the status of the work request that is updating the API gateway, enter:

```bash
oci api-gateway work-request get --work-request-id <work-request-ocid>
```

c. (Optional) To view the logs of the work request that is updating the API gateway, enter:

```bash
oci api-gateway work-request-log list --work-request-id <work-request-ocid>
```

d. (Optional) If the work request that is updating the API gateway fails and you want to review the error logs, enter:

```bash
oci api-gateway work-request-error --work-request-id <work-request-ocid>
```

e. (Optional) To verify that the API gateway has been updated, enter the following command and confirm that the API gateway's properties are as you expect:

```bash
oci api-gateway gateway get --gateway-id <gateway-ocid>
```

3. To update an existing API deployment:

a. Open a command prompt and run `oci api-gateway deployment update` to update the API deployment:

```bash
oci api-gateway deployment update --deployment-id <deployment-ocid> --specification file:///<filename>
```

where:

- `<deployment-ocid>` is the OCID of the API deployment to update. To find out the API deployment's OCID, see Listing API Gateways and API Deployments on page 386.
- `<filename>` is the relative location and filename of the JSON file containing the replacement API deployment specification. For example, `replacement-specification.json`. For more
information about defining API deployment specifications, see Creating an API Deployment Specification on page 361.

For example:

```mermaid
circle: oci api-gateway deployment update --deployment-id ocid1.apideployment.oc1..aaaaaaaaab______pwa --specification file:///Users/jdoe/work/replacement-specification.json
```

The response to the command includes:

- The lifecycle state (for example, ACTIVE, FAILED).
- The id of the work request to update the API deployment (details of work requests are available for seven days after completion, cancellation, or failure).

If you want the command to wait to return control until the API deployment is active (or the request has failed), include either or both the following parameters:

- `--wait-for-state ACTIVE`
- `--wait-for-state FAILED`

For example:

```mermaid
circle: oci api-gateway deployment update --deployment-id ocid1.apideployment.oc1..aaaaaaaaab______pwa --specification file:///Users/jdoe/work/replacement-specification.json --wait-for-state ACTIVE
```

b. (Optional) To see the status of the work request that is updating the API deployment, enter:

```mermaid
circle: oci api-gateway work-request get --work-request-id <work-request-ocid>
```

c. (Optional) To view the logs of the work request that is updating the API deployment, enter:

```mermaid
circle: oci api-gateway work-request-log list --work-request-id <work-request-ocid>
```

d. (Optional) If the work request that is updating the API deployment fails and you want to review the error logs, enter:

```mermaid
circle: oci api-gateway work-request-error --work-request-id <work-request-ocid>
```

e. (Optional) To verify that the API deployment has been updated, enter the following command and confirm that the API deployment's properties are as you expect:

```mermaid
circle: oci api-gateway deployment get --deployment-id <deployment-ocid>
```

For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the:

- `UpdateGateway` operation to update an API gateway
- `UpdateDeployment` operation to update an API deployment
Moving API Gateways and API Deployments Between Compartments

Having created an API gateway, and deployed an API on the API gateway by creating an API deployment, you might decide to move either or both from one compartment to another. An API gateway and the individual API deployments deployed on it can be in different compartments.

Note that calls to an API deployment will be disrupted while the API deployment (or the API gateway on which it is deployed) is being moved to a different compartment. Do not call the API deployment until the move operation is complete.

Using the Console

To move an API gateway or an API deployment to a different compartment using the Console:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click API Gateway.
2. Choose a Compartment you have permission to work in.
3. On the Gateways page, click the name of the API gateway that you want to move (or that contains the API deployment you want to move) to show the Gateway Details page.
4. On the Gateway Details page:
   - To move the API gateway, click Move Resource, select the compartment to which you want to move the API gateway, and click Move Resource to start the process of moving the API gateway. Note that API deployments on the API gateway are not moved to the new compartment.
   - To move an API deployment, select Deployments from the Resources list, click Move Resource, select the compartment to which you want to move the API deployment, and click Move Resource to start the process of moving the API deployment.

Do not call an API deployment while the API deployment (or the API gateway on which it is deployed) is in the process of being moved to the new compartment.

5. On the Gateway Details page, select Work Requests from the Resources list and confirm the move operation is complete.

   When the move operation is complete, resume calls to the API deployment.

Using the CLI

To move API gateways and API deployments to a different compartment using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).
2. To move an API gateway to a different compartment:
   a. Open a command prompt and run `oci api-gateway gateway change-compartment` to move the API gateway:

   ```
   oci api-gateway gateway change-compartment --gateway-id <gateway-ocid>
   --compartment-id <compartment-ocid>
   ```

   where:
   - `<gateway-ocid>` is the OCID of the API gateway to move. To find out the API gateway's OCID, see [Listing API Gateways and API Deployments](page 386) on page 386.
   - `<compartment-ocid>` is the OCID of the compartment to which to move the API gateway.

   For example:

   ```
   oci api-gateway gateway change-compartment --gateway-id ocid1.apigateway.oc1..aaaaaaaab______hga
   --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq
   ```

   Note that API deployments on the API gateway are not moved.

   The response to the command includes:
   - The lifecycle state (for example, ACTIVE, FAILED).
   - The id of the work request to move the API gateway (details of work requests are available for seven days after completion, cancellation, or failure).

   If you want the command to wait to return control until the API gateway is active (or the request has failed), include either or both the following parameters:
   - `--wait-for-state ACTIVE`
   - `--wait-for-state FAILED`

   For example:

   ```
   oci api-gateway gateway change-compartment --gateway-id
   ocid1.apigateway.oc1..aaaaaaaab______hga
   --compartment-id
   ocid1.compartment.oc1..aaaaaaaa7______ysq
   --wait-for-state ACTIVE
   ```

   b. (Optional) To see the status of the work request that is moving the API gateway, enter:

   ```
   oci api-gateway work-request get --work-request-id <work-request-ocid>
   ```

c. (Optional) To view the logs of the work request that is moving the API gateway, enter:

   ```
   oci api-gateway work-request-log list --work-request-id <work-request-ocid>
   ```

d. (Optional) If the work request that is moving the API gateway fails and you want to review the error logs, enter:

   ```
   oci api-gateway work-request-error --work-request-id <work-request-ocid>
   ```

e. (Optional) To verify that the API gateway has been moved, enter the following command and confirm that the API gateway's new compartment OCID is as you expect:

   ```
   oci api-gateway gateway get --gateway-id <gateway-ocid>
   ```
3. To move an API deployment to a different compartment:
   
   a. Open a command prompt and run `oci api-gateway deployment change-compartment` to move the API deployment:

   ```
   oci api-gateway deployment change-compartment --deployment-id <deployment-ocid> --compartment-id <compartment-ocid>
   ```

   where:
   
   - `<deployment-ocid>` is the OCID of the API deployment to move. To find out the API deployment's OCID, see Listing API Gateways and API Deployments on page 386.
   - `<compartment-ocid>` is the OCID of the compartment to which to move the API deployment.

   For example:

   ```
   oci api-gateway deployment change-compartment --deployment-id ocid1.apideployment.oc1..aaaaaaaaab_____pwa --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq
   ```

   The response to the command includes:

   - The lifecycle state (for example, ACTIVE, FAILED).
   - The id of the work request to move the API deployment (details of work requests are available for seven days after completion, cancellation, or failure).

   If you want the command to wait to return control until the API deployment is active (or the request has failed), include either or both the following parameters:

   - `--wait-for-state ACTIVE`
   - `--wait-for-state FAILED`

   For example:

   ```
   oci api-gateway deployment change-compartment --deployment-id ocid1.apideployment.oc1..aaaaaaaaab_____pwa --compartment-id ocid1.compartment.oc1..aaaaaaaa7______ysq --wait-for-state ACTIVE
   ```

   b. (Optional) To see the status of the work request that is moving the API deployment, enter:

   ```
   oci api-gateway work-request get --work-request-id <work-request-ocid>
   ```

   c. (Optional) To view the logs of the work request that is moving the API deployment, enter:

   ```
   oci api-gateway work-request-log list --work-request-id <work-request-ocid>
   ```

   d. (Optional) If the work request that is moving the API deployment fails and you want to review the error logs, enter:

   ```
   oci api-gateway work-request-error --work-request-id <work-request-ocid>
   ```

   e. (Optional) To verify that the API deployment has been moved, enter the following command and confirm that the API deployment's new compartment OCID is as you expect:

   ```
   oci api-gateway deployment get --deployment-id <deployment-ocid>
   ```

   For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the:

• ChangeGatewayCompartment operation to move an API gateway to a different compartment.
• ChangeDeploymentCompartment operation to move an API deployment to a different compartment.

Deleting API Gateways and API Deployments

Having created an API gateway, and deployed an API on the API gateway by creating an API deployment, you might decide that either or both are no longer required.

You can delete an API gateway from the API Gateway service, provided there are no API deployments on it.

You can delete individual API deployments on an API gateway, one at a time. Note that when you delete an API deployment, its API deployment specification is permanently removed.

Note that deleted API gateways and API deployments continue to be shown in the Console for 90 days, with a status of Deleted. After 90 days, deleted API gateways and API deployments are no longer shown.

Using the Console

To delete an API gateway or an API deployment using the Console:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click API Gateway.
2. Choose a Compartment you have permission to work in.
3. On the Gateways page, click the name of the API gateway that you want to delete (or that contains the API deployment you want to delete) to show the Gateway Details page.
4. On the Gateway Details page:
   • To delete the API gateway, click Delete below the API gateway's name. The API gateway is permanently removed. Note that you cannot delete an API gateway if it still has API deployments on it. You must delete the API deployments first.
   • To delete an API deployment, select Deployments from the Resources list, click the Actions icon (three dots) beside the API deployment you want to delete, and select Delete. The API deployment and its API deployment specification are permanently removed.

Using the CLI

To delete API gateways and API deployments using the CLI:

1. Configure your client environment to use the CLI (Configuring Your Client Environment to use the CLI for API Gateway Development on page 355).
2. To delete an existing API gateway:
   a. Open a command prompt and run `oci api-gateway gateway delete` to delete the API gateway:

   ```bash
   oci api-gateway gateway delete --gateway-id <gateway-ocid>
   ```

   where:
   - `<gateway-ocid>` is the OCID of the API gateway to delete. To find out the API gateway's OCID, see `Listing API Gateways and API Deployments` on page 386.

   For example:

   ```bash
   oci api-gateway gateway delete --gateway-id ocid1.apigateway.oc1..aaaaaaab______hga
   ```

   Note that you cannot delete an API gateway if it still has API deployments on it (including API deployments that are in different compartments to the API gateway itself). You must delete the API deployments first.

   The response to the command includes:
   - The lifecycle state (for example, DELETED, FAILED).
   - The id of the work request to delete the API gateway (details of work requests are available for seven days after completion, cancellation, or failure).

   If you want the command to wait to return control until the API gateway has been deleted (or the request has failed), include either or both the following parameters:
   - `--wait-for-state DELETED`
   - `--wait-for-state FAILED`

   For example:

   ```bash
   oci api-gateway gateway delete --gateway-id ocid1.apigateway.oc1..aaaaaaab______hga --wait-for-state DELETED
   ```

   b. (Optional) To see the status of the work request that is deleting the API gateway, enter:

   ```bash
   oci api-gateway work-request get --work-request-id <work-request-ocid>
   ```

c. (Optional) To view the logs of the work request that is deleting the API gateway, enter:

   ```bash
   oci api-gateway work-request-log list --work-request-id <work-request-ocid>
   ```

d. (Optional) If the work request that is deleting the API gateway fails and you want to review the error logs, enter:

   ```bash
   oci api-gateway work-request-error --work-request-id <work-request-ocid>
   ```

e. (Optional) To verify that the API gateway has been deleted, enter the following command and confirm that the API gateway's lifecycle state is DELETED:

   ```bash
   oci api-gateway gateway get --gateway-id <gateway-ocid>
   ```
3. To delete an existing API deployment:

a. Open a command prompt and run `oci api-gateway deployment delete` to delete the API deployment:

```
oci api-gateway deployment delete --deployment-id <deployment-ocid>
```

where:

- `<deployment-ocid>` is the OCID of the API deployment to delete. To find out the API deployment's OCID, see Listing API Gateways and API Deployments on page 386.

For example:

```
oci api-gateway deployment delete --deployment-id ocid1.apideployment.oc1..aaaaaaaaab______pwa
```

The response to the command includes:

- The lifecycle state (for example, ACTIVE, DELETED).
- The id of the work request to delete the API deployment (details of work requests are available for seven days after completion, cancellation, or failure).

If you want the command to wait to return control until the API deployment is active (or the request has failed), include either or both of the following parameters:

- `--wait-for-state DELETED`
- `--wait-for-state FAILED`

For example:

```
oci api-gateway deployment delete --deployment-id ocid1.apideployment.oc1..aaaaaaaaab______pwa --wait-for-state DELETED
```

b. (Optional) To see the status of the work request that is deleting the API deployment, enter:

```
oci api-gateway work-request get --work-request-id <work-request-ocid>
```

c. (Optional) To view the logs of the work request that is deleting the API deployment, enter:

```
oci api-gateway work-request-log list --work-request-id <work-request-ocid>
```

d. (Optional) If the work request that is deleting the API deployment fails and you want to review the error logs, enter:

```
oci api-gateway work-request-error --work-request-id <work-request-ocid>
```

e. (Optional) To verify that the API deployment has been deleted, enter the following command and confirm that the API deployment’s lifecycle state is DELETED:

```
oci api-gateway deployment get --deployment-id <deployment-ocid>
```

For more information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225. Use the:
Adding Logging to API Deployments

Having created an API gateway and deployed one or more APIs on it, there will likely be occasions when you'll need to see more detail about the flow of traffic into and out of the API gateway. For example, you might want to review responses returned to API clients, or to troubleshoot errors. You can specify that the API Gateway service stores information about requests and responses going through an API gateway, and information about processing within an API gateway, as logs in the Oracle Cloud Infrastructure Logging service.

You can define and store two kinds of logs for API deployments in the Oracle Cloud Infrastructure Logging service:

- Access logs, that record a summary of every request and response that goes through the API gateway to and from an API deployment. For more information about access log content, see API Deployment Access Log on page 2597.
- Execution logs, that record information about processing within the API gateway for an API deployment. For more information about execution log content, see API Deployment Execution Log on page 2598. You can specify a log level for execution logs as one of the following:
  - Information, to record a summary of every processing stage.
  - Warning, to record only transient errors that occur during processing. For example, a connection reset.
  - Error, to record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

You can set an execution log level for an API deployment, and also set different execution log levels for individual routes to override the execution log level inherited from the API deployment.

Note:

In earlier API Gateway releases (prior to the release of the Oracle Cloud Infrastructure Logging service), you could direct API Gateway to store access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage. This functionality is still available for any API deployments you created in earlier releases where you previously specified a logging policy.

You can set up a logging policy in the API deployment specification for all routes in the API deployment specification, and optionally also set up different logging policies for individual routes to override the policy set at the API deployment level. Each log object contains the log messages output in a ten minute logging window. Log objects are available in Object Storage approximately ten minutes after the end of the logging window.

However, note the following:

- If you set up Oracle Cloud Infrastructure Logging to store logs for an API deployment, you are no longer able to store logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage for that API deployment.
- The ability to store access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage will be deprecated in a future release.
- To store access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage, you have to define the logging policy in a JSON file. You cannot use the Console to store access logs and execution logs in Oracle Cloud Infrastructure Object Storage.

You can add logging to an API deployment specification by:

- using the Console
using a JSON file

Using the Console to Add Logging

Using the Console to Configure and Enable Logs in Oracle Cloud Infrastructure Logging

To configure and enable API deployment logs using the Console to store logs in Oracle Cloud Infrastructure Logging:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. In the API Logging Policies section of the Basic Information page, specify one of the following options as the Execution Log Level to record information about processing within the API gateway:

   • Information: Record a summary of every processing stage. This is the default option.
   • Warning: Record only transient errors that occur during processing. For example, a connection reset.
   • Error: Record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

3. Click Next to enter details for individual routes in the API deployment on the Routes page and click Show Route Logging Policies.

4. Specify one of the following options as the Execution Log Level Override that applies to an individual route (to override the execution log level inherited from the API deployment):

   • Information: Record a summary of every processing stage.
   • Warning: Record only transient errors that occur during processing. For example, a connection reset.
   • Error: Record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

5. Click Next to review the details you entered for the API deployment.

6. Click Create or Save Changes to create or update the API deployment.

   The API deployment is shown on the API Deployment Details page.

7. Under Resources, click Logs, and then click the Enable Logging slider to create and enable a new API deployment log in the Oracle Cloud Infrastructure Logging service in the Create Log entry panel:

   • Compartment: By default, the current compartment.
   • Log Group: By default, the first log group in the compartment.
   • Log Category: Select either Execution or Access.
   • Log Name: By default, <deployment-name>_execution or <deployment-name>_access, depending on which category you select.

   For more information, see Enabling Logging for a Resource on page 2591.

8. Click Enable Log to create the new log and enable it.

Editing a JSON File to Add Logging

Editing a JSON File to Set Execution Log Level for Logs Stored in Oracle Cloud Infrastructure Logging

To edit the API deployment specification in a JSON file to set the log level for execution logs stored in Oracle Cloud Infrastructure Logging:
1. Using your preferred JSON editor, edit the existing API deployment specification in which you want to set the log level for execution logs stored in Oracle Cloud Infrastructure Logging, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

At a minimum, the API deployment specification will include a `routes` section containing:

- A path. For example, `/hello`
- One or more methods. For example, `GET`
- A definition of a back end. For example, a URL, or the OCID of a function in Oracle Functions.

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        }
    ]
}
```

2. (Optional) To set the log level for execution logs that applies globally to all routes in the API deployment specification:

   a. Insert a `loggingPolicies` section before the `routes` section. For example:

   ```json
   {
       "loggingPolicies": {},
       "routes": [
           {
               "path": "/hello",
               "methods": ["GET"],
               "backend": {
                   "type": "ORACLE_FUNCTIONS_BACKEND",
                   "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
               }
           }
       ]
   }
   ```

   b. Specify the level of detail to record about processing within the API gateway for all routes by including the `executionLog` policy in the `loggingPolicies` section, and setting the `logLevel` property to one of the following:

   - `INFO` to record a summary of every processing stage.
   - `WARN` to record only transient errors that occur during processing. For example, a connection reset.
   - `ERROR` to record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

   For example:

   ```json
   {
       "loggingPolicies": {
           "executionLog": {
               "logLevel": "INFO"
           }
       }
   }
   ```
3. (Optional) To set the log level for execution logs for a particular route (overriding the global execution log level inherited from the API deployment):

a. Insert a `loggingPolicies` section after the route's `backend` section. For example:

```json
{
  "loggingPolicies": {
    "executionLog": {
      "logLevel": "INFO"
    }
  },
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "loggingPolicies": {}
    }
  ]
}
```

b. Specify the level of detail to record about processing within the API gateway for the route by including the `executionLog` policy in the `loggingPolicies` section, and setting the `logLevel` property to one of the following:

- `INFO` to record a summary of every processing stage.
- `WARN` to record only transient errors that occur during processing. For example, a connection reset.
- `ERROR` to record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

For example:

```json
{
  "loggingPolicies": {
    "executionLog": {
      "logLevel": "INFO"
    }
  },
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "loggingPolicies": {}
    }
  ]
}
```
4. Save the JSON file containing the API deployment specification.

5. Use the API deployment specification when you create or update an API deployment in the following ways:
   - by specifying the JSON file in the Console when you select the **Upload an existing API** option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see [Deploying an API on an API Gateway by Creating an API Deployment](#) on page 363.

6. Having set the log level for execution logs, follow the instructions in [Enabling Logging for a Resource](#) on page 2591 to create and enable a new API deployment log in the Oracle Cloud Infrastructure Logging service.

### Editing a JSON File to Set Up Logging Policies to Store Logs in Object Storage

In earlier API Gateway releases (prior to the release of the Oracle Cloud Infrastructure Logging service), you could direct API Gateway to store and view access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage. This functionality is still available for any API deployments you created in earlier releases where you previously specified a logging policy, as described below. However, note the following:

- If you set up Oracle Cloud Infrastructure Logging to store logs for an API deployment, you are no longer able to store logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage for that API deployment.
- The ability to store access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage will be deprecated in a future release.

To edit the API deployment specification in a JSON file to store logs in Object Storage:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add a logging policy, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

   At a minimum, the API deployment specification will include a **routes** section containing:

   - A path. For example, `/hello`
   - One or more methods. For example, GET
   - A definition of a back end. For example, a URL, or the OCID of a function in Oracle Functions.

   For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

   ```json
   {
     "routes": [
       {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
           "type": "ORACLE_FUNCTIONS_BACKEND",
           "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
       }
     ]
   }
   ```
2. (Optional) To add a logging policy to the API deployment specification that applies globally to all routes in the API deployment specification:

   a. Insert a `loggingPolicies` section before the `routes` section. For example:

   ```json
   {
     "loggingPolicies": {},
     "routes": [
       {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
           "type": "ORACLE_FUNCTIONS_BACKEND",
           "functionId": "ocid1.fnfunc.ocl.phxaaaaaaaaab______xmq"
         }
       }
     ]
   }
   
   b. (Optional) Record a summary of every request and response that goes through the gateway by including the `accessLog` policy in the `loggingPolicies` section, and setting the `isEnabled` property to `true`. For example:

   ```json
   {
     "loggingPolicies": {
       "accessLog": {
         "isEnabled": true
       },
       "routes": [
         {
           "path": "/hello",
           "methods": ["GET"],
           "backend": {
             "type": "ORACLE_FUNCTIONS_BACKEND",
             "functionId": "ocid1.fnfunc.ocl.phxaaaaaaaaab______xmq"
           }
         }
       ]
     }
   }
   
   c. (Optional) Record information about processing within the API gateway by including the `executionLog` policy in the `loggingPolicies` section, setting the `isEnabled` property to `true`, and setting the `logLevel` property to one of the following:

   - `INFO` to record a summary of every processing stage.
   - `WARN` to record only transient errors that occur during processing. For example, a connection reset.
   - `ERROR` to record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

   For example:

   ```json
   {
     "loggingPolicies": {
       "accessLog": {
         "isEnabled": true
       },
       "executionLog": {
         "isEnabled": true,
         "logLevel": "INFO"
       }
     }
   }
   ```
3. (Optional) To add a logging policy to the API deployment specification that applies to a particular route (overriding the global logging policy):

a. Insert a `loggingPolicies` section after the route's `backend` section. For example:

```json
    
    "loggingPolicies": { 
    
    "accessLog": { 
    
    "isEnabled": true 
    
    },
    "executionLog": { 
    
    "isEnabled": true, 
    
    "logLevel": "INFO"
    
    }
    
    }
    
    "routes": [ 
    
    { 
    
    "path": "/hello",
    "methods": ["GET"],
    "backend": { 
    
    "type": "ORACLE_FUNCTIONS_BACKEND",
    "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
    
    }
    
    }
    
    
    }  
    
    "loggingPolicies": {}  
    
    }
```

b. (Optional) Record a summary of every request and response that goes through the gateway to the route by including the `accessLog` policy in the `loggingPolicies` section, and setting the `isEnabled` property to `true`.

For example:

```json
    
    "loggingPolicies": { 
    
    "accessLog": { 
    
    "isEnabled": true 
    
    },
    "executionLog": { 
    
    "isEnabled": true, 
    
    "logLevel": "INFO"
    
    }
    
    }
    
    "routes": [ 
    
    { 
    
    "path": "/hello",
    "methods": ["GET"],
    "backend": { 
    
    "type": "ORACLE_FUNCTIONS_BACKEND",
    "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
    
    }
    
    }
    
    
    }  
    
    "loggingPolicies": {}  
    
    }
```
c. (Optional) Record information about processing within the API gateway for the route by including the executionLog policy in the loggingPolicies section, setting the isEnabled property to true, and setting the logLevel property to one of the following:

- **INFO** to record a summary of every processing stage.
- **WARN** to record only transient errors that occur during processing. For example, a connection reset.
- **ERROR** to record only persistent errors that occur during processing. For example, an internal error, or a call to a function that returns a 404 message.

For example:

```json
{
    "loggingPolicies": {
        "accessLog": {
            "isEnabled": true
        },
        "executionLog": {
            "isEnabled": true,
            "logLevel": "INFO"
        }
    },
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            },
            "loggingPolicies": {
                "accessLog": {
                    "isEnabled": true
                },
                "executionLog": {
                    "isEnabled": true,
                    "logLevel": "ERROR"
                }
            }
        }
    ]
}
```

4. Save the JSON file containing the API deployment specification.

5. Use the API deployment specification when you create or update an API deployment in the following ways:

- by specifying the JSON file in the Console when you select the **Upload an existing API** option
- by specifying the JSON file in a request to the API Gateway REST API

For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363.
Viewing Logs

Having added logging to an API deployment specification and deployed the API on an API gateway, the API Gateway service writes logs accordingly.

Viewing Logs in Oracle Cloud Infrastructure Logging

You can view the content of an API deployment log in Oracle Cloud Infrastructure Logging from the API Deployment Details page. Under Resources, click Logs, and then click the name of the log you want to view.

Alternatively, you can view the content of an API deployment log from the Oracle Cloud Infrastructure Logging Log Search page. See To view the contents of logs on page 2581.

For more information about the content of access and execution logs, see:

- API Deployment Access Log on page 2597
- API Deployment Execution Log on page 2598

Viewing Logs in Oracle Cloud Infrastructure Object Storage

In earlier API Gateway releases (prior to the release of the Oracle Cloud Infrastructure Logging service), you could direct API Gateway to store and view access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage. This functionality is still available for any API deployments you created in earlier releases where you previously specified a logging policy, as described below. However, note the following:

- If you set up Oracle Cloud Infrastructure Logging to store logs for an API deployment, you are no longer able to store logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage for that API deployment.
- The ability to store access logs and execution logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage will be deprecated in a future release.

To view logs that have been stored in a storage bucket in Oracle Cloud Infrastructure Object Storage:

1. In the Console, under Core Infrastructure, click Object Storage.
2. Choose the Compartment that owns API Gateway-related resources. If the API gateway and the API deployment are in different compartments, choose the compartment that owns the API gateway.

   The Object Storage page shows the storage buckets in the compartment.

3. On the Object Storage page, click the storage bucket name that includes the OCID of the compartment that owns the API Gateway-related resources.
4. Click Objects under Resources to see a list of log objects in the storage bucket, each with a name in the format:

   `api_gateway_deployment_access_log/<deployment-ocid>/<datetimestamp>.log.gz`

   where:

   - `<deployment-ocid>` is the OCID of the API deployment.
   - `<datetimestamp>` is the date and time at the start of the logging window.

5. Click the Actions icon (three dots) beside the log you want to view, and then click Download and save the log as a file in a convenient location.
6. Open the log file in a text editor to view the log messages.

   Each log message contains:
   • the number of bytes sent in the message
   • the compartment OCID
   • the API deployment OCID
   • the API gateway OCID
   • the user agent
   • the request and the endpoint
   • the client IP address
   • the request duration (in seconds)
   • the message number
   • the timestamp

For example:

```
{"bodybytesSent":292,"compartmentId":"ocid1.compartment.oc1..aaaaaa7______ysq","deploymentId":"ocid1.apideployment.oc1.p.../marketing/hello
"remoteAddr":"123.45.678.90","remoteUser":"","requestDuration":0.167","re...
```

Adding an HTTP or HTTPS URL as an API Gateway Back End

A common requirement is to build an API with the HTTP or HTTPS URL of a back-end service, and an API gateway providing front-end access to the back-end URL.

Having used the API Gateway service to create an API gateway, you can create an API deployment to access HTTP and HTTPS URLs.

The HTTP or HTTPS URL that you specify for the back-end service can be:

• The URL of a service that is publicly available on the internet.
• The URL of an Oracle Cloud Infrastructure service (for example, Oracle Functions).
• The URL of a service on your own private or internal network (for example, connected to the VCN by FastConnect).

The URL you provide in the API deployment specification to identify the HTTP or HTTPS back-end service can include the host name or the host IP address. If you provide the host name, use the DHCP Options property of the API gateway's subnet to control how host names included in the API deployment specification are resolved to IP addresses at runtime:

• If the host name for a back-end service is publicly published on the internet, or if the host name belongs to an instance in the same VCN, select a DHCP options set for the API gateway's subnet that has the Oracle-provided Internet and VCN Resolver as the DNS Type. This is the default if you do not explicitly select a DHCP options set.
• If the host name is for a back-end service on your own private or internal network, select a DHCP options set for the API gateway's subnet that has Custom Resolver as the DNS Type, and has the URL of a suitable DNS server that can resolve the host name to an IP address.

Note that you can change the DNS server details in the DHCP options set specified for an API gateway's subnet. The API gateway will be reconfigured to use the updated DNS server details within two hours. For more information about resolving host names to IP addresses, see DNS in Your Virtual Cloud Network on page 2910 and DHCP Options on page 2917.

You can add HTTP and HTTPS back ends to an API deployment specification by:

• using the Console
• editing a JSON file
Using the Console to Add HTTP or HTTPS Back Ends to an API Deployment Specification

To add an HTTP or HTTPS back end to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. On the Routes page, create a new route and specify:
   - **Path**: A path for API calls using the listed methods to the back-end service. Note that the route path you specify:
     - is relative to the deployment path prefix (see Deploying an API on an API Gateway by Creating an API Deployment on page 363)
     - must be preceded by a forward slash (/), and can be just that single forward slash
     - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
     - can include alphanumeric uppercase and lowercase characters
     - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
     - can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)
   - **Methods**: One or more methods accepted by the back-end service. For example, GET, PUT.
   - **Type**: The type of the back-end service as HTTP.
   - **URL**: The URL you want to use as the back-end service, in the format `<protocol>://<host>[:<port>]/<path>` where:
     - `<protocol>` is either http or https.
     - `<host>` is the host name or the host IP address of the back-end service. For example, api.weather.gov. If you provide a host name, use the DHCP Options property of the API gateway's subnet to control how host names are resolved to IP addresses at runtime.
     - `<port>` is optionally a port number.
     - `<path>` is optionally a subdirectory or file at the host where the back-end service is located.

   Note that `<path>` must not contain parameters directly, but can contain context variables. For more information and examples showing how to use context variables to substitute path, query, and header parameters into the path, see Adding Context Variables to Policies and HTTP Back End Definitions on page 378.

   For example, "url": "https://api.weather.gov".

   - **Connection establishment timeout in seconds**: Optionally, a floating point value indicating how long (in seconds) to allow when establishing a connection with the back-end service. The minimum is 1.0, the maximum is 75.0. If not specified, the default of 60.0 seconds is used.
   - **Request transmit timeout in seconds**: Optionally, a floating point value indicating how long (in seconds) to allow when transmitting a request to the back-end service. The minimum is 1.0, the maximum is 300.0. If not specified, the default of 10.0 seconds is used.
   - **Reading response timeout in seconds**: Optionally, a floating point value indicating how long (in seconds) to allow when reading a response from the back-end service. The minimum is 1.0, the maximum is 300.0. If not specified, the default of 10.0 seconds is used.
   - **Disable SSL verification**: Whether to disable SSL verification when communicating with the back-end service. By default, this option is not selected.

In this example, the route defines a weather service as an HTTP back end.

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>/weather</td>
</tr>
<tr>
<td>Field</td>
<td>Enter:</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Methods:</td>
<td>GET</td>
</tr>
<tr>
<td>Type:</td>
<td>HTTP</td>
</tr>
<tr>
<td>URL:</td>
<td><a href="https://api.weather.gov">https://api.weather.gov</a></td>
</tr>
<tr>
<td>Connection establishment timeout in seconds:</td>
<td>45</td>
</tr>
<tr>
<td>Request transmit timeout in seconds:</td>
<td>15</td>
</tr>
<tr>
<td>Reading response timeout in seconds:</td>
<td>15</td>
</tr>
<tr>
<td>Disable SSL verification:</td>
<td>(Not selected)</td>
</tr>
</tbody>
</table>

3. (Optional) Click **Another Route** to enter details of additional routes.
4. Click **Next** to review the details you entered for the API deployment.
5. Click **Create** or **Save Changes** to create or update the API deployment.
6. (Optional) Confirm the API has been deployed successfully by calling it (see **Calling an API Deployed on an API Gateway** on page 384).

### Editing a JSON File to Add HTTP or HTTPS Back Ends to an API Deployment Specification

To add an HTTP or HTTPS back end to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, create a new API deployment specification (see **Creating an API Deployment Specification** on page 361) in the format:

   ```json
   {
       "requestPolicies": {},
       "routes": [
           {
               "path": "<api-route-path>",
               "methods": ["<method-list>"],
               "backend": {
                   "type": "HTTP_BACKEND",
                   "url": "<identifier>",
                   "connectTimeoutInSeconds": <seconds>,
                   "readTimeoutInSeconds": <seconds>,
                   "sendTimeoutInSeconds": <seconds>,
                   "isSSLVerifyDisabled": <true|false>
               },
               "requestPolicies": {}
           }
       ]
   }
   ```

   where:

   - "requestPolicies" specifies optional policies to control the behavior of an API deployment. If you want to apply policies to all routes in an API deployment specification, place the policies outside the `routes` section. If you want to apply the policies just to a particular route, place the policies inside the `routes` section.
• `<api-route-path>` specifies a path for API calls using the listed methods to the back-end service. Note that the route path you specify:
  • is relative to the deployment path prefix (see Deploying an API on an API Gateway by Creating an API Deployment on page 363)
  • must be preceded by a forward slash (/), and can be just that single forward slash
  • can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  • can include alphanumeric uppercase and lowercase characters
  • can include the special characters $ – _ . + ! * ' ( ) , % ; : @ & =
  • can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)
• `<method-list>` specifies one or more methods accepted by the back-end service, separated by commas. For example, "GET, PUT".
• "type": "HTTP_BACKEND" specifies the API gateway back end is an HTTP or HTTPS URL.
• "url": "<identifier>" specifies the URL you want to use as the back-end service, in the format <protocol>://<host>:<port>/<path> where:
  • <protocol> is either http or https.
  • <host> is the host name or the host IP address of the back-end service. For example, api.weather.gov. If you provide a host name, use the DHCP Options property of the API gateway's subnet to control how host names are resolved to IP addresses at runtime.
  • <port> is optionally a port number.
  • <path> is optionally a subdirectory or file at the host where the back-end service is located.
    Note that <path> must not contain parameters directly, but can contain context variables. For more information and examples showing how to use context variables to substitute path, query, and header parameters into the path, see Adding Context Variables to Policies and HTTP Back End Definitions on page 378.
For example, "url": "https://api.weather.gov".
• "connectTimeoutInSeconds": <seconds> is an optional floating point value indicating how long (in seconds) to allow when establishing a connection with the back-end service. The minimum is 0.0, the maximum is 75.0. If not specified, the default of 60.0 seconds is used.
• "readTimeoutInSeconds": <seconds> is an optional floating point value indicating how long (in seconds) to allow when reading a response from the back-end service. The minimum is 0.0, the maximum is 300.0. If not specified, the default of 10.0 seconds is used.
• "sendTimeoutInSeconds": <seconds> is an optional floating point value indicating how long (in seconds) to allow when transmitting a request to the back-end service. The minimum is 0.0, the maximum is 300.0. If not specified, the default of 10.0 seconds is used.
• "isSSLVerifyDisabled": <true|false> is an optional boolean value (either true or false) indicating whether to disable SSL verification when communicating with the back-end service. If not specified, the default of false is used.
For example, the following basic API deployment specification defines a weather service as an HTTP back end:

```json
{
    "routes": [
        {
            "path": "/weather",
            "methods": ["GET"],
            "backend": {
                "type": "HTTP_BACKEND",
                "url": "https://api.weather.gov",
                "connectTimeoutInSeconds": 45,
                "readTimeoutInSeconds": 15,
                "sendTimeoutInSeconds": 15,
            }]
    }
}
```
2. Save the JSON file containing the API deployment specification.
3. Use the API deployment specification when you create or update an API deployment in the following ways:
   • by specifying the JSON file in the Console when you select the Upload an existing API option
   • by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363.

4. (Optional) Confirm the API has been deployed by calling it (see Calling an API Deployed on an API Gateway on page 384).

Adding a Function in Oracle Functions as an API Gateway Back End

A common requirement is to build an API with serverless functions as a back end, and an API gateway providing front-end access to those functions.

Oracle Functions enables you to create serverless functions that are built as Docker images and pushed to a specified Docker registry. A definition of each function is stored as metadata in the Oracle Functions server. When a function is invoked for the first time, Oracle Functions pulls the function’s Docker image from the specified Docker registry, runs it as a Docker container, and executes the function. If there are subsequent requests to the same function, Oracle Functions directs those requests to the same running container. After a period being idle, the Docker container is stopped.

Having used the API Gateway service to create an API gateway, you can create an API deployment that invokes serverless functions defined in Oracle Functions.

Before you can use serverless functions in Oracle Functions as the back end for an API:

• Serverless functions referenced in the API deployment specification must have already been created and deployed in Oracle Functions. The functions must be routable from the VCN specified for the API gateway, either through an internet gateway (in the case of a public API gateway) or through a service gateway (in the case of a private API gateway). See Creating and Deploying Functions on page 2063. For a related Developer Tutorial, see Functions: Call a Function using API Gateway.
• Appropriate policies must already exist that give access to serverless functions defined in Oracle Functions to:
  • a group to which your user account belongs (see Create a Policy to Give API Gateway Users Access to Functions on page 344)
  • API gateways (see Create a Policy to Give API Gateways Access to Functions on page 345)

You can add serverless function back ends to an API deployment specification by:

• using the Console
• editing a JSON file

Creating and Deploying a Serverless Function in Oracle Functions for Use as an API Gateway Back End

To create a serverless function in Oracle Functions that can be invoked from an API gateway, follow the instructions in the Oracle Functions documentation to:

• Confirm that you have completed the prerequisite steps for using Oracle Functions, as described in Preparing for Oracle Functions on page 2038.
• Create and deploy the function in a compartment to which API gateways have been granted access, as described in Creating and Deploying Functions on page 2063.
Using the Console to Add Serverless Function Back Ends to an API Deployment Specification

To add an Oracle Functions function back end to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the **From Scratch** option, and enter details on the **Basic Information** page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. On the **Routes** page, create a new route and specify:
   - **Path:** A path for API calls using the listed methods to the back-end service. Note that the route path you specify:
     - is relative to the deployment path prefix (see Deploying an API on an API Gateway by Creating an API Deployment on page 363)
     - must be preceded by a forward slash (/), and can be just that single forward slash
     - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
     - can include alphanumeric uppercase and lowercase characters
     - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
     - can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)
   - **Methods:** One or more methods accepted by the back-end service. For example, GET, PUT.
   - **Type:** The type of the back-end service as Oracle Functions.
   - **Application in <compartment-name>:** The name of the application in Oracle Functions that contains the function. You can select an application from a different compartment.
   - **Function Name:** The name of the function in Oracle Functions.

   In this example, the route defines a simple Hello World serverless function in Oracle Functions as a single back end.

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path:</td>
<td>/hello</td>
</tr>
<tr>
<td>Methods:</td>
<td>GET</td>
</tr>
<tr>
<td>Type:</td>
<td>Oracle Functions</td>
</tr>
<tr>
<td>Application in &lt;compartment-name&gt;:</td>
<td>acmeapp</td>
</tr>
<tr>
<td>Function Name:</td>
<td>acme-func</td>
</tr>
</tbody>
</table>

3. (Optional) Click **Another Route** to enter details of additional routes.

4. Click **Next** to review the details you entered for the API deployment.

5. Click **Create** or **Save Changes** to create or update the API deployment.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

   If the serverless function accepts parameters, include those in the call to the API. For example:

   ```bash
curl -k -X GET https://lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com/marketing/hello/ -d "name=John"
```

Editing a JSON File to Add Serverless Function Back Ends to an API Deployment Specification

To add an Oracle Functions function back end to an API deployment specification in a JSON file:
1. Using your preferred JSON editor, create the API deployment specification in a JSON file in the format:

```json
{
    "requestPolicies": {},
    "routes": [
        {
            "path": "<api-route-path>",
            "methods": ["<method-list>"]
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "<identifier>
            },
            "requestPolicies": {}
        }
    ]
}
```

where:

- "requestPolicies" specifies optional policies to control the behavior of an API deployment. If you want to apply policies to all routes in an API deployment specification, place the policies outside the `routes` section. If you want to apply the policies just to a particular route, place the policies inside the `routes` section. See [Adding Request Policies and Response Policies to API Deployment Specifications](#) on page 417.

- `<api-route-path>` specifies a path for API calls using the listed methods to the back-end service. Note that the route path you specify:
  - is relative to the deployment path prefix (see [Deploying an API on an API Gateway by Creating an API Deployment](#) on page 363)
  - must be preceded by a forward slash (/), and can be just that single forward slash
  - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - can include parameters and wildcards (see [Adding Path Parameters and Wildcards to Route Paths](#) on page 377)

- `<method-list>` specifies one or more methods accepted by the back-end service, separated by commas. For example, "GET, PUT".

- `<identifier>` specifies the OCID of the function you want to use as the back-end service. For example, "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq".

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        }
    ]
}
```

2. Save the JSON file containing the API deployment specification.
3. Use the API deployment specification when you create or update an API deployment in the following ways:
   • by specifying the JSON file in the Console when you select the **Upload an existing API** option
   • by specifying the JSON file in a request to the API Gateway REST API

   For more information, see **Deploying an API on an API Gateway by Creating an API Deployment** on page 363.

4. (Optional) Confirm the API has been deployed and that the serverless function in Oracle Functions can be invoked successfully by calling the API (see **Calling an API Deployed on an API Gateway** on page 384). If the serverless function accepts parameters, include those in the call to the API. For example:

   curl -k -X GET https://lak...sjd.apigateway.us-phoenix-1.oci.customer-oci.com/marketing/hello/ -d "name=john"

### Adding Stock Responses as an API Gateway Back End

You'll often want to verify that an API has been successfully deployed on an API gateway without having to set up an actual back-end service. One approach is to define a route in the API deployment specification that has a path to a 'dummy' back end. On receiving a request to that path, the API gateway itself acts as the back end and returns a stock response you've specified.

Equally, there are some situations in a production deployment where you'll want a particular path for a route to consistently return the same stock response without sending a request to a back end. For example, when you want a call to a path to always return a specific HTTP status code in the response.

Using the API Gateway service, you can define a path to a stock response back end that always returns the same:

- HTTP status code
- HTTP header fields (name-value pairs)
- content in the body of the response

Note the following restrictions when defining stock responses and stock response back ends:

- each header name must not exceed 1KB in length
- each header value must not exceed 4KB in length
- each body response must not exceed 5KB in length (including any encoding)
- a stock response back end definition must not include more than 50 header fields

You can add stock response back ends to an API deployment specification by:

- using the Console
- editing a JSON file

### Using the Console to Add Stock Responses to an API Deployment Specification

To add stock responses to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the **From Scratch** option, and enter details on the **Basic Information** page.

   For more information, see **Deploying an API on an API Gateway by Creating an API Deployment** on page 363 and **Updating API Gateways and API Deployments** on page 387.
2. On the **Routes** page, create a new route and specify:

- **Path:** A path for API calls using the listed methods to the back-end service. Note that the route path you specify:
  - is relative to the deployment path prefix (see *Deploying an API on an API Gateway by Creating an API Deployment* on page 363)
  - must be preceded by a forward slash (/), and can be just that single forward slash
  - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - can include parameters and wildcards (see *Adding Path Parameters and Wildcards to Route Paths* on page 377)

- **Methods:** One or more methods accepted by the back-end service. For example, **GET,** **PUT**.

- **Type:** The type of the back-end service as **Stock Response**.

- **Status Code:** Any valid HTTP response code. For example, **200**

- **Body:** Optionally specifies the content of the response body, in an appropriate format. For example:
  - If you specify a **Header Name** and **Header Value** of **Content-Type** and **text/plain** respectively, the response body might be "Hello world.".
  - If you specify a **Header Name** and **Header Value** of **Content-Type** and **application/json** respectively, the response body might be ("username": "john.doe").

Note that the response body must not exceed 5KB in length (including any encoding).

- **Header Name** and **Header Value:** Optionally, you can specify the name of an HTTP response header and its value. For example, a name of **Content-Type** and a value of **application/json**. You can specify multiple header name and value pairs (up to a maximum of 50). Note that in each case:
  - the header name must not exceed 1KB in length
  - the header value must not exceed 4KB in length

In this example, a request to the **/test** path returns a 200 status code and a JSON payload in the body of the response.

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path:</td>
<td>/test</td>
</tr>
<tr>
<td>Methods:</td>
<td>GET</td>
</tr>
<tr>
<td>Type:</td>
<td>Stock Response</td>
</tr>
<tr>
<td>Status Code:</td>
<td>200</td>
</tr>
<tr>
<td>Body:</td>
<td>(&quot;username&quot;: &quot;john.doe&quot;)</td>
</tr>
<tr>
<td>Header Name:</td>
<td>Content-Type</td>
</tr>
<tr>
<td>Header Value:</td>
<td>application/json</td>
</tr>
</tbody>
</table>

In this example, a request to the **/test-redirect** path returns a 302 status code and a temporary url in the **Location** header of the response.

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path:</td>
<td>/test-redirect</td>
</tr>
<tr>
<td>Methods:</td>
<td>GET</td>
</tr>
<tr>
<td>Type:</td>
<td>Stock Response</td>
</tr>
<tr>
<td>Status Code:</td>
<td>302</td>
</tr>
</tbody>
</table>
3. (Optional) Click **Another Route** to enter details of additional routes.
4. Click **Next** to review the details you entered for the API deployment.
5. Click **Create** or **Save Changes** to create or update the API deployment.
6. (Optional) Confirm the API has been deployed successfully by calling it (see [Calling an API Deployed on an API Gateway](#) on page 384).

## Editing a JSON File to Add Stock Responses to an API Deployment Specification

To add stock responses to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add a stock response back end, or create a new API deployment specification (see [Creating an API Deployment Specification](#) on page 361).

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
    "routes": [  
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        }
    ]
}
```

2. In the `routes` section, include a new `path` section for a stock response back end:

```json
{
    "routes": [  
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        },
        {
            "path": "<api-route-path>",
            "methods": ["<method-list>"],
            "backend": {
                "type": "STOCK_RESPONSE_BACKEND",
                "status": <http-response-code>,
                "headers": [{
                    "name": "<header-name>",
                    "value": "<header-value>
                }],
                "body": "<body-content>"
            }
        }
    ]
}
```
where:

- `<api-route-path>` specifies a path for API calls using the listed methods to the stock response back end. Note that the route path you specify:
  - is relative to the deployment path prefix (see Deploying an API on an API Gateway by Creating an API Deployment on page 363)
  - must be preceded by a forward slash (/), and can be just that single forward slash
  - can contain multiple forward slashes (provided they are not adjacent), and can end with a forward slash
  - can include alphanumeric uppercase and lowercase characters
  - can include the special characters $ - _ . + ! * ' ( ) , % ; : @ & =
  - can include parameters and wildcards (see Adding Path Parameters and Wildcards to Route Paths on page 377)
- `<method-list>` specifies one or more methods accepted by the stock response back end, separated by commas. For example, "GET, PUT".
- "type": "STOCK_RESPONSE_BACKEND" indicates that the API gateway itself will act as the back end and return the stock response you define (the status code, the header fields and the body content).
- `<http-response-code>` is any valid HTTP response code. For example, 200
- "name": "<header-name>", "value": "<header-value>" optionally specifies the name of an HTTP response header and its value. For example, "name": "Content-Type", "value": "application/json". You can specify multiple "name": "<header-name>", "value": "<header-value>" pairs in the headers: section (up to a maximum of 50). Note that in each case:
  - `<header-name>` must not exceed 1KB in length
  - `<header-value>` must not exceed 4KB in length
- "body": "<body-content>" optionally specifies the content of the response body, in an appropriate format. For example:
  - If the Content-Type header is text/plain, the response body might be "body": "Hello world".
  - If the Content-Type header is application/json, the response body might be "body": 
    "\"username\": \"john.doe\"\". In the case of a JSON response, note that quotation marks in the response have to be escaped with a backslash (\) character.

Note that `<body-content>` must not exceed 5KB in length (including any encoding).

In this example, a request to the /test path returns a 200 status code and a JSON payload in the body of the response.

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      }
    },
    {
      "path": "/test",
      "methods": ["GET"],
      "backend": {
        "type": "STOCK_RESPONSE_BACKEND",
        "status": 200,
        "headers": [
```
In this example, a request to the /test-redirect path returns a 302 status code and a temporary url in the Location header of the response. This example also demonstrates that you can create an API deployment specification with just one route to a back end of type STOCK_RESPONSE_BACKEND.

```
{
  "routes": [
    {
      "path": "/test-redirect",
      "methods": ["GET"],
      "backend": {
        "type": "STOCK_RESPONSE_BACKEND",
        "status": 302,
        "headers": [{
          "name": "Location",
          "value": "http://www.example.com"
        }]
      }
    }
  ]
}
```

3. Save the JSON file containing the API deployment specification.
4. Use the API deployment specification when you create or update an API deployment in the following ways:
   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.
5. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

### Adding Request Policies and Response Policies to API Deployment Specifications

You can control the behavior of an API deployment you create on an API gateway by adding request and response policies to the API deployment specification:

- a request policy describes actions to be performed on an incoming request from an API client before it is sent to a back end
- a response policy describes actions to be performed on a response returned from a back end before it is sent to an API client

You can use request policies and/or response policies to:

- limit the number of requests sent to back-end services
- enable CORS (Cross-Origin Resource Sharing) support
- provide authentication and authorization
- modify incoming requests and outgoing responses

You can add policies to an API deployment specification that apply globally to all routes in the API deployment specification, as well as policies that apply only to particular routes.
Note that API Gateway request policies and response policies are different to IAM policies, which control access to Oracle Cloud Infrastructure resources.

You can add request and response policies to an API deployment specification by:

• using the Console
• editing a JSON file

**Using the Console to Add Request Policies and Response Policies**

To add request policies and response policies to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the **From Scratch** option, and enter details on the **Basic Information** page.
   
   For more information, see [Deploying an API on an API Gateway by Creating an API Deployment](#) on page 363 and [Updating API Gateways and API Deployments](#) on page 387.

2. In the **API Request Policies** section of the **Basic Information** page, specify request policies that apply globally to all routes in the API deployment specification:
   
   • **Authentication**: A policy to control access to APIs you deploy to API gateways based on the end user sending a request, and define what it is that they are allowed to do. Having specified a global authentication policy first, you can then specify authorization policies that apply to individual routes in the API deployment specification. See [Adding Authentication and Authorization to API Deployments](#) on page 431.
   
   • **CORS**: A policy to enable CORS support in the APIs you deploy to API gateways. You can also specify CORS policies that apply to individual routes in the API deployment specification (you don't need to have entered a global CORS policy first). See [Adding CORS support to API Deployments](#) on page 424.
   
   • **Rate Limiting**: A policy to limit the rate at which API clients can make requests to back-end services. You can only apply a rate-limiting policy globally to all routes in the API deployment specification (not to individual routes). See [Limiting the Number of Requests to API Gateway Back Ends](#) on page 421.

3. Click **Next** to enter details for individual routes in the API deployment on the **Routes** page.

4. To specify request policies that apply to an individual route, click **Show Route Request Policies** and specify:
   
   • **Authorization**: A policy to specify the operations an end user is allowed to perform, based on the end user's access scopes. Note that you must have already specified a global authentication policy before you can specify an authorization policy on an individual route. See [Adding Authentication and Authorization to API Deployments](#) on page 431.
   
   • **CORS**: A policy to enable CORS support for individual routes in the API deployment specification (you don't need to have entered a global CORS policy first). See [Adding CORS support to API Deployments](#) on page 424.
   
   • **Header Transformations**: A policy to add, remove, and modify headers in requests. See [Using the Console to Add Header Transformation Request Policies](#) on page 453.
   
   • **Query Transformations**: A policy to add, remove, and modify query parameters in requests. See [Using the Console to Add Query Parameter Transformation Request Policies](#) on page 459.

5. To specify response policies that apply to an individual route, click **Show Route Response Policies** and specify:
   
   • **Header Transformations**: A policy to add, remove, and modify headers in responses. See [Using the Console to Add Header Transformation Response Policies](#) on page 465.

6. Click **Next** to review the details you entered for the API deployment.

7. Click **Create** or **Save Changes** to create or update the API deployment.

8. (Optional) Confirm the API has been deployed successfully by calling it (see [Calling an API Deployed on an API Gateway](#) on page 384).

**Editing a JSON File to Add Request Policies and Response Policies**

To add request policies and response policies to an API deployment specification in a JSON file:
1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add a request policy or response policy, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

At a minimum, the API deployment specification will include a routes section containing:

- A path. For example, /hello
- One or more methods. For example, GET
- A definition of a back end. For example, a URL, or the OCID of a function in Oracle Functions.

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
   "routes": [
      {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
            "type": "ORACLE_FUNCTIONS_BACKEND",
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
      }
   ]
}
```

2. To add a request policy that applies globally to all routes in the API deployment specification:
   a. Insert a requestPolicies section before the routes section. For example:

```json
{
   "requestPolicies": {},
   "routes": [
      {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
            "type": "ORACLE_FUNCTIONS_BACKEND",
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
      }
   ]
}
```
   b. Include a request policy in the requestPolicies section.

For example, to limit the number of requests sent to all routes in an API deployment specification, you'd include the rateLimiting policy in the requestPolicies section as follows:

```json
{
   "requestPolicies": {
      "rateLimiting": {
         "rateKey": "CLIENT_IP",
         "rateInRequestsPerSecond": 10
      }
   },
   "routes": [
      {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
            "type": "ORACLE_FUNCTIONS_BACKEND",
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
      }
   ]
}
```
For more information about the rateLimiting request policy, see Limiting the Number of Requests to API Gateway Back Ends on page 421.

3. To add a request policy that applies to an individual route in the API deployment specification:

   a. Insert a requestPolicies section after the route's backend section. For example:

   ```json
   { "routes": [ { "path": "/hello", "methods": ["GET"], "backend": { "type": "ORACLE_FUNCTIONS_BACKEND", "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq" }, "requestPolicies": {} ] } }
   ```

   b. Include a request policy in the requestPolicies section.

      For example, to enable CORS support in an API deployment for a particular route, you'd include the cors policy in the requestPolicies section as follows:

      ```json
      { "routes": [ { "path": "/hello", "methods": ["GET"], "backend": { "type": "ORACLE_FUNCTIONS_BACKEND", "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq" }, "requestPolicies": { "cors": { "allowedOrigins": ["*", "https://oracle.com"], "allowedMethods": ["*", "GET"], "allowedHeaders": [], "exposedHeaders": [], "isAllowCredentialsEnabled": false, "maxAgeInSeconds": 3000 } } ] } }
      ```

      For more information about the cors request policy, see Adding CORS support to API Deployments on page 424.

4. To add a response policy that applies to an individual route in the API deployment specification:

   a. Insert a responsePolicies section after the route's backend section. For example:

   ```json
   { "routes": [ { "path": "/hello", }
   ```
b. Include a response policy in the `responsePolicies` section.

For example, to rename any `X-Username` header to `X-User-ID` in the response from a particular route, you'd include the `headerTransformations` policy in the `responsePolicies` section as follows:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "responsePolicies": {
        "headerTransformations": {
          "renameHeaders": {
            "items": [
              {
                "from": "X-Username",
                "to": "X-User-ID"
              }
            ]
          }
        }
      }
    }
  ]
}
```

For more information about the `headerTransformations` response policy, see Editing a JSON File to Add Header Transformation Response Policies on page 466.

5. Save the JSON file containing the API deployment specification.

6. Use the API deployment specification when you create or update an API deployment in the following ways:

   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363.

### Limiting the Number of Requests to API Gateway Back Ends

Having created an API gateway and deployed one or more APIs on it, you'll typically want to limit the rate at which API clients can make requests to back-end services. For example, to:

- maintain high availability and fair use of resources by protecting back ends from being overwhelmed by too many requests
- prevent denial-of-service attacks
- constrain costs of resource consumption
- restrict usage of APIs by your customers' users in order to monetize APIs

You apply a rate limit globally to all routes in an API deployment specification.
If a request is denied because the rate limit has been exceeded, the response header specifies when the request can be retried.

You use a request policy to limit the number of requests (see Adding Request Policies and Response Policies to API Deployment Specifications on page 417).

You can add a rate-limiting request policy to an API deployment specification by:

- using the Console
- editing a JSON file

**Using the Console to Add Rate-Limiting Request Policies**

To add a rate-limiting request policy to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the **From Scratch** option, and enter details on the **Basic Information** page.
   
   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. In the **API Request Policies** section of the **Basic Information** page, click the **Add** button beside **Rate Limiting** and specify:
   
   - **Number of Requests per Second**: The maximum number of requests per second to send to any one route.
   - **Type of Rate Limit**: How the maximum number of requests per second threshold is applied. You can specify that the maximum applies either to the number of requests sent from any one API client (identified by its IP address), or to the total number of requests sent from all API clients.

3. Click **Save Changes**, and then click **Next** to enter details for individual routes in the API deployment on the **Routes** page. Note that you cannot apply rate-limiting policies to individual routes in the API deployment specification.

4. Click **Next** to review the details you entered for the API deployment.

5. Click **Create** or **Save Changes** to create or update the API deployment.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

**Editing a JSON File to Add Rate-Limiting Request Policies**

To add a rate-limiting request policy to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add a request limit, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

   For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

   ```json
   {
   "routes": [
   {
   "path": "/hello",
   "methods": ["GET"],
   "backend": {
   "type": "ORACLE_FUNCTIONS_BACKEND",
   "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
   }
   }
   }
   ```

2. Insert a requestPolicies section before the routes section, if one doesn't exist already. For example:

   ```json
   {
   "requestPolicies": {
   }
   ```
API Gateway

```
"requestPolicies": {},
"routes": [ 
    
    
],

3. Add the following rateLimiting policy to the new requestPolicies section to apply to all routes defined in the specification:

```

```
{ "requestPolicies": { 
    "rateLimiting": { 
        "rateKey": "<ratekey-value>",
        "rateInRequestsPerSecond": <requests-per-second>
    }

},

"routes": [ 
    
    
],
```

where:

- `<ratekey-value>` specifies whether the maximum number of requests threshold applies to the number of requests from individual API clients (each identified by their IP address) or to the total number of requests sent to the back-end service. Valid values are CLIENT_IP and TOTAL.
- `<requests-per-second>` is the maximum number of requests per second to send to any route.

For example:

```

```

```
{ "requestPolicies": { 
    "rateLimiting": { 
        "rateKey": "CLIENT_IP",
        "rateInRequestsPerSecond": 10
    }

},

"routes": [ 
    
    
],
```

Oracle Cloud Infrastructure User Guide 423
4. Save the JSON file containing the API deployment specification.

5. Use the API deployment specification when you create or update an API deployment in the following ways:
   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

Adding CORS support to API Deployments

Web browsers typically implement a "same-origin policy" to prevent code from making requests against a different origin to the one from which the code was served. The intention of the same-origin policy is to provide protection from malicious web sites. However, the same-origin policy can also prevent legitimate interactions between a server and clients of a known and trusted origin.

Cross-Origin Resource Sharing (CORS) is a cross-origin sharing standard to relax the same-origin policy by allowing code on a web page to consume a REST API served from a different origin. The CORS standard uses additional HTTP request headers and response headers to specify the origins that can be accessed.

The CORS standard also requires that for certain HTTP request methods, the request must be "pre-flighted". Before sending the actual request, the web browser sends a pre-flight request to the server to determine whether the methods in the actual request are supported. The server responds with the methods it will allow in an actual request. The web browser only sends the actual request if the response from the server indicates that the methods in the actual request are allowed. The CORS standard also enables servers to notify clients whether requests can include credentials (cookies, authorization headers, or TLS client certificates).

For more information about CORS, see resources available online including those from W3C and Mozilla.

Using the API Gateway service, you can enable CORS support in the APIs you deploy to API gateways. When you enable CORS support in an API deployment, HTTP pre-flight requests and actual requests to the API deployment return one or more CORS response headers to the API client. You set the CORS response header values in the API deployment specification.

You use request policies to add CORS support to APIs (see Adding Request Policies and Response Policies to API Deployment Specifications on page 417). You can apply a CORS request policy globally to all routes in an API deployment specification, or just to particular routes.

You can add a CORS request policy to an API deployment specification by:
   - using the Console
   - editing a JSON file

Using the Console to Add CORS Request Policies

To add a CORS request policy to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.
2. In the API Request Policies section of the Basic Information page, click the Add button beside CORS and specify:
   - **Allowed Origins**: An origin that is allowed to access the API deployment. For example, https://oracle.com. Click + Another Origin to enter second and subsequent origins.
   - **Allowed Methods**: One or more methods that are allowed in the actual request to the API deployment. For example, GET, PUT.
   - **Allowed Headers**: Optionally, an HTTP header that is allowed in the actual request to the API deployment. For example, opc-request-id or If-Match. Click + Another Header to enter second and subsequent headers.
   - **Exposed Headers**: Optionally, an HTTP header that API clients can access in the API deployment's response to an actual request. For example, ETag or opc-request-id. Click + Another Header to enter second and subsequent headers.
   - **Max age in seconds**: Optionally, an integer value indicating how long (in delta-seconds) the results of a preflight request can be cached by a browser. If you don't specify a value, the default is 0.
   - **Enable Allow Credentials**: Whether the actual request to the API deployment can be made using credentials (cookies, authorization headers, or TLS client certificates). By default, this option is not selected.

To find out how the different fields in the CORS request policy map onto different CORS response headers, see How a CORS Request Policy Maps to a CORS Response on page 429.

3. Click Save Changes, and then click Next to enter details for individual routes in the API deployment on the Routes page. To specify CORS request policies that apply to an individual route, click Show Route Request Policies, click the Add button beside CORS, and specify:
   - **Allowed Origins**: An origin that is allowed to access the route. For example, https://oracle.com. Click + Another Origin to enter second and subsequent origins.
   - **Allowed Methods**: One or more methods that are allowed in the actual request to the route. For example, GET, PUT.
   - **Allowed Headers**: Optionally, an HTTP header that is allowed in the actual request to the route. For example, opc-request-id or If-Match. Click + Another Header to enter second and subsequent headers.
   - **Exposed Headers**: Optionally, an HTTP header that API clients can access in the API deployment's response to an actual request. For example, ETag or opc-request-id. Click + Another Header to enter second and subsequent headers.
   - **Max age in seconds**: Optionally, an integer value indicating how long (in delta-seconds) the results of a preflight request can be cached by a browser. If you don't specify a value, the default is 0.
   - **Enable Allow Credentials**: Whether the actual request to the route can be made using credentials (cookies, authorization headers, or TLS client certificates). By default, this option is not selected.

To find out how the different fields in the CORS request policy map onto different CORS response headers, see How a CORS Request Policy Maps to a CORS Response on page 429.

4. Click Save Changes, and then click Next to review the details you entered for the API deployment and for individual routes.

5. Click Create or Save Changes to create or update the API deployment.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

**Editing a JSON File to Add CORS Request Policies**

To add a CORS request policy to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add CORS support, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

   For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:
2. To specify a CORS request policy that applies globally to all the routes in an API deployment:
   
a. Insert a requestPolicies section before the routes section, if one doesn't exist already. For example:

```json
{  
  "requestPolicies": {},  
  "routes": [  
    {  
      "path": "/hello",  
      "methods": ["GET"],  
      "backend": {  
        "type": "ORACLE_FUNCTIONS_BACKEND",  
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"  
      }  
    }  
  ]
}
```

b. Add the following cors policy to the new requestPolicies section to apply globally to all the routes in an API deployment:

```json
{  
  "requestPolicies": {  
    "cors":{  
      "allowedOrigins": [<list-of-origins>],  
      "allowedMethods": [<list-of-methods>],  
      "allowedHeaders": [<list-of-implicit-headers>],  
      "exposedHeaders": [<list-of-exposed-headers>],  
      "isAllowCredentialsEnabled": <true|false>,  
      "maxAgeInSeconds": <seconds>
    }  
  },  
  "routes": [  
    {  
      "path": "/hello",  
      "methods": ["GET"],  
      "backend": {  
        "type": "ORACLE_FUNCTIONS_BACKEND",  
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"  
      }  
    }  
  ]
}
```
where:

- "allowedOrigins": [<list-of-origins>] is a required comma-separated list of origins that are allowed to access the API deployment. For example, "allowedOrigins": ["*", "https://oracle.com"]
- "allowedMethods": [<list-of-methods>] is an optional comma-separated list of HTTP methods that are allowed in the actual request to the API deployment. For example, "allowedMethods": ["*", "GET"]
- "allowedHeaders": [<list-of-implicit-headers>] is an optional comma-separated list of HTTP headers that are allowed in the actual request to the API deployment. For example, "allowedHeaders": ["opc-request-id", "If-Match"]
- "exposedHeaders": [<list-of-exposed-headers>] is an optional comma-separated list of HTTP headers that API clients can access in the API deployment's response to an actual request. For example, "exposedHeaders": ["ETag", "opc-request-id"]
- "isAllowCredentialsEnabled": <true|false> is either true or false, indicating whether the actual request to the API deployment can be made using credentials (cookies, authorization headers, or TLS client certificates). If not specified, the default is false.
- "maxAgeInSeconds": <seconds> is an integer value, indicating how long (in delta-seconds) the results of a preflight request can be cached by a browser. If not specified, the default is 0.

For example:

```json
{
    "requestPolicies": {
        "cors": {
            "allowedOrigins": ["*", "https://oracle.com"],
            "allowedMethods": ["*", "GET"],
            "allowedHeaders": [],
            "exposedHeaders": [],
            "isAllowCredentialsEnabled": false,
            "maxAgeInSeconds": 3000
        }
    },
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        }
    ]
}
```

To find out how the different fields in the CORS request policy map onto different CORS response headers, see How a CORS Request Policy Maps to a CORS Response on page 429.

3. To specify a CORS request policy that applies to an individual route:

   **a.** Insert a requestPolicies section after the backend section for the route to which you want the policy to apply. For example:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
```
b. Add the following cors policy to the new requestPolicies section to apply to just this particular route:

```
  "requestPolicies": {
    "cors": {
      "allowedOrigins": [<list-of-origins>],
      "allowedMethods": [<list-of-methods>],
      "allowedHeaders": [<list-of-implicit-headers>],
      "exposedHeaders": [<list-of-exposed-headers>],
      "isAllowCredentialsEnabled": <true|false>,
      "maxAgeInSeconds": <seconds>
    }
  }
}
```

where:

- **"allowedOrigins": [<list-of-origins>]** is a required comma-separated list of origins that are allowed to access the API deployment. For example, "allowedOrigins": ["*", "https://oracle.com"]
- **"allowedMethods": [<list-of-methods>]** is an optional comma-separated list of HTTP methods that are allowed in the actual request to the API deployment. For example, "allowedMethods": ["*", "GET"]
- **"allowedHeaders": [<list-of-implicit-headers>]** is an optional comma-separated list of HTTP headers that are allowed in the actual request to the API deployment. For example, "allowedHeaders": ["opc-request-id", "If-Match"]
- **"exposedHeaders": [<list-of-exposed-headers>]** is an optional comma-separated list of HTTP headers that API clients can access in the API deployment's response to an actual request. For example, "exposedHeaders": ["ETag", "opc-request-id"]
- **"isAllowCredentialsEnabled": <true|false>** is either true or false, indicating whether the actual request to the API deployment can be made using credentials (cookies, authorization headers, or TLS client certificates). If not specified, the default is false.
- **"maxAgeInSeconds": <seconds>** is an integer value, indicating how long (in delta-seconds) the results of a preflight request can be cached by a browser. If not specified, the default is 0.

For example:

```
  "requestPolicies": {
    "cors": {
      "allowedOrigins": ["https://example.com", "https://another.com"],
      "allowedMethods": ["GET", "POST"],
      "allowedHeaders": [
        "Content-Type",
        "Authorization",
        "Accept-Language"
      ],
      "exposedHeaders": [
        "ETag",
        "Location",
        "Vary"
      ],
      "isAllowCredentialsEnabled": true,
      "maxAgeInSeconds": 3600
    }
  }
```

To find out how the different fields in the CORS request policy map onto different CORS response headers, see How a CORS Request Policy Maps to a CORS Response on page 429.

4. Save the JSON file containing the API deployment specification.

5. Use the API deployment specification when you create or update an API deployment in the following ways:
   - by specifying the JSON file in the Console when you select the **Upload an existing API** option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

### How a CORS Request Policy Maps to a CORS Response

The different fields in a CORS request policy map onto different CORS response headers as shown in the table:

<table>
<thead>
<tr>
<th>Field</th>
<th>In pre-flight response</th>
<th>In actual request</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowed Origins</td>
<td>Required?: Yes</td>
<td>Datatype: string[]</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>Default: n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used to return a comma-separated list of origins that are allowed to access the API deployment. Only one origin is allowed by the CORS specification, so in the case of multiple origins the client origin needs to be dynamically checked against the list of allowed values. Values &quot;*&quot; and &quot;null&quot; are allowed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Required?</td>
<td>Datatype</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>cors.host</td>
<td>No</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>cors.methods</td>
<td>No</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>cors.headers</td>
<td>No</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>cors.exposed.headers</td>
<td>No</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>cors.credentials</td>
<td>No</td>
<td>boolean</td>
<td>false</td>
</tr>
<tr>
<td>cors.maxage</td>
<td>No</td>
<td>integer</td>
<td>0</td>
</tr>
</tbody>
</table>

**Notes**

- **allowed Methods**
  - **Access-Control-Allow-Methods**: Used to return a comma-separated list of HTTP methods that are allowed in the actual request to the API deployment. The default of Access-Control-Allow-Methods is to allow through all simple methods, even on preflight requests.

- **allowed Headers**
  - **Access-Control-Allow-Headers**: Used to return a comma-separated list of HTTP headers that are allowed in the actual request to the API deployment.

- **exposed Headers**
  - **Access-Control-Expose-Headers**: Used to return a comma-separated list of HTTP headers that clients can access in the API deployment's response to an actual request. This list of HTTP headers is in addition to the CORS-safelisted response headers.

- **isAllow Credentials Enabled**
  - **Access-Control-Allow-Credentials**: Used to return true or false, indicating whether the actual request to the API deployment can be made using credentials (cookies, authorization headers, or TLS client certificates).

  To allow requests to be made with credentials, set isAllowCredentialsEnabled to true.

- **maxAge InSeconds**
  - **Access-Control-Max-Age**: Used to indicate how long (in delta-seconds) the results of a preflight request can be cached by a browser. Ignored if set to 0.
Adding Authentication and Authorization to API Deployments

You can control access to APIs you deploy to API gateways based on the end user sending a request, and define what it is that they are allowed to do. For the APIs you deploy, you'll typically provide:

- Authentication functionality to determine the end user's identity. Is the end user really who they claim to be?
- Authorization functionality to determine appropriate access for an end user, and grant the necessary permissions. What is the end user allowed to do?

You can add authentication and authorization functionality to API gateways to support:

- HTTP Basic Authentication
- API Key Authentication
- OAuth Authentication and Authorization
- Oracle Identity Cloud Service (IDCS) Authentication

You can add authentication and authorization functionality to an API gateway as follows:

- You can have the API gateway pass an access token included in a request to an authorizer function deployed on Oracle Functions to perform validation (see Using Authorizer Functions to Add Authentication and Authorization to API Deployments on page 431).
- You can have the API gateway itself validate a JSON Web Token (JWT) included in the request with an identity provider (see Using JSON Web Tokens (JWTs) to Add Authentication and Authorization to API Deployments on page 440).

Using Authorizer Functions to Add Authentication and Authorization to API Deployments

You can control access to APIs you deploy to API gateways using an 'authorizer function' (as described in this topic), or using JWTs (as described in Using JSON Web Tokens (JWTs) to Add Authentication and Authorization to API Deployments on page 440).

You can add authentication and authorization functionality to API gateways by writing an 'authorizer function' that:

- Processes request attributes to verify the identity of an end user with an identity provider.
- Determines the operations that the end user is allowed to perform.
- Returns the operations the end user is allowed to perform as a list of 'access scopes' (an 'access scope' is an arbitrary string used to determine access).
- Optionally returns a key-value pair for use by the API deployment. For example, as a context variable for use in an HTTP back end definition (see Adding Context Variables to Policies and HTTP Back End Definitions on page 378).

You then deploy the authorizer function to Oracle Functions. See Creating an Authorizer Function on page 432. For a related Developer Tutorial containing an example authorizer function, see Functions: Validate an API Key with API Gateway.

Having deployed the authorizer function, you enable authentication and authorization for an API deployment by including two different kinds of request policy in the API deployment specification:

- An authentication request policy for the entire API deployment that specifies:
  - The OCID of the authorizer function that you deployed to Oracle Functions that will perform authentication and authorization.
  - The request attributes to pass to the authorizer function.
  - Whether unauthenticated end users can access routes in the API deployment.
- An authorization request policy for each route that specifies the operations an end user is allowed to perform, based on the end user's access scopes as returned by the authorizer function.

You can add authentication and authorization request policies to an API deployment specification by:

- Using the Console.
Prerequisites for Using Authorizer Functions

Before you can enable authentication and authorization for API deployments using authorizer functions:

- An identity provider (for example, Oracle Identity Cloud Service (IDCS), Auth0) must have already been set up, containing access scopes for users allowed to access the API deployment. See the identity provider documentation for more information (for example, the Oracle Identity Cloud Service (IDCS) documentation, the Auth0 documentation).
- An authorizer function must have been deployed to Oracle Functions already, and an appropriate policy must give API gateways access to Oracle Functions. For more information, see Creating an Authorizer Function on page 432.

If you use the Console to include an authentication request policy (rather than by editing a JSON file), you select the authorizer function and the application that contains it from a list.

Note that to use the Console (rather than a JSON file) to define an authentication request policy and specify an authorizer function, your user account must belong to a group that has been given access to the authorizer function by an IAM policy (see Create a Policy to Give API Gateway Users Access to Functions on page 344).

Creating an Authorizer Function

To create an authorizer function:

1. Write code to implement authentication and authorization:
   a. Write code in the authorizer function that accepts the following JSON input from API Gateway:

   ```json
   {
   "type": "TOKEN",
   "token": "<token-value>"
   }
   ```

   where:
   - "type": "TOKEN" indicates that the value being passed to the authorizer function is an auth token.
   - "token": "<token-value>" is the auth token being passed to the authorizer function.

   For example:

   ```json
   {
   "type": "TOKEN",
   "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1nHyDtTwR3SEJ3z489..."
   }
   ```

   b. Write code in the authorizer function that returns the following JSON to API Gateway as an HTTP 200 response when the access token has been successfully verified:

   ```json
   { 
   "active": true,
   "principal": "<user-principal>",
   "scope": ["<scopes>"],
   "clientId": "<client-id>"
   }
   ```
where:

- "active": true indicates the access token originally passed to the authorizer function has been successfully verified.
- "principal": "<user-principal>" is the user or application obtained by the authorizer function from the identity provider.
- "scope": ["<scopes>"] is a comma-delimited list of strings that are the access scopes obtained by the authorizer function from the identity provider.
- "clientId": "<client-id>" is optionally the requestor's host (for example, the hostname or the client IP). Returning a clientId is not required.
- "expiresAt": "<date-time>" is a date-time string in ISO-8601 format indicating when the access token originally passed to the authorizer function will expire. This value is used when determining how long to cache results after calling the authorizer function.
- "context": {"<key>": "<value>", ... } is an optional comma-delimited list of key-value pairs in JSON format to return to API Gateway. The authorizer function can return any key-value pair for use by the API deployment (for example, the username or email address of the end user). For more information about using the value in the key-value pair returned by an authorizer function as a context variable in an HTTP back end definition, see Adding Context Variables to Policies and HTTP Back End Definitions on page 378.

For example:

```json
{
    "active": true,
    "principal": "https://example.com/users/jdoe",
    "scope": ["list:hello", "read:hello", "create:hello", "update:hello",
               "delete:hello", "someScope"],
    "clientId": "host123",
    "expiresAt": "2019-05-30T10:15:30+01:00",
    "context": {
        "email": "john.doe@example.com"
    }
}
```

c. Write code that returns the following JSON to API Gateway as an HTTP 5xx response if token verification is unsuccessful, or in the event of an error in the authorizer function or in Oracle Functions:

```json
{
    "active": false,
    "expiresAt": "<date-time>",
    "context": {
        "<key>": "<value>", ...
    },
    "wwwAuthenticate": "<directive>"
}
```

where:

- "active": false indicates the access token originally passed to the authorizer function has not been successfully verified.
- "expiresAt": "<date-time>" is a date-time string in ISO-8601 format indicating when the access token originally passed to the authorizer function will expire.
- "context": {"<key>": "<value>", ... } is an optional comma-delimited list of key-value pairs in JSON format to return to API Gateway. The authorizer function can return any key-value pair
(for example, the username or email address of the end user). Returning context key-value pairs is not required.

- "wwwAuthenticate": "<directive>" is the value of the WWW-Authenticate header to be returned by the authorizer function if verification fails, indicating the type of authentication that is required (such as Basic or Bearer). API Gateway returns the WWW-Authenticate header in the response to the API client, along with a 401 status code. For example, "wwwAuthenticate": "Bearer realm=\"example.com\"". For more information, see RFC 2617 HTTP Authentication: Basic and Digest Access Authentication.

For example:

```json
{
  "active": false,
  "expiresAt": "2019-05-30T10:15:30+01:00",
  "context": {
    "email": "james.doe@example.com"
  },
  "wwwAuthenticate": "Bearer realm=\"example.com\"
}
```

For a related Developer Tutorial containing an example authorizer function, see Functions: Validate an API Key with API Gateway.

2. Build a Docker image from the code, push the Docker image to a Docker registry, and create a new function in Oracle Functions based on the image. You can do this in different ways:

- You can use the Fn Project CLI command `fn deploy` to build a new Docker image, push the image to the Docker registry, and create a new function in Oracle Functions based on the image. See Creating and Deploying Functions on page 2063.

- You can use Docker commands to build the image and push it to the Docker registry, and then use the Fn Project CLI command `fn create function` (or the `CreateFunction` API operation) to create a new function in Oracle Functions based on the image. See Creating Functions from Existing Docker Images on page 2066.

3. Make a note of the OCID of the function you create in Oracle Functions. For example, `ocid1.fnfunc.oc1.phx.aaaaaaaaac2______kg6fq`

4. If one doesn't exist already, create an Oracle Cloud Infrastructure policy and specify a policy statement to give API gateways access to function-related resources. The policy enables API deployments on those API gateways to invoke the authorizer function. For more information, see Create a Policy to Give API Gateways Access to Functions on page 345

**Using the Console to Add Authentication and Authorization Request Policies**

To add authentication and authorization request policies to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the **From Scratch** option, and enter details on the **Basic Information** page.

For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.
2. In the API Request Policies section of the Basic Information page, click the Add button beside Authentication and specify:

- **Authentication Type**: Select Custom.
- **Application in <compartment-name>**: The name of the application in Oracle Functions that contains the authorizer function. You can select an application from a different compartment.
- **Function Name**: The name of the authorizer function in Oracle Functions.
- **Authentication Token**: Whether the access token is contained in a request header or a query parameter.
- **Authentication Token Value**: Depending on whether the access token is contained in a request header or a query parameter, specify:
  - **Header Name**: If the access token is contained in a request header, enter the name of the header.
  - **Parameter Name**: If the access token is contained in a query parameter, enter the name of the query parameter.
- **Enable Anonymous Access**: Whether unauthenticated (that is, anonymous) end users can access routes in the API deployment. By default, this option is not selected. If you never want anonymous users to be able to access routes, don't select this option. Note that if you do select this option, you also have to explicitly specify every route to which anonymous access is allowed by selecting Anonymous as the Authorization Type in each route's authorization policy.

3. Click Save Changes, and then click Next to enter details for individual routes in the API deployment on the Routes page. To specify an authorization policy that applies to an individual route, click Show Route Request Policies, click the Add button beside Authorization, and specify:

- **Authorization Type**: How to grant access to the route. Specify:
  - **Any**: Only grant access to end users that have been successfully authenticated, provided the authorizer function has also returned one of the access scopes you specify in the Allowed Scope field. In this case, the authentication policy's Enable Anonymous Access option has no effect.
  - **Anonymous**: Grant access to all end users, even if they have not been successfully authenticated by the authorizer function. In this case, you must have selected the authentication policy's Enable Anonymous Access option.
  - **Authentication only**: Only grant access to end users that have been successfully authenticated by the authorizer function. In this case, the authentication policy's Enable Anonymous Access option has no effect.

- **Allowed Scope**: If you selected Any as the Authorization Type, enter a comma-delimited list of one or more strings that correspond to access scopes returned by the authorizer function. Access will only be granted to end users that have been successfully authenticated if the authorizer function returns one of the access scopes you specify. For example, read:hello

---

**Note:**

If you don't include an authorization policy for a particular route, access is granted as if such a policy does exist and Authorization Type is set to Authentication only. In other words, regardless of the setting of the authentication policy's Enable Anonymous Access option:

- only authenticated end users can access the route
- all authenticated end users can access the route regardless of access scopes returned by the authorizer function
- anonymous end users cannot access the route

4. Click Save Changes, and then click Next to review the details you entered for the API deployment.
5. Click Create or Save Changes to create or update the API deployment.
6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

**Editing a JSON File to Add Authentication and Authorization Request Policies**

To add authentication and authorization request policies to an API deployment specification in a JSON file:
1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add authentication and authorization functionality, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

At a minimum, the API deployment specification will include a routes section containing:

- A path. For example, /hello
- One or more methods. For example, GET
- A definition of a back end. For example, a URL, or the OCID of a function in Oracle Functions.

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      }
    }
  ]
}
```

2. Add an authentication request policy that applies to all routes in the API deployment specification:

   a. Insert a requestPolicies section before the routes section, if one doesn't exist already. For example:

   ```json
   {
     "requestPolicies": {},
     "routes": [
       {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
           "type": "ORACLE_FUNCTIONS_BACKEND",
           "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
       }
     ]
   }
   ```

   b. Add the following authentication policy to the new requestPolicies section.

   ```json
   {
     "requestPolicies": {
       "authentication": {
         "type": "<type-value>",
         "isAnonymousAccessAllowed": <true|false>,
         "functionId": "<function-ocid>",
         "<tokenHeader>|"tokenQueryParam": <"<token-header-name>|"<token-query-param-name>">"
       }
     },
     "routes": [
       {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
           "type": "ORACLE_FUNCTIONS_BACKEND",
           "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         }
       }
     ]
   }
   ```
where:

- `<type-value>` is the authentication type. To use an authorizer function for authentication, specify `CUSTOM_AUTHENTICATION`.
- "isAnonymousAccessAllowed": `<true|false>` optionally indicates whether unauthenticated (that is, anonymous) end users can access routes in the API deployment specification. If you never want anonymous end users to be able to access routes, set this property to `false`. If you don’t include this property in the authentication policy, the default of `false` is used. Note that if you do include this property and set it to `true`, you also have to explicitly specify every route to which anonymous access is allowed by setting the `type` property to "ANONYMOUS" in each route’s authorization policy.
- `<function-ocid>` is the OCID of the authorizer function deployed to Oracle Functions.
- `<"tokenHeader"|"tokenQueryParam">: `<"token-header-name"|"token-query-param-name">` indicates whether it is a request header that contains the access token (and if so, the name of the header), or a query parameter that contains the access token (and if so, the name of the query parameter). Note that you can specify either "tokenHeader": "<token-header-name>" or "tokenQueryParam": "<token-query-param-name>", but not both.

For example, the following authentication policy specifies an OCI function that will validate the access token in the Authorization request header:

```json
{
    "requestPolicies": {
        "authentication": {
            "type": "CUSTOM_AUTHENTICATION",
            "isAnonymousAccessAllowed": false,
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaac2_____kg6fq",
            "tokenHeader": "Authorization"
        }
    },
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        }
    ]
}
```

3. Add an authorization request policy for each route in the API deployment specification:

   a. Insert a `requestPolicies` section after the first route’s `backend` section, if one doesn't exist already. For example:

```json
{
    "requestPolicies": {
        "authentication": {
            "type": "CUSTOM_AUTHENTICATION",
            "isAnonymousAccessAllowed": false,
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaac2_____kg6fq",
            "tokenHeader": "Authorization"
        }
    },
    "routes": [
```
b. Add the following authorization policy to the requestPolicies section:

```json
{
    "requestPolicies": {
        "authentication": {
            "type": "CUSTOM_AUTHENTICATION",
            "isAnonymousAccessAllowed": false,
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaac2______kg6fq",
            "tokenHeader": "Authorization"
        }
    },
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            },
            "requestPolicies": {
                "authorization": {
                    "type": <"AUTHENTICATION_ONLY"|"ANY_OF"|"ANONYMOUS">,
                    "allowedScope": [ "<scope>" ]
                }
            }
        }
    ]
}
```

where:

- "type": <"AUTHENTICATION_ONLY"|"ANY_OF"|"ANONYMOUS"> indicates how to grant access to the route:
  - "AUTHENTICATION_ONLY": Only grant access to end users that have been successfully authenticated. In this case, the "isAnonymousAccessAllowed" property in the API deployment specification's authentication policy has no effect.
  - "ANY_OF": Only grant access to end users that have been successfully authenticated, provided the authorizer function has also returned one of the access scopes you specify in the allowedScope property. In this case, the "isAnonymousAccessAllowed" property in the API deployment specification's authentication policy has no effect.
  - "ANONYMOUS": Grant access to all end users, even if they have not been successfully authenticated. In this case, you must explicitly set the "isAnonymousAccessAllowed" property to true in the API deployment specification's authentication policy.
  - "allowedScope": [ "<scope>" ] is a comma-delimited list of one or more strings that correspond to access scopes returned by the authorizer function. In this case, you must set the type property to "ANY_OF" (the "allowedScope" property is ignored if the type property is set to...
"AUTHENTICATION_ONLY" or "ANONYMOUS"). Also note that if you specify more than one scope, access to the route is granted if any of the scopes you specify is returned by the authorizer function.

For example, the following request policy defines a /hello route that only allows authenticated end users with the read:hello scope to access it:

```json
{
   "requestPolicies": {
      "authentication": {
         "type": "CUSTOM_AUTHENTICATION",
         "isAnonymousAccessAllowed": false,
         "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaac2______kg6fq",
         "tokenHeader": "Authorization"
      }
   },
   "routes": [
      {
         "path": "/hello",
         "methods": ["GET"],
         "backend": {
            "type": "ORACLE_FUNCTIONS_BACKEND",
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
         },
         "requestPolicies": {
            "authorization": {
               "type": "ANY_OF",
               "allowedScope": [ "read:hello" ]
            }
         }
      }
   ]
}
```

c. Add an authorization request policy for all remaining routes in the API deployment specification.

**Note:**

If you don't include an authorization policy for a particular route, access is granted as if such a policy does exist and the type property is set to "AUTHENTICATION_ONLY". In other words, regardless of the setting of the isAnonymousAccessAllowed property in the API deployment specification's authentication policy:

- only authenticated end users can access the route
- all authenticated end users can access the route regardless of access scopes returned by the authorizer function
- anonymous end users cannot access the route

4. Save the JSON file containing the API deployment specification.

5. Use the API deployment specification when you create or update an API deployment in the following ways:

   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).
Using JSON Web Tokens (JWTs) to Add Authentication and Authorization to API Deployments

You can control access to APIs you deploy to API gateways using JSON Web Tokens (JWTs) as described in this topic, or using an 'authorizer function' (as described in Using Authorizer Functions to Add Authentication and Authorization to API Deployments on page 431).

A JWT is a JSON-based access token sent in an HTTP request from an API client to a resource. JWTs are issued by identity providers (for example, Oracle Identity Cloud Service (IDCS), Auth0, Okta). When an API client attempts to access a protected resource, it must include a JWT. The resource validates the JWT with an authorization server using a corresponding public verification key, either by invoking a validation end-point on the authorization server or by using a local verification key provided by the authorization server.

A JWT comprises:

- A header, which identifies the type of token and the cryptographic algorithm used to generate the signature.
- A payload, containing claims about the end user's identity, and the properties of the JWT itself. A claim is a key value pair, where the key is the name of the claim. A payload is recommended (although not required) to contain certain reserved claims with particular names, such as expiration time (exp), audience (aud), issuer (iss), and not before (nbf). A payload can also contain custom claims with user-defined names.
- A signature, to validate the authenticity of the JWT (derived by base64 encoding the header and the payload).

You enable an API deployment to use JWTs for authentication and authorization by including two different kinds of request policy in the API deployment specification:

- An authentication request policy for the entire API deployment that specifies the use of JWTs, including how to validate them and whether unauthenticated end users can access routes in the API deployment.
- An authorization request policy for each route that specifies the operations an end user is allowed to perform, optionally based on values specified for the scope claim in the JWT.

Before an end user can access an API deployment that uses JWTs for authentication and authorization, they must obtain a JWT from an identity provider.

When calling an API deployed on an API gateway, the API client provides the JWT as a query parameter or in the header of the request. The API gateway validates the JWT using a corresponding public verification key provided by the issuing identity provider. Using the API deployment's authentication request policy, you can configure how the API gateway validates JWTs:

- You can configure the API gateway to retrieve public verification keys from the identity provider at runtime. In this case, the identity provider acts as the authorization server.
- You can configure the API gateway in advance with public verification keys already issued by an identity provider (referred to as 'static keys'), enabling the API gateway to verify JWTs locally at runtime without having to contact the identity provider. The result is faster token validation.

As well as using the public verification key from the issuing identity provider to verify the authenticity of a JWT, you can specify that reserved claims in the JWT's payload must have particular values before the API gateway considers the JWT to be valid. By default, API gateways validate JWTs using the expiration (exp), audience (aud), and issuer (iss) claims, along with the not before (nbf) claim if present. You can also specify acceptable values for custom claims. See Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI on page 451.

When the JWT has been validated, the API gateway extracts claims from the JWT's payload as key value pairs and saves them as records in the request.auth context table for use by the API deployment. For example, as context variables for use in an HTTP back end definition (see Adding Context Variables to Policies and HTTP Back End Definitions on page 378). If the JWT's payload contains the scope claim, you can use the claim's values in authorization request policies for individual routes to specify the operations an end user is allowed to perform.

You can add authentication and authorization request policies to an API deployment specification by:

- Using the Console.
- Editing a JSON file.
Prerequisites for using JWTs

Before you can enable authentication and authorization for API deployments using JWTs:

- An identity provider (for example, Oracle Identity Cloud Service (IDCS), Auth0) must have already been set up to issue JWTs for users allowed to access the API deployment.
- If you want to use custom claims in authorization policies, the identity provider must be set up to add the custom claims to the JWTs it issues.

See the identity provider documentation for more information (for example, the Oracle Identity Cloud Service (IDCS) documentation, the Auth0 documentation).

Also note that to validate the JWT using a corresponding public verification key provided by the issuing identity provider:

- the signing algorithm used to generate the JWT's signature must be one of RS256, RS384, or RS512
- the public verification key must have a minimum length of 2048 bits and must not exceed 4096 bits

Using the Console to Add Authentication and Authorization Request Policies

To add authentication and authorization request policies to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.
   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. In the API Request Policies section of the Basic Information page, click the Add button beside Authentication and specify:

   - **Authentication Type**: Select JWT.
   - **Authentication Token**: Whether the JWT is contained in a request header or a query parameter.
   - **Authentication Token Value**: Depending on whether the JWT is contained in a request header or a query parameter, specify:
     - **Header Name** and **Authentication Scheme**: If the JWT is contained in a request header, enter the name of the header (for example Authorization), and the HTTP authentication scheme (only Bearer is currently supported).
     - **Parameter Name**: If the JWT is contained in a query parameter, enter the name of the query parameter.
   - **Enable Anonymous Access**: Whether unauthenticated (that is, anonymous) end users can access routes in the API deployment. By default, this option is not selected. If you never want anonymous end users to be able to access routes, don't select this option. Note that if you do select this option, you also have to explicitly specify every route to which anonymous access is allowed by selecting Anonymous as the Authorization Type in each route's authorization policy.

3. In the Issuers section, specify values that are allowed in the issuer (iss) claim of a JWT being used to access the API deployment:

   - **Allowed Issuers**: Specify the URL (or a text string) for an identity provider that is allowed in the issuer (iss) claim of a JWT to be used to access the API deployment. For example, to enable a JWT issued by the Oracle Identity Cloud Service (IDCS) to be used to access the API deployment, enter https://identity.oraclecloud.com/. See Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI on page 451.
   - **Another Issuer**: Click to add additional identity providers (up to a maximum of five).

4. In the Audiences section, specify values that are allowed in the audience (aud) claim of a JWT being used to access the API deployment:

   - **Allowed Audiences**: Specify a value that is allowed in the audience (aud) claim of a JWT to identify the intended recipient of the token. For example, the audience could be, but need not be, the API gateway's hostname. See Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI on page 451.
   - **Another Audience**: Click to add additional audiences (up to a maximum of five).
5. In the **Public Keys** section of the Authentication Policy window, specify how you want the API gateway to validate JWTs using public verification keys:

   - To configure the API gateway to validate JWTs by retrieving public verification keys from the identity provider at runtime, select **Remote JWKS** from the **Type** list and specify:

     - **URI**: The URI from which to retrieve the JSON Web Key Set (JWKS) to use to verify the signature on JWTs. For example, https://www.somejwksprovider.com/oauth2/v3/certs. For more information about the URI to specify, see **Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI** on page 451.

   Note the following:

     - The URI must be routable from the subnet containing the API gateway on which the API is deployed.
     - URIs that require authentication or authorization to return the JWKS are not supported.
     - If the API gateway fails to retrieve the JWKS, all requests to the API deployment will return an HTTP 500 response code. Refer to the API gateway's execution log for more information about the error (see **Adding Logging to API Deployments** on page 397).
     - Certain key parameters must be present in the JWKS to verify the JWT's signature (see **Key Parameters Required to Verify JWT Signatures** on page 452).

     - **Cache Duration in Hours**: The number of hours (between 1 and 24) the API gateway is to cache the JWKS set after retrieving it.

     - **Disable SSL Verification**: Whether to disable SSL verification when communicating with the identity provider. By default, this option is not selected. Oracle recommends not selecting this option because it can compromise JWT validation. API Gateway trusts certificates from multiple Certificate Authorities issued for Oracle Identity Cloud Service (IDCS), Auth0, Okta.

   - To configure the API gateway to validate JWTs with public verification keys already issued by an identity provider (enabling the API gateway to verify JWTs locally without having to contact the identity provider), select **Static Keys** from the **Type** list and specify:

     - **Key ID**: The identifier of the static key used to sign the JWT. The value must match the `kid` claim in the JWT header. For example, `master_key`.

     - **Format**: The format of the static key, as either a JSON Web Key or a PEM-encoded Public Key.

       - **JSON Web Key**: If the static key is a JSON Web Key, paste the key into this field. For example:

         ```
         {
           "kty": "RSA",
           "n": "0vx7agoebGc...KnqDKgw",
           "e": "AQAB",
           "alg": "RS256",
           "use": "sig"
         }
         ```

         Note that certain parameters must be present in the static key to verify the JWT's signature (see **Key Parameters Required to Verify JWT Signatures** on page 452). Also note that RSA is currently the only supported key type (`kty`).

       - **PEM-Encoded Public Key**: If the static key is a PEM-encoded public key, paste the key into this field. For example:

         ```
         -----BEGIN PUBLIC KEY-----
         XsE1CeYgglwW/KAhSSNRVdD60q1XYMWHOxZsFDZCLWxXxKMXCIyurVnrZ8x3oSmxwL5/8qVudomoP+yycJ2gWPIqgsZcQRheJWxVC5ep0MeEHlvLnEvC19utpAnjrsZCQ7plfZVFX7ORvezwqQhBw7wA2
         ```
6. (Optional) Click Show Advanced Options to specify a time difference to take into account when validating JWTs, and to specify additional claims in JWTs to process:

- **Maximum Clock Skew in Seconds:** (Optional) The maximum time difference between the system clocks of the identity provider that issued a JWT and the API gateway. The value you enter here is taken into account when the API gateway validates the JWT to determine whether it is still valid, using the not before (nbf) claim (if present) and the expiration (exp) claim in the JWT. The minimum (and default) is 0, the maximum is 120.

- **Verify Claims:** (Optional) In addition to the values for the audience `aud` and issuer `iss` claims that you already specified, you can specify names and values for one or more additional claims to validate in a JWT. Note that any key names and values you enter are simply handled as strings, and must match exactly with names and values in the JWT. Pattern matching and other datatypes are not supported. Also note that you can specify a claim can or must appear in the JWT without specifying a value for the claim by entering the claim's name in the **Claim Key** field, leaving the **Claim Values** field blank, and selecting **Required**:

  - **Claim Key:** (Optional) Specify the name of a claim that can be, or must be, included in a JWT. If the claim must be included in the JWT, select **Required**. The claim name you specify can be a reserved claim name such as the subject (`sub`) claim, or a custom claim name issued by a particular identity provider.

  - **Claim Values:** (Optional) Specify an acceptable value for the claim in the **Claim Key** field. Click the plus sign (+) to enter another acceptable value. If you specify one or more acceptable values for the claim, the API gateway validates that the claim has one of the values you specify.

  - **Required:** Select if the claim in the **Claim Key** field must be included in the JWT.

- **Another Claim:** Click to add additional claims (up to a maximum of ten).

7. Click **Save Changes**, and then click **Next** to enter details for individual routes in the API deployment on the **Routes** page. To specify an authorization policy that applies to an individual route, click **Show Route Request Policies**, click the **Add** button beside **Authorization**, and specify:

- **Authorization Type:** How to grant access to the route. Specify:
  
  - **Any:** Only grant access to end users that have been successfully authenticated, provided the JWT has a `scope` claim that includes at least one of the access scopes you specify in the **Allowed Scope** field. In this case, the authentication policy's **Enable Anonymous Access** option has no effect.
  
  - **Anonymous:** Grant access to all end users, even if they have not been successfully authenticated using the JWT. In this case, you must have selected the authentication policy's **Enable Anonymous Access** option.

- **Authentication only:** Only grant access to end users that have been successfully authenticated using the JWT. In this case, the authentication policy's **Enable Anonymous Access** option has no effect.

- **Allowed Scope:** If you selected **Any** as the **Authorization Type**, enter a comma-delimited list of one or more strings that correspond to access scopes in the JWT. Access will only be granted to end users that have been successfully authenticated if the JWT has a `scope` claim that includes one of the access scopes you specify. For example, `read:hello`

8. Click **Save Changes**, and then click **Next** to review the details you entered for the API deployment.
9. Click **Create** or **Save Changes** to create or update the API deployment.

10. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

### Editing a JSON File to Add Authentication and Authorization Request Policies

To add authentication and authorization request policies to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add authentication and authorization functionality, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

At a minimum, the API deployment specification will include a `routes` section containing:

- A path. For example, `/hello`
- One or more methods. For example, `GET`
- A definition of a back end. For example, a URL, or the OCID of a function in Oracle Functions.

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            }
        }
    ]
}
```

2. Add an **authentication** request policy that applies to all routes in the API deployment specification:

   a. Insert a `requestPolicies` section before the `routes` section, if one doesn’t exist already. For example:

   ```json
   {
       "requestPolicies": {},
       "routes": [
           {
               "path": "/hello",
               "methods": ["GET"],
               "backend": {
                   "type": "ORACLE_FUNCTIONS_BACKEND",
                   "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
               }
           }
       ]
   }
   ```

   b. Add the following **authentication** policy to the new `requestPolicies` section.

   ```json
   {
       "requestPolicies": {
           "authentication": {
               "type": "<type-value>",
               "isAnonymousAccessAllowed": <true|false>,
               "issuers": ["<issuer-url>", "<issuer-url>"],
               "<tokenHeader>"|"<tokenQueryParam>": "<token-header-name>"|"<token-query-param-name>",
               "tokenAuthScheme": "<authentication-scheme>",
               ...
           }
       }
   }
   ```
"audiences": ["<intended-audience>"],
"publicKeys": {
  "type": "<REMOTE_JWKS" | "STATIC_KEYS">,
  <public-key-config>
},
"verifyClaims": [ 
  {"key": "<claim-name>",&
  "values": ["<acceptable-value>"],
  "isRequired": <true|false>
  }
],
"maxClockSkewInSeconds": <seconds-difference>
}
},
"routes": [ 
  {"path": "/hello",
  "methods": ["GET"],
  "backend": { 
    "type": "ORACLE_FUNCTIONS_BACKEND",
    "functionId": "ocidl.fnfunc.ocl.phx.aaaaaaaaab______xmq"
  }
  }
]
}

where:

- `<type-value>` is the authentication type. To use JWTs for authentication, specify JWT_AUTHENTICATION.
- "isAnonymousAccessAllowed": <true|false> optionally indicates whether unauthenticated (that is, anonymous) end users can access routes in the API deployment specification. If you never want anonymous end users to be able to access routes, set this property to false. If you don’t include this property in the authentication policy, the default of false is used. Note that if you do include this property and set it to true, you also have to explicitly specify every route to which anonymous access is allowed by setting the type property to "ANONYMOUS" in each route's authorization policy.
- `<issuer-url>` is the URL (or a text string) for an identity provider that is allowed in the issuer (iss) claim of a JWT to be used to access the API deployment. For example, to enable a JWT issued by the Oracle Identity Cloud Service (IDCS) to be used to access the API deployment, enter https://identity.oraclecloud.com/. You can specify one or multiple identity providers (up to a maximum of five). See Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI on page 451.
- "<"tokenHeader"|"tokenQueryParam">: <"token-header-name">|"<token-query-param-name>" indicates whether it is a request header that contains the JWT (and if so, the name of the header), or a query parameter that contains the access token (and if so, the name of the query parameter). Note that you can specify either "tokenHeader": "<token-header-name>" or "tokenQueryParam": "<token-query-param-name">", but not both.
- <tokenAuthScheme> is the name of the authentication scheme to use if the JWT is contained in a request header. For example, "Bearer".
- `<intended-audience>` is a value that is allowed in the audience (aud) claim of a JWT to identify the intended recipient of the token. For example, the audience could be, but need not be, the API gateway's hostname. You can specify one audience or multiple audiences (up to a maximum of five). See Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI on page 451.
- "type": "<REMOTE_JWKS" | "STATIC_KEYS" indicates how you want the API gateway to validate JWTs using public verification keys. Specify REMOTE_JWKS to configure the API gateway to retrieve public verification keys from the identity provider at runtime. Specify STATIC_KEYS to
configure the API gateway with public verification keys already issued by an identity provider (enabling
the API gateway to verify JWTs locally without having to contact the identity provider).

- `<public-key-config>` provides the details of JWT validation, according to whether you specified
  "REMOTE_JWKS" or "STATIC_KEYS" as the value of "type": as follows:

  - If you specified "type": "REMOTE_JWKS" to configure the API gateway to validate JWTs by
    retrieving public verification keys from the identity provider at runtime, provide details as follows:

```
"publicKeys": {
  "type": "REMOTE_JWKS",
  "uri": "<uri-for-jwks>",
  "maxCacheDurationInHours": <cache-time>,
  "isSslVerifyDisabled": <true|false>
}
```

  where:

  - "uri": "<uri-for-jwks>" specifies the URI from which to retrieve the JSON Web Key
    Set (JWKS) to use to verify the signature on JWTs. For more information about the URI to specify,
    see Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI on page 451.
    Note the following:
    - The URI must be routable from the subnet containing the API gateway on which the API is
      deployed.
    - URIs that require authentication or authorization to return the JWKS are not supported.
    - If the API gateway fails to retrieve the JWKS, all requests to the API deployment will return an
      HTTP 500 response code. Refer to the API gateway's execution log for more information about
      the error (see Adding Logging to API Deployments on page 397).
    - Certain key parameters must be present in the JWKS to verify the JWT's signature (see Key
      Parameters Required to Verify JWT Signatures on page 452).
    - "maxCacheDurationInHours": <cache-time> specifies the number of hours (between 1
      and 24) the API gateway is to cache the JWKS set after retrieving it.
    - "isSslVerifyDisabled": <true|false> indicates whether to disable SSL verification
      when communicating with the identity provider. Oracle recommends not setting this option to
      true because it can compromise JWT validation. API Gateway trusts certificates from multiple
      Certificate Authorities issued for Oracle Identity Cloud Service (IDCS), Auth0, and Okta.

    For example:

```
"publicKeys": {
  "type": "REMOTE_JWKS",
  "uri": "https://www.somejwksprovider.com/oauth2/v3/certs",
  "maxCacheDurationInHours": 3,
  "isSslVerifyDisabled": false
}
```

- If you specified "type": "STATIC_KEYS", the details to provide depend on the format of the key
  already issued by the identity provider:

  - If the static key is a JSON Web Key, specify "format": "JSON_WEB_KEY", specify the
    identifier of the static key used to sign the JWT as the value of the "kid" parameter, and provide
    values for other parameters to verify the JWT's signature.

    For example:

```
"publicKeys": {
  "type": "STATIC_KEYS",
  "keys": [ 
  { "format": "JSON_WEB_KEY",
```

Oracle Cloud Infrastructure User Guide 446
"kid": "master_key",
"kty": "RSA",
"n": "0vx7agoebGc...KnqDKgw",
"e": "AQAB",
"alg": "RS256",
"use": "sig"
}
]

Note that certain parameters must be present in the static key to verify the JWT's signature (see Key Parameters Required to Verify JWT Signatures on page 452). Also note that RSA is currently the only supported key type (kty).

- If the static key is a PEM-encoded public key, specify "format": "PEM", specify the identifier of the static key used to sign the JWT as the value of "kid", and provide the key as the value of "key".

For example:

```json
"publicKeys": {
  "type": "STATIC_KEYS",
  "keys": [
    {
      "format": "PEM",
      "kid": "master_key"
      "key": "-----BEGIN PUBLIC KEY-----XsEiCeYgg1wW/KAhSSNRVd60QlXWzGh0hXzSFD2ClfdWxXKmZC1MvVr5rB1zmFEXnFmcsO2mxw1L5/8qQudomoP+yycJ2gWPiggs2cQRheJWxVC5ep0MeEHlvLnEvCi9utpAnjrsZCQ7p1fZVFJ7XORvezwqQhBfYzwEND PUBLIC KEY-----
    }
  ]
}
```

Note that the -----BEGIN PUBLIC KEY----- and -----END PUBLIC KEY----- markers are required.

- **verifyClaims** optionally specifies additional claim names and values for one or more additional claims to validate in a JWT (up to a maximum of ten).
  - "key": "<claim-name>" is the name of a claim that can be, or must be, included in a JWT. The claim name you specify can be a reserved claim name such as the subject (sub) claim, or a custom claim name issued by a particular identity provider.
  - "values": ["<acceptable-value>", "<acceptable-value>"], (optionally) indicates one or more acceptable values for the claim.
  - "isRequired": <true|false> indicates whether the claim must be included in the JWT.

Note that any key names and values you enter are simply handled as strings, and must match exactly with names and values in the JWT. Pattern matching and other datatypes are not supported.

- **maxClockSkewInSeconds**: <seconds-difference> optionally specifies the maximum time difference between the system clocks of the identity provider that issued a JWT and the API gateway. The value you specify is taken into account when the API gateway validates the JWT to determine whether it is still valid, using the not before (nbf) claim (if present) and the expiration (exp) claim in the JWT. The minimum (and default) is 0, the maximum is 120.

For example, the following authentication policy specifies an OCI function that will validate the access token in the Authorization request header:

```json
{
  "requestPolicies": {
    "authentication": {
      "type": "JWT_AUTHENTICATION",
      "isAnonymousAccessAllowed": false,
      "issuers": ["https://identity.oraclecloud.com/"],
      "verifyClaims": {
        "key": "custom-claim",
        "values": ["accepted-value-1", "accepted-value-2"],
        "isRequired": true
      }
    }
  }
}
```
3. Add an authorization request policy for each route in the API deployment specification:

   a. Insert a requestPolicies section after the first route's backend section, if one doesn't exist already. For example:

```json
"requestPolicies": {
  "authentication": {
    "type": "JWT_AUTHENTICATION",
    "isAnonymousAccessAllowed": false,
    "issuers": ["https://identity.oraclecloud.com/"],
    "tokenHeader": "Authorization",
    "tokenAuthScheme": "Bearer",
    "audiences": ["api.dev.io"],
    "publicKeys": {
      "type": "STATIC_KEYS",
      "keys": [
        {
          "format": "JSON_WEB_KEY",
          "kid": "master_key",
          "kty": "RSA",
          "n": "0vx7agoebGc...KnqDKgw",
          "e": "AQAB",
          "alg": "RS256",
          "use": "sig"
        }
      ]
    },
    "verifyClaims": {
      "key": "is_admin",
      "values": ["service:app", "read:hello"],
      "isRequired": true
    }
  },
  "maxClockSkewInSeconds": 10
}
```

b. Add the following authorization policy to the requestPolicies section:

```
{
  "requestPolicies": {
    "authentication": {
      "type": "JWT_AUTHENTICATION",
      "isAnonymousAccessAllowed": false,
      "issuers": ["https://identity.oraclecloud.com/"]
    },
    "verifyClaims": [
      {
        "key": "is_admin",
        "values": ["service:app", "read:hello"],
        "isRequired": true
      }
    ],
    "maxClockSkewInSeconds": 10
  },
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {}
    }
  ]
}
```
API Gateway

"methods": ["GET"],
"backend": {
  "type": "ORACLE_FUNCTIONS_BACKEND",
  "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaab________xmq"
},
"requestPolicies": {
  "authorization": {
    "type": "<"AUTHENTICATION_ONLY"|"ANY_OF"|"ANONYMOUS">,
    "allowedScope": [ "<scope>" ]
  }
}
}

where:

- "type": "<"AUTHENTICATION ONLY"|"ANY_OF"|"ANONYMOUS""> indicates how to grant access to the route:
  - "AUTHENTICATION ONLY": Only grant access to end users that have been successfully authenticated. In this case, the "isAnonymousAccessAllowed" property in the API deployment specification's authentication policy has no effect.
  - "ANY_OF": Only grant access to end users that have been successfully authenticated, provided the JWT's scope claim includes one of the access scopes you specify in the allowedScope property. In this case, the "isAnonymousAccessAllowed" property in the API deployment specification's authentication policy has no effect.
  - "ANONYMOUS": Grant access to all end users, even if they have not been successfully authenticated. In this case, you must explicitly set the "isAnonymousAccessAllowed" property to true in the API deployment specification's authentication policy.

- "allowedScope": [ "<scope>" ] is a comma-delimited list of one or more strings that correspond to access scopes included in the JWT's scope claim. In this case, you must set the type property to "ANY_OF" (the "allowedScope" property is ignored if the type property is set to "AUTHENTICATION ONLY" or "ANONYMOUS"). Also note that if you specify more than one scope, access to the route is granted if any of the scopes you specify is included in the JWT's scope claim.

For example, the following request policy defines a /hello route that only allows authenticated end users with the read:hello scope to access it:

```json
{
  "requestPolicies": {
    "authentication": {
      "type": "JWT_AUTHENTICATION",
      "isAnonymousAccessAllowed": false,
      "issuers": ["https://identity.oraclecloud.com/"],
      "tokenHeader": "Authorization",
      "tokenAuthScheme": "Bearer",
      "audiences": ["api.dev.io"],
      "publicKeys": {
        "type": "STATIC_KEYS",
        "keys": [
          { "format": "JSON_WEB_KEY",
            "kid": "master_key",
            "kty": "RSA",
            "n": "0vx7agoebGc...KnqDKgw",
            "e": "AQAB",
            "alg": "RS256",
            "use": "sig"
          }
        ]
      }
    }
  }
}
```
API Gateway

```
},

"verifyClaims": [

  {
    "key": "is_admin",
    "values": ["service:app", "read:hello"],
    "isRequired": true
  }
],

"maxClockSkewInSeconds": 10
}
]

"routes": [

  {
    "path": "/hello",
    "methods": ["GET"],
    "backend": {
      "type": "ORACLE_FUNCTIONS_BACKEND",
      "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
    },
    "requestPolicies": {
      "authorization": {
        "type": "ANY_OF",
        "allowedScope": ["read:hello"]
      }
    }
  }
]
}
```

c. Add an authorization request policy for all remaining routes in the API deployment specification.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you don't include an authorization policy for a particular route, access is granted as if such a policy does exist and the type property is set to &quot;AUTHENTICATION_ONLY&quot;. In other words, regardless of the setting of the isAnonymousAccessAllowed property in the API deployment specification's authentication policy:</td>
</tr>
<tr>
<td>• only authenticated end users can access the route</td>
</tr>
<tr>
<td>• all authenticated end users can access the route regardless of access scopes in the JWT's scope claim</td>
</tr>
<tr>
<td>• anonymous end users cannot access the route</td>
</tr>
</tbody>
</table>

4. Save the JSON file containing the API deployment specification.

5. Use the API deployment specification when you create or update an API deployment in the following ways:

   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

6. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

Identity Provider Details to Use for iss and aud Claims, and for the JWKS URI

The identity provider that issued the JWT determines the allowed values you have to specify for the issuer (iss) and the audience (aud) claims in the JWT. Which identity provider issued the JWT also determines the URI from which to retrieve the JSON Web Key Set (JWKS) to verify the signature on the JWT. Note that URIs that require authentication or authorization to return the JWKS are not supported.

Use the following table to find out what to specify for JWTs issued by the Oracle Identity Cloud Service (IDCS), Okta, and Auth0 identity providers.
<table>
<thead>
<tr>
<th>Identity Provider</th>
<th>Issuer (iss) claim</th>
<th>Audience (aud) claim</th>
<th>Format of URI from which to retrieve the JWKS</th>
</tr>
</thead>
</table>
To obtain the JWKS without logging in to Oracle Identity Cloud Service, see Change Default Settings in the Oracle Identity Cloud Service documentation. |
See the Okta documentation. |
| Auth0             | https://<your-account-name>.auth0.com/ | Customer-specific.  
See Audience in the Auth0 documentation. | https://<your-account-name>.auth0.com/.well-known/jwks.json |

**Key Parameters Required to Verify JWT Signatures**

To verify the signature on a JWT, API gateways require the following key parameters are present in either the JWKS returned from a URI or the static JSON Web Key you specify.

<table>
<thead>
<tr>
<th>Key Parameter</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>kid</td>
<td>The identifier of the key used to sign the JWT. The value must match the <code>kid</code> claim in the JWT header. For example, <code>master_key</code>.</td>
</tr>
<tr>
<td>kty</td>
<td>The type of the key used to sign the JWT. Note that RSA is currently the only supported key type.</td>
</tr>
<tr>
<td>use or key_ops</td>
<td>If the <code>use</code> parameter is present, then it must be set to <code>sig</code>. If the <code>key-ops</code> parameter is present, then <code>verify</code> must be one of the valid values.</td>
</tr>
<tr>
<td>n</td>
<td>The public key modulus.</td>
</tr>
<tr>
<td>e</td>
<td>The public key exponent.</td>
</tr>
<tr>
<td>alg</td>
<td>The signing algorithm (if present) must be set to one of RS256, RS384 or RS512.</td>
</tr>
</tbody>
</table>
Transforming Incoming Requests and Outgoing Responses

There are often situations when you'll want an API gateway to modify incoming requests before sending them to back-end services. Similarly, you might want the API gateway to modify responses returned by back-end services. For example:

- Back-end services might require requests to include a particular set of HTTP headers (for example, Accept-Language and Accept-Encoding). To hide this implementation detail from API consumers and API clients, you can use your API gateway to add the required headers.
- Web servers often include full version information in response headers. For security reasons, you might want to prevent API consumers and API clients knowing about the underlying technology stack. You can use your API gateway to remove server headers from responses.
- Back-end services might include sensitive information in a response. You can use your API gateway to remove such information.

Using an API gateway, you can:

- Add, remove, and modify headers in requests and responses.
- Add, remove, and modify query parameters in requests.
- Rewrite request URLs from a public format to an internal format, perhaps to support legacy applications and migrations.

You use request and response policies to transform the headers and query parameters of incoming requests, and the headers of outgoing responses (see Adding Request Policies and Response Policies to API Deployment Specifications on page 417).

You can include context variables in header and query parameter transformation request and response policies. Including context variables enables you to modify headers and query parameters with the values of other headers, query parameters, path parameters, and authentication parameters. Note that values of context variable values are extracted from the original request or response, and are not subsequently updated as an API gateway uses a transformation policy to evaluate a request or response. For more information about context variables, see Adding Context Variables to Policies and HTTP Back End Definitions on page 378.

If a header or query parameter transformation request or response policy will result in an invalid header or query parameter, the transformation policy is ignored.

You can add header and query parameter transformation request and response policies to an API deployment specification by:

- using the Console
- editing a JSON file

Adding Header Transformation Request Policies

You can add header transformation request policies to API deployment specifications using the Console or by editing a JSON file.

Using the Console to Add Header Transformation Request Policies

To add header transformation request policies to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. Click Save Changes, and then click Next to enter details for individual routes in the API deployment on the Routes page.

3. On the Routes page, select the route for which you want to specify header transformation request policies.

4. Click Show Route Request Policies.
5. Click the Add button beside **Header Transformations** to update the headers included in a request to the API gateway for the current route.

6. To limit the headers included in a request, specify:
   - **Action**: Filter.
   - **Type**: Either Block to remove from the request the headers you explicitly list, or Allow to only allow in the request the headers you explicitly list (any other headers are removed from the request).
   - **Header Names**: The list of headers to remove from the request or allow in the request (depending on the setting of **Type**). The names you specify are not case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items you filter as allowed). For example, User-Agent.

7. To change the name of a header included in a request (whilst keeping its original value), specify:
   - **Action**: Rename.
   - **From**: The original name of the header that you are renaming. The name you specify is not case-sensitive, and must not be included in any other transformation request policies for the route. For example, X-Username.
   - **To**: The new name of the header you are renaming. The name you specify is not case-sensitive (capitalization might be ignored), and must not be included in any other transformation request policies for the route (with the exception of items you filter as allowed). For example, X-User-ID.

8. To add a new header to a request (or to change or retain the values of an existing header already included in a request), specify:
   - **Action**: Set.
   - **Behavior**: If the header already exists, specify what to do with the header's existing value:
     - **Overwrite**, to replace the header's existing value with the value you specify.
     - **Append**, to append the value you specify to the header's existing value.
     - **Skip**, to keep the header's existing value.
   - **Name**: The name of the header to add to the request (or to change the value of). The name you specify is not case-sensitive (capitalization might be ignored), and must not be included in any other transformation request policies for the route (with the exception of items you filter as allowed). For example, X-Api-Key.
   - **Values**: The value of the new header (or the value to replace or append to an existing header's value, depending on the setting of **Behavior**). The value you specify can be a simple string, or can include context variables enclosed within ${...} delimiters. For example, "value": "zyx987wvu654tsu321", "value": "${request.path[region]}", "value": "${request.headers[opc-request-id]}". You can specify multiple values.

9. Click **Save Changes**, and then click **Next** to review the details you entered for individual routes.

10. Click **Create** or **Save Changes** to create or update the API deployment.

11. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

### Editing a JSON File to Add Header Transformation Request Policies

To add header transformation request policies to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add header transformation request policies, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
```
2. Insert a `requestPolicies` section after the `backend` section for the route to which you want the header transformation request policy to apply. For example:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {}
    }
  ]
}
```

3. Add a `headerTransformations` section to the `requestPolicies` section.

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "headerTransformations":{}
      }
    }
  ]
}
```

4. To limit the headers included in a request, specify a `filterHeaders` header transformation request policy:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "headerTransformations": {
          "filterHeaders": {
            "type": "<BLOCK|ALLOW>",
            "items": [  
              "name": "<header-name>"
            ]
          }
        }
      }
    }
  ]
}
```
where:

- "type": "<BLOCK|ALLOW>" indicates what to do with the headers specified by "items": 
  
  ```
  [{ "name": "<header-name>" }]:
  ```

  - Use BLOCK to remove from the request the headers you explicitly list.
  - Use ALLOW to only allow in the request the headers you explicitly list (any other headers are removed from the request).

- "name": "<header-name>" is a header to remove from the request or allow in the request (depending on the setting of "type": "<BLOCK|ALLOW>".

  The name you specify is not case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items in ALLOW lists).

  For example, User-Agent.

You can remove and allow up to 50 headers in a `filterHeaders` header transformation request policy.

For example:

```json
{
 "routes": [
  {
   "path": "/hello",
   "methods": ["GET"],
   "backend": {
     "type": "ORACLE_FUNCTIONS_BACKEND",
     "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
   },
   "requestPolicies": {
     "headerTransformations": {
       "filterHeaders": {
         "type": "BLOCK",
         "items": [
           {
             "name": "User-Agent"
           }
         ]
       }
     }
   }
  }
]
}
```

In this example, the API gateway removes the User-Agent header from all incoming requests.

5. To change the name of a header included in a request (whilst keeping its original value), specify a `renameHeaders` header transformation request policy:

```json
{
 "routes": [
  {
   "path": "/hello",
   "methods": ["GET"],
   "backend": {
     "type": "ORACLE_FUNCTIONS_BACKEND",
     "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
   },
   "requestPolicies": {
     "renameHeaders": {
       "items": [
         {
          "oldName": "User-Agent",
          "newName": "New-Agent"
         }
       ]
     }
   }
  }
]
}
```
API Gateway

```
"headerTransformations": {
  "renameHeaders": {
    "items": [
      {
        "from": "<original-name>",
        "to": "<new-name>"
      }
    ]
  }
}
```

where:

- "from": "<original-name>" is the original name of the header that you are renaming. The name you specify is not case-sensitive, and must not be included in any other transformation request policies for the route. For example, X-Username.
- "to": "<new-name>" is the new name of the header you are renaming. The name you specify is not case-sensitive (capitalization might be ignored), and must not be included in any other transformation request policies for the route (with the exception of items in ALLOW lists). For example, X-User-ID.

You can rename up to 20 headers in a `renameHeaders` header transformation request policy.

For example:

```
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "headerTransformations": {
          "renameHeaders": {
            "items": [
              {
                "from": "X-Username",
                "to": "X-User-ID"
              }
            ]
          }
        }
      }
    }
  ]
}
```

In this example, the API gateway renames any X-Username header to X-User-ID, whilst keeping the header's original value.

6. To add a new header to a request (or to change or retain the values of an existing header already included in a request), specify a `setHeaders` header transformation request policy:

```
{
  "routes": [
    {
      "path": "/hello",
```
"methods": ["GET"],
"backend": {
"type": "ORACLE_FUNCTIONS_BACKEND",
"functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
},
"requestPolicies": {
"headerTransformations": {
"setHeaders": {
"items": [
{
"name": "<header-name>",
"values": ["<header-value>"],
"ifExists": "<OVERWRITE|APPEND|SKIP>"
}
]
}
}
}
}

where:

- "name": "<header-name>" is the name of the header to add to the request (or to change the value of). The name you specify is not case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items in ALLOW lists). For example, X-Api-Key.
- "values": ["<header-value>"] is the value of the new header (or the value to replace or append to an existing header's value, depending on the setting of "ifExists": "<OVERWRITE|APPEND|SKIP>"). The value you specify can be a simple string, or can include context variables enclosed within ${...} delimiters. For example, "values": "zyx987wvu654tsu321", "values": "${request.path[region]}", "values": "${request.headers[opc-request-id]}".

You can specify up to 10 values. If you specify multiple values, the API gateway adds a header for each value.
- "ifExists": "<OVERWRITE|APPEND|SKIP>" indicates what to do with the header's existing value if the header specified by "<header-name>" already exists:
  - Use OVERWRITE to replace the header's existing value with the value you specify.
  - Use APPEND to append the value you specify to the header's existing value.
  - Use SKIP to keep the header's existing value.

If not specified, the default is OVERWRITE.

You can add (or change the values of) up to 20 headers in a setHeaders header transformation request policy.

For example:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "headerTransformations": {
          "setHeaders": {
            "items": [
              {
                "name": "X-Api-Key",
                "values": ["zyx987wvu654tsu321"],
```

```text*Oracle Cloud Infrastructure User Guide 458*`
In this example, the API gateway adds the X-Api-Key: zyx987wvu654tsu321 header to all incoming requests. If an incoming request already has an X-Api-Key header set to a different value, the API gateway replaces the existing value with zyx987wvu654tsu321.

7. Save the JSON file containing the API deployment specification.
8. Use the API deployment specification when you create or update an API deployment in the following ways:

   • by specifying the JSON file in the Console when you select the Upload an existing API option
   • by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

9. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

Adding Query Parameter Transformation Request Policies

You can add query parameter transformation request policies to API deployment specifications using the Console or by editing a JSON file.

Using the Console to Add Query Parameter Transformation Request Policies

To add query parameter transformation request policies to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. Click Save Changes, and then click Next to enter details for individual routes in the API deployment on the Routes page.

3. On the Routes page, select the route for which you want to specify query parameter transformation request policies.

4. Click Show Route Request Policies.

5. Click the Add button beside Query Parameter Transformations to update the query parameters included in a request to the API gateway for the current route.

6. To limit the query parameters included in a request, specify:

   • Action: Filter.
   • Type: Either Block to remove from the request the query parameters you explicitly list, or Allow to only allow in the request the query parameters you explicitly list (any other query parameters are removed from the request).
   • Query Parameter Names: The list of query parameters to remove from the request or allow in the request (depending on the setting of Type). The names you specify are case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items you filter as allowed). For example, User-Agent.
7. To change the name of a query parameter included in a request (whilst keeping its original value), specify:
   - **Action**: Rename.
   - **From**: The original name of the query parameter that you are renaming. The name you specify is case-sensitive, and must not be included in any other transformation request policies for the route. For example, `X-Username`.
   - **To**: The new name of the query parameter you are renaming. The name you specify is case-sensitive (capitalization is respected), and must not be included in any other transformation request policies for the route (with the exception of items you filter as allowed). For example, `X-User-ID`.

8. To add a new query parameter to a request (or to change or retain the values of an existing query parameter already included in a request), specify:
   - **Action**: Set.
   - **Behavior**: If the query parameter already exists, specify what to do with the query parameter's existing value:
     - **Overwrite**, to replace the query parameter's existing value with the value you specify.
     - **Append**, to append the value you specify to the query parameter's existing value.
     - **Skip**, to keep the query parameter's existing value.
   - **Query Parameter Name**: The name of the query parameter to add to the request (or to change the value of). The name you specify is case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items you filter as allowed). For example, `X-Api-Key`.
   - **Values**: The value of the new query parameter (or the value to replace or append to an existing query parameter's value, depending on the setting of **Behavior**). The value you specify can be a simple string, or can include context variables enclosed within `_${...}_` delimiters. For example, "value": "zyx987wvu654tsu321", "value": "${request.path[region]}", "value": "${request.headers[opc-request-id]}". You can specify multiple values.

9. Click **Save Changes**, and then click **Next** to review the details you entered for individual routes.

10. Click **Create** or **Save Changes** to create or update the API deployment.

11. (Optional) Confirm the API has been deployed successfully by calling it (see **Calling an API Deployed on an API Gateway** on page 384).

**Editing a JSON File to Add Query Parameter Transformation Request Policies**

To add query parameter transformation request policies to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add query parameter transformation request policies, or create a new API deployment specification (see **Creating an API Deployment Specification** on page 361).

   For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

   ```json
   {
      "routes": [
        {
          "path": "/hello",
          "methods": ["GET"],
          "backend": {
            "type": "ORACLE_FUNCTIONS_BACKEND",
            "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
          }
        }
      ]
   }
   ```

   2. Insert a **requestPolicies** section after the **backend** section for the route to which you want the query parameter transformation request policy to apply. For example:

   ```json
   {
   }
3. Add a `queryParameterTransformations` section to the `requestPolicies` section.

```
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "queryParameterTransformations": {}
      }
    }
  ]
}
```

4. To limit the query parameters included in a request, specify a `filterQueryParameters` query parameters transformation request policy:

```
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "queryParameterTransformations": {
          "filterQueryParameters": {
            "type": "<BLOCK|ALLOW>",
            "items": [
              { "name": "<query-parameter-name>" }
            ]
          }
        }
      }
    }
  ]
}
```
where:

- "type": "<BLOCK|ALLOW>" indicates what to do with the query parameters specified by "items":
  - Use BLOCK to remove from the request the query parameters you explicitly list.
  - Use ALLOW to only allow in the request the query parameters you explicitly list (any other query parameters are removed from the request).
- "name": "<query-parameter-name>" is a query parameter to remove from the request or allow in the request (depending on the setting of "type": "<BLOCK|ALLOW>"). The name you specify is case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items in ALLOW lists). For example, User-Agent.

You can remove and allow up to 50 query parameters in a filterQueryParameters query parameter transformation request policy.

For example:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.ocl.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "queryParameterTransformations": {
          "filterQueryParameters": {
            "type": "BLOCK",
            "items": [
              {
                "name": "User-Agent"
              }
            ]
          }
        }
      }
    }
  ]
}
```

In this example, the API gateway removes the User-Agent query parameter from all incoming requests.

5. To change the name of a query parameter included in a request (whilst keeping its original value), specify a renameQueryParameters query parameter transformation request policy:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.ocl.phx.aaaaaaaaab______xmq"
      },
      "requestPolicies": {
        "queryParameterTransformations": {
          "renameQueryParameters": {
            "name": "User-Agent",
            "items": [
              {
                "name": "New-Parameter-Name"
              }
            ]
          }
        }
      }
    }
  ]
}
```

In this example, the API gateway changes the name of the User-Agent query parameter to New-Parameter-Name.
API Gateway

```
{
    "from": "<original-name>",
    "to": "<new-name>
}
```

where:

- "from": "<original-name>" is the original name of the query parameter that you are renaming. The name you specify is case-sensitive, and must not be included in any other transformation request policies for the route. For example, X-Username.
- "to": "<new-name>" is the new name of the query parameter you are renaming. The name you specify is case-sensitive (capitalization is respected), and must not be included in any other transformation request policies for the route (with the exception of items in ALLOW lists). For example, X-User-ID.

You can rename up to 20 query parameters in a renameQueryParameters query parameter transformation request policy.

For example:

```
{
    "routes": [ 
    {
        "path": "/hello",
        "methods": ["GET"],
        "backend": { 
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______.xmq"
        },
        "requestPolicies": { 
        "queryParameterTransformations": { 
        "renameQueryParameters": { 
        "items": [ 
        {
            "from": "X-Username",
            "to": "X-User-ID"
        ]
        ]
        }
        }
        }
    } 
    ]
}
```

In this example, the API gateway renames any X-Username query parameter to X-User-ID, whilst keeping the query parameter's original value.

6. To add a new query parameter to a request (or to change or retain the values of an existing query parameter already included in a request), specify a setQueryParameters query parameter transformation request policy:

```
{
    "routes": [ 
    {
        "path": "/hello",
        "methods": ["GET"],
```

Oracle Cloud Infrastructure User Guide 463
"backend": {
    "type": "ORACLE_FUNCTIONS_BACKEND",
    "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
},
"requestPolicies": {
    "queryParameterTransformations": {
        "setQueryParameters": {
            "items": [
                {
                    "name": "<query-parameter-name>",
                    "values": ["<query-parameter-value>"]
                }
            ]
        }
    }
}

where:

- "name": "<query-parameter-name>" is the name of the query parameter to add to the request (or to change the value of). The name you specify is case-sensitive, and must not be included in any other transformation request policies for the route (with the exception of items in ALLOW lists). For example, X-API-Key.
- "values": ["<query-parameter-value>"] is the value of the new query parameter (or the value to replace or append to an existing query parameter's value, depending on the setting of "ifExists": "<OVERWRITE|APPEND|SKIP>"). The value you specify can be a simple string, or can include context variables enclosed within ${...} delimiters. For example, "values": "zyx987wvu654tsu321", "values": "${request.path[region]}", "values": "${request.headers[opc-request-id]}".

You can specify up to 10 values. If you specify multiple values, the API gateway adds a query parameter for each value.

- "ifExists": "<OVERWRITE|APPEND|SKIP>" indicates what to do with the query parameter's existing value if the query parameter specified by <query-parameter-name> already exists:
  - Use OVERWRITE to replace the query parameter's existing value with the value you specify.
  - Use APPEND to append the value you specify to the query parameter's existing value.
  - Use SKIP to keep the query parameter's existing value.

If not specified, the default is OVERWRITE.

You can add (or change the values of) up to 20 query parameters in a setQueryParameters query parameter transformation request policy.

For example:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            },
            "requestPolicies": {
                "queryParameterTransformations": {
                    "setQueryParameters": {
                        "items": []
                    }
                }
            }
        }
    ]
}
```
In this example, the API gateway adds the X-Api-Key:zyx987wvu654tsu321 query parameter to all incoming requests. If an incoming request already has an X-Api-Key query parameter set to a different value, the API gateway replaces the existing value with zyx987wvu654tsu321.

7. Save the JSON file containing the API deployment specification.
8. Use the API deployment specification when you create or update an API deployment in the following ways:
   - by specifying the JSON file in the Console when you select the Upload an existing API option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.
9. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

Adding Header Transformation Response Policies

You can add header transformation response policies to API deployment specifications using the Console or by editing a JSON file.

Using the Console to Add Header Transformation Response Policies

To add header transformation response policies to an API deployment specification using the Console:

1. Create or update an API deployment using the Console, select the From Scratch option, and enter details on the Basic Information page.

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

2. Click Save Changes, and then click Next to enter details for individual routes in the API deployment on the Routes page.

3. On the Routes page, select the route for which you want to specify header transformation response policies.

4. Click Show Route Response Policies.

5. Click the Add button beside Header Transformations to update the headers included in a response from the API gateway for the current route.

6. To limit the headers included in a response, specify:
   - Action: Filter.
   - Type: Either Block to remove from the response the headers you explicitly list, or Allow to only allow in the response the headers you explicitly list (any other headers are removed from the response).
   - Header Names: The list of headers to remove from the response or allow in the response (depending on the setting of Type). The names you specify are not case-sensitive, and must not be included in any other transformation response policies for the route (with the exception of items you filter as allowed). For example, User-Agent.
7. To change the name of a header included in a response (whilst keeping its original value), specify:
   
   • **Action**: Rename.
   • **From**: The original name of the header that you are renaming. The name you specify is not case-sensitive, and must not be included in any other transformation response policies for the route. For example, X-Username.
   • **To**: The new name of the header you are renaming. The name you specify is not case-sensitive (capitalization might be ignored), and must not be included in any other transformation response policies for the route (with the exception of items in ALLOW lists). For example, X-User-ID.

8. To add a new header to a response (or to change or retain the values of an existing header already included in a response), specify:
   
   • **Action**: Set.
   • **Behavior**: If the header already exists, specify what to do with the header's existing value:
     • **Overwrite**, to replace the header's existing value with the value you specify.
     • **Append**, to append the value you specify to the header's existing value.
     • **Skip**, to keep the header's existing value.
   • **Name**: The name of the header to add to the response (or to change the value of). The name you specify is not case-sensitive, and must not be included in any other transformation response policies for the route (with the exception of items you filter as allowed). For example, X-Api-Key.
   • **Values**: The value of the new header (or the value to replace or append to an existing header's value, depending on the setting of **Behavior**). The value you specify can be a simple string, or can include context variables enclosed within ${...} delimiters. For example, "value": "zyx987wvu654tsu321". You can specify multiple values.

9. Click **Save Changes**, and then click **Next** to review the details you entered for individual routes.

10. Click **Create** or **Save Changes** to create or update the API deployment.

11. (Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).

**Editing a JSON File to Add Header Transformation Response Policies**

To add header transformation response policies to an API deployment specification in a JSON file:

1. Using your preferred JSON editor, edit the existing API deployment specification to which you want to add header transformation response policies, or create a new API deployment specification (see Creating an API Deployment Specification on page 361).

For example, the following basic API deployment specification defines a simple Hello World serverless function in Oracle Functions as a single back end:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.ocl.phx.aaaaaaaaab______xmq"
      }
    }
  ]
}
```

2. Insert a `responsePolicies` section after the `backend` section for the route to which you want the header transformation response policy to apply. For example:

```json
{
  "routes": [
    {
      "path": "/hello",
      "responsePolicies": {
        "headers": [
          {
            "headers": [
              {
                "name": "X-Api-Key",
                "values": "abc123",
                "behavior": "overwrite"
              }
            ]
          }
        ]
      }
    }
  ]
}
```
3. Add a `headerTransformations` section to the `responsePolicies` section.

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            },
            "responsePolicies": {
                "headerTransformations": {};
            }
        }
    ]
}
```

4. To limit the headers included in a response, specify a `filterHeaders` header transformation response policy:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            },
            "responsePolicies": {
                "headerTransformations": {
                    "filterHeaders": {
                        "type": "<BLOCK|ALLOW>",
                        "items": [
                            {
                                "name": "<header-name>"
                            }
                        ]
                    }
                }
            }
        }
    ]
}
```
where:

- "type": "<BLOCK|ALLOW>" indicates what to do with the headers specified by "items":
  
  - Use BLOCK to remove from the response the headers you explicitly list.
  - Use ALLOW to only allow in the response the headers you explicitly list (any other headers are removed from the response).
- "name": "<header-name>" is a header to remove from the response or allow in the response (depending on the setting of "type": "<BLOCK|ALLOW>"). The name you specify is not case-sensitive, and must not be included in any other transformation response policies for the route (with the exception of items in ALLOW lists). For example, User-Agent.

You can remove and allow up to 20 headers in a filterHeaders header transformation response policy.

For example:

```
{
   "routes": [
   {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
         "type": "ORACLE_FUNCTIONS_BACKEND",
         "functionId": "ocid1.fnfunc.ocl.phx.aaaaaaaaab______xmq"
      },
      "responsePolicies": {
         "headerTransformations": {
            "filterHeaders": {
               "type": "BLOCK",
               "items": [
               {
                  "name": "User-Agent"
               }
               ]
            }
         }
      }
   }
   ]
}
```

In this example, the API gateway removes the User-Agent header from all outgoing responses.

5. To change the name of a header included in a response (whilst keeping its original value), specify a renameHeaders header transformation response policy:

```
{
   "routes": [
   {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
         "type": "ORACLE_FUNCTIONS_BACKEND",
         "functionId": "ocid1.fnfunc.ocl.phx.aaaaaaaaab______xmq"
      },
      "responsePolicies": {
         "headerTransformations": {
            "renameHeaders": {
               "items": [
               
```

Oracle Cloud Infrastructure User Guide
API Gateway

where:

- "from": "<original-name>" is the original name of the header that you are renaming. The name you specify is not case-sensitive, and must not be included in any other transformation response policies for the route. For example, X-Username.

- "to": "<new-name>" is the new name of the header you are renaming. The name you specify is not case-sensitive (capitalization might be ignored), and must not be included in any other transformation response policies for the route (with the exception of items in ALLOW lists). For example, X-User-ID.

You can rename up to 20 headers in a renameHeaders header transformation response policy.

For example:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "responsePolicies": {
        "headerTransformations": {
          "renameHeaders": {
            "items": [
              {
                "from": "X-Username",
                "to": "X-User-ID"
              }
            ]
          }
        }
      }
    }
  ]
}
```

In this example, the API gateway renames any X-Username header to X-User-ID, whilst keeping the header's original value.

6. To add a new header to a response (or to change or retain the values of an existing header already included in a response), specify a setHeaders header transformation response policy:

```json
{
  "routes": [
    {
      "path": "/hello",
      "methods": ["GET"],
      "backend": {
        "type": "ORACLE_FUNCTIONS_BACKEND",
        "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
      },
      "responsePolicies": {
        "headerTransformations": {
          "setHeaders": {
            "items": [
              {
                "name": "User-Id",
                "value": "123456"
              }
            ]
          }
        }
      }
    }
  ]
}
```
where:

- "name": "<header-name>" is the name of the header to add to the response (or to change the value of). The name you specify is not case-sensitive, and must not be included in any other transformation response policies for the route (with the exception of items in ALLOW lists). For example, X-API-Key.
- "values": ["<header-value>"] is the value of the new header (or the value to replace or append to an existing header's value, depending on the setting of "ifExists": "<OVERWRITE|APPEND|SKIP>"). The value you specify can be a simple string, or can include context variables enclosed within ${...} delimiters. For example, "values": "zyx987wvu654tsu321".

You can specify up to 10 values. If you specify multiple values, the API gateway adds a header for each value.
- "ifExists": "<OVERWRITE|APPEND|SKIP>" indicates what to do with the header's existing value if the header specified by <header-name> already exists:
  - Use OVERWRITE to replace the header's existing value with the value you specify.
  - Use APPEND to append the value you specify to the header's existing value.
  - Use SKIP to keep the header's existing value.

If not specified, the default is OVERWRITE.

You can add (or change the values of) up to 20 headers in a setHeaders header transformation response policy. For example:

```json
{
    "routes": [
        {
            "path": "/hello",
            "methods": ["GET"],
            "backend": {
                "type": "ORACLE_FUNCTIONS_BACKEND",
                "functionId": "ocid1.fnfunc.oc1.phx.aaaaaaaaab______xmq"
            },
            "responsePolicies": {
                "headerTransformations": {
                    "setHeaders": {
                        "items": [
                            {
                                "name": "X-API-Key",
                                "values": ["zyx987wvu654tsu321"],
                                "ifExists": "OVERWRITE"
                            }
                        ]
                    }
                }
            }
        }
    ]
}
```
In this example, the API gateway adds the `X-API-Key:zyx987wvu654tsu321` header to all outgoing responses. If an outgoing response already has an `X-API-Key` header set to a different value, the API gateway replaces the existing value with `zyx987wvu654tsu321`.

7. Save the JSON file containing the API deployment specification.

8. Use the API deployment specification when you create or update an API deployment in the following ways:

   - by specifying the JSON file in the Console when you select the **Upload an existing API** option
   - by specifying the JSON file in a request to the API Gateway REST API

   For more information, see Deploying an API on an API Gateway by Creating an API Deployment on page 363 and Updating API Gateways and API Deployments on page 387.

9. **(Optional) Confirm the API has been deployed successfully by calling it (see Calling an API Deployed on an API Gateway on page 384).**

### Examples

The examples in this section assume the following API deployment definition and basic API deployment specification in a JSON file:

```json
{
    "displayName": "Marketing Deployment",
    "gatewayId": "ocid1.apigateway.oc1..aaaaaaaab______hga",
    "compartmentId": "ocid1.compartment.oc1..aaaaaaaa7______ysq",
    "pathPrefix": "/marketing",
    "specification": {
        "routes": [
            {
                "path": "/weather",
                "methods": ["GET"],
                "backend": {
                    "type": "HTTP_BACKEND",
                    "url": "https://api.weather.gov"
                },
                "requestPolicies": {}
            }
        ],
        "freeformTags": {},
        "definedTags": {}
    }
}
```

Note the examples also apply when you're defining an API deployment specification using dialogs in the Console.

**Example 1: Transforming header parameters to query parameters**

In this example, assume an existing HTTP back end only handles requests containing query parameters, not header parameters. However, you want the HTTP back end to handle requests that include header parameters. To achieve this, you create an API deployment specification that includes a query parameter transformation request policy to pass the value obtained from a request header to the HTTP back end as a query parameter.

```json
"requestPolicies": {
    "queryParameterTransformations": {
        "setQueryParameters": {
            "items": [
                {
                    "name": "region",
                    "transform": "header/region",
                    "default": "default" // Optional default value
                }
            ]
        }
    }
}
```
In this example, a request like `curl -H "region: west" https://<gateway-hostname>/marketing/weather` resolves to `https://api.weather.gov?region=west`.

**Example 2: Transforming one header to a different header**

In this example, assume an existing HTTP back end only handles requests containing a particular header. However, you want the HTTP back end to handle requests that include a different header. To achieve this, you create an API deployment specification that includes a header transformation request policy to take the value obtained from one request header and pass it to the HTTP back end as a different request header.

```
"requestPolicies": { 
  "headerTransformations": { 
    "setHeaders": { 
      "items": [ 
        { 
          "name": "region",
          "values": ["${request.headers[locale]}"],
          "ifExists": "OVERWRITE"
        }
      ]
    }
  }
}
```

In this example, a request like `curl -H "locale: west" https://<gateway-hostname>/marketing/weather` resolves to the request `curl -H "region: west" https://api.weather.gov`.

**Example 3: Adding an authentication parameter obtained from a JWT as a request header**

In this example, assume an existing HTTP back end requires the value of the sub claim in a validated JSON Web Token (JWT) to be included in a request as a header with the name JWT_SUBJECT. The API Gateway service has saved the value of the sub claim included in the JWT as an authentication parameter in the request.auth table.

To include the value of sub in a header named JWT_SUBJECT, you create an API deployment specification that includes a header transformation request policy. The request policy obtains the sub value from the request.auth table and passes it to the HTTP back end as the value of the JWT_SUBJECT header.

```
"requestPolicies": { 
  "headerTransformations": { 
    "setHeaders": { 
      "items": [ 
        { 
          "name": "JWT_SUBJECT",
          "values": ["${request.auth[sub]}"],
          "ifExists": "OVERWRITE"
        }
      ]
    }
  }
}
```
In this example, when a request has been successfully validated, the JWT_SUBJECT header is added to the request passed to the HTTP back end.

**Example 4: Adding a key obtained from an authorizer function as a query parameter**

In this example, assume an existing HTTP back end requires requests to include a query parameter named access_key for authentication purposes. You want the access_key query parameter to have the value of a key named apiKey that has been returned by an authorizer function that has successfully validated the request. The API Gateway service has saved the apiKey value as an authentication parameter in the request.auth table.

To include the access_key query parameter in the request, you create an API deployment specification that includes a query parameter transformation request policy. The request policy obtains the apiKey value from the request.auth table and passes it to the HTTP back end as the value of the access_key query parameter.

```json
"requestPolicies": {
  "queryParameterTransformations": {
    "setQueryParameters": {
      "items": [
        {
          "name": "access_key",
          "values": ["${request.auth[apiKey]}"],
          "ifExists": "OVERWRITE"
        }
      ]
    }
  }
}
```

In this example, the access_key query parameter is added to the request passed to the HTTP back end, with the apiKey value from the request.auth table. A request like `https://<gateway-hostname>/marketing/weather` resolves to a request like `https://api.weather.gov?access_key=fw5n9abi0ep`

**Example 5: Adding a default value for an optional query parameter**

In this example, assume an existing HTTP back end requires requests to include a query parameter named country. However, the country query parameter is optional, and it’s not included by some of the API clients sending requests. If a request already includes a country query parameter and a value, you want both passed as-is to the HTTP back end. However, if a request doesn’t already include a country query parameter, you want the country query parameter and a default value added to the request.

To make sure every request includes a country query parameter, you create an API deployment specification that includes a query parameter transformation request policy. The request policy adds the country query parameter and a default value to any requests that do not already include the country query parameter.

```json
"requestPolicies": {
  "queryParameterTransformations": {
    "setQueryParameters": {
      "items": [
        {
          "name": "country",
          "values": ["usa"],
          "ifExists": "SKIP"
        }
      ]
    }
  }
}
```

Troubleshooting API Gateway

This topic covers common issues related to the API Gateway service and how you can address them.

Creating a new API gateway stalls with a state of Creating, or fails

It can take a few minutes to create a new API gateway. While it is being created, the API gateway is shown with a state of Creating on the Gateways page. When it has been created successfully, the new API gateway is shown with a state of Active.

If you have waited more than a few minutes for the API gateway to be shown with an Active state (or if the API gateway creation operation has failed):

1. Click the name of the API gateway, and click Work Requests to see an overview of the API gateway creation operation.
2. Click the Create Gateway operation to see more information about the operation (including error messages, log messages, and the status of associated resources) that will help to diagnose the cause of the problem.

Creating a new API deployment stalls with a state of Creating, or fails

It can take a few minutes to create a new API deployment. While it is being created, the API deployment is shown with a state of Creating on the Gateway Details page. When it has been created successfully, the new API deployment is shown with a state of Active.

If you have waited more than a few minutes for the API deployment to be shown with an Active state (or if the API deployment creation operation has failed):

1. Click the name of the API deployment, and click Work Requests to see an overview of the API deployment creation operation.
2. Click the Create Deployment operation to see more information about the operation (including error messages, log messages, and the status of associated resources) that will help to diagnose the cause of the problem.

Creating a new API gateway returns a "VNIC attachment failed due to the limit for number of private IP addresses for this subnet" message

When creating a new API gateway, you might see the following message:

```
VNIC attachment failed due to the limit for number of private IP addresses for this subnet
```

This message indicates that there are not enough private IP addresses available to create the API gateway in the specified subnet. An API gateway consumes three private IP addresses in the subnet.

To address this issue, use a subnet that has at least three available private IP addresses.

Creating a new API gateway returns a "The limit for number of private IP addresses for this subnet has been exceeded" message

When creating a new API gateway, you might see the following message:

```
The limit for number of private IP addresses for this subnet has been exceeded
```

This message indicates that there are not enough private IP addresses available to create the API gateway in the specified subnet. An API gateway consumes three private IP addresses in the subnet.
To address this issue, use a subnet that has at least three available private IP addresses.

**Creating a new public API gateway returns a "The limit for number of public IP addresses for this compartment has been exceeded" message**

When creating a new public API gateway, you might see the following message:

```
The limit for number of public IP addresses for this compartment has been exceeded
```

This message indicates that there are not enough public IP addresses available to create the public API gateway in the specified subnet's compartment. When creating a new public API gateway, an attempt is made to create a new public IP address in the subnet's compartment. The attempt to create the new public IP address fails if the quota for public IP addresses is exceeded in that compartment or tenancy. Note the public IP address is in addition to the three private IP addresses consumed by all API gateways.

To address this issue:

- If the compartment's quota is exceeded, contact your tenancy administrator to request additional public IP addresses for the compartment.
- If the tenancy's quota is exceeded, contact Oracle Support to request an increase to the tenancy's quota.

**Creating a new API gateway returns a "Work request was cancelled" message**

When creating a new API gateway, you might see the following message:

```
Work request was cancelled
```

This message indicates that you cancelled the work request to create the API gateway. The API gateway is shown with a status of Failed.

**Creating a new API gateway returns a "An unexpected error occurred. Contact Oracle Support for assistance" message**

When creating a new API gateway, you might see the following message:

```
An unexpected error occurred. Contact Oracle Support for assistance.
```

To address this issue, contact Oracle Support to request assistance.

**Creating a new API gateway returns an "Unknown resource <subnet-ocid>, make sure subnet exists,..." message and a 400 error**

When creating a new API gateway using the Console, API, SDK, or CLI, you might see the following error message and a 400 error code:

```
Unknown resource <subnet-ocid>, make sure subnet exists, the user can access the subnet and it is in the same region where the gateway will be created
```

This message indicates that the API Gateway service cannot access the subnet specified for the new API gateway.

To address this issue, double-check that:

- The subnet exists.
- You can access the subnet.
- The subnet is in the same region in which the API gateway will be created.
**API Gateway Internal Limits**

This topic describes various internal limits enforced by the API Gateway service, their default values, and whether you can change them.

**API Gateway Resource Limits**

This table describes internal limits enforced by the API Gateway service on API gateway resources.

<table>
<thead>
<tr>
<th>Limit</th>
<th>Description</th>
<th>Default Limit Value</th>
<th>Can you change it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of API gateways</td>
<td>Maximum number of active API gateways per tenant.</td>
<td>10</td>
<td>Yes, contact us.</td>
</tr>
</tbody>
</table>

**API Deployment Resource Limits**

This table describes internal limits enforced by the API Gateway service on API deployment resources.

<table>
<thead>
<tr>
<th>Limit</th>
<th>Description</th>
<th>Default Limit Value</th>
<th>Can you change it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of API deployments</td>
<td>Maximum number of active API deployments per gateway.</td>
<td>20</td>
<td>Yes, contact us.</td>
</tr>
<tr>
<td>Number of routes per API deployment</td>
<td>Maximum number of routes defined inside the API deployment specification.</td>
<td>50</td>
<td>Yes, contact us.</td>
</tr>
<tr>
<td>Path prefix length</td>
<td>Maximum length of path for API deployment.</td>
<td>2,000 characters</td>
<td>No</td>
</tr>
<tr>
<td>Route pattern length</td>
<td>Maximum length of path for a route in an API deployment.</td>
<td>2,000 characters</td>
<td>No</td>
</tr>
<tr>
<td>API deployment specification Size</td>
<td>Maximum length of json encoded API deployment specification in bytes.</td>
<td>1,000,000 bytes</td>
<td>No</td>
</tr>
<tr>
<td>Stock Response - header length</td>
<td>Maximum length of UTF-8 encoded json of stock response headers.</td>
<td>4096 bytes</td>
<td>No</td>
</tr>
<tr>
<td>Stock Response - header name length</td>
<td>Maximum length of a stock response header name.</td>
<td>1024 bytes</td>
<td>No</td>
</tr>
<tr>
<td>Stock Response - header value length</td>
<td>Maximum length of a stock response header value.</td>
<td>4096 bytes</td>
<td>No</td>
</tr>
<tr>
<td>Stock Response - number of headers</td>
<td>Maximum number of stock response headers.</td>
<td>50</td>
<td>No</td>
</tr>
<tr>
<td>Stock Response - body size</td>
<td>Maximum body size in UTF-8 bytes.</td>
<td>4096 bytes</td>
<td>No</td>
</tr>
<tr>
<td>CORS Policy - number of headers</td>
<td>Maximum number of CORS allowed/exposed headers.</td>
<td>50</td>
<td>No</td>
</tr>
<tr>
<td>Limit</td>
<td>Description</td>
<td>Default Limit Value</td>
<td>Can you change it?</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>CORS Policy - number of allowed methods</td>
<td>Maximum number of CORS allowed methods.</td>
<td>50</td>
<td>No</td>
</tr>
</tbody>
</table>

**API Gateway Certificate Resource Limits**

This table describes internal limits enforced by the API Gateway service on API Gateway certificate resources.

<table>
<thead>
<tr>
<th>Limit</th>
<th>Description</th>
<th>Default Limit Value</th>
<th>Can you change it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaf Certificate - maximum length</td>
<td>Maximum length of the leaf certificate.</td>
<td>4096 bits</td>
<td>No</td>
</tr>
<tr>
<td>Intermediate Certificates - maximum length</td>
<td>Maximum combined length of any intermediate certificates.</td>
<td>10240 bits</td>
<td>No</td>
</tr>
<tr>
<td>Private key - maximum length</td>
<td>Maximum private key size.</td>
<td>4096 bits</td>
<td>No</td>
</tr>
<tr>
<td>Private key - minimum length</td>
<td>Minimum private key size.</td>
<td>2048 bits</td>
<td>No</td>
</tr>
</tbody>
</table>

**HTTP Back End Resource Limits**

This table describes internal limits enforced by the API Gateway service on HTTP back ends.

<table>
<thead>
<tr>
<th>Limit</th>
<th>Description</th>
<th>Default Limit Value</th>
<th>Can you change it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect timeout</td>
<td>Maximum configurable HTTP back end connect timeout in seconds.</td>
<td>60.0 seconds</td>
<td>Yes, by changing the timeout setting in the API deployment specification to between 1.0 and 75.0 seconds (see Adding an HTTP or HTTPS URL as an API Gateway Back End on page 406).</td>
</tr>
<tr>
<td>Read timeout</td>
<td>Maximum configurable HTTP back end read timeout in seconds.</td>
<td>10.0 seconds</td>
<td>Yes, by changing the timeout setting in the API deployment specification to between 1.0 and 300.0 seconds (see Adding an HTTP or HTTPS URL as an API Gateway Back End on page 406).</td>
</tr>
<tr>
<td>Send timeout</td>
<td>Maximum configurable HTTP back end send timeout in seconds.</td>
<td>10.0 seconds</td>
<td>Yes, by changing the timeout setting in the API deployment specification to between 1.0 and 300.0 seconds (see Adding an HTTP or HTTPS URL as an API Gateway Back End on page 406).</td>
</tr>
</tbody>
</table>
API Gateway Invocation Limits

This table describes internal limits enforced by the API Gateway service on API gateway invocations.

<table>
<thead>
<tr>
<th>Limit</th>
<th>Description</th>
<th>Default Limit Value</th>
<th>Can you change it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simultaneous connections per IP address</td>
<td>Maximum number of simultaneous HTTPS connections from a single IP address to an API gateway.</td>
<td>1000</td>
<td>No</td>
</tr>
<tr>
<td>Request body size</td>
<td>Maximum request body size.</td>
<td>6 MB</td>
<td>No</td>
</tr>
<tr>
<td>Request header read timeout</td>
<td>Time between reads of request header bytes.</td>
<td>15 seconds</td>
<td>No</td>
</tr>
<tr>
<td>Request body read timeout</td>
<td>Time between reads of request body bytes.</td>
<td>15 seconds</td>
<td>No</td>
</tr>
<tr>
<td>Response body read timeout</td>
<td>Time between sends of response body bytes.</td>
<td>15 seconds</td>
<td>No</td>
</tr>
<tr>
<td>Maximum header size</td>
<td>Maximum length of header (including method, URI, and headers).</td>
<td>8 KB</td>
<td>No</td>
</tr>
<tr>
<td>Function back end latency</td>
<td>Maximum duration of a full request to a function back end.</td>
<td>300 seconds</td>
<td>No</td>
</tr>
<tr>
<td>HTTP back end latency</td>
<td>Maximum duration of a full request to an HTTP back end.</td>
<td>300 seconds</td>
<td>No</td>
</tr>
</tbody>
</table>

API Gateway Metrics

You can monitor the health, capacity, and performance of API gateways and API deployments managed by the API Gateway service using metrics, alarms, and notifications.

This topic describes the metrics emitted by the API Gateway service in the oci_apigateway metric namespace.

Resources: gateways

Overview of the API Gateway Service Metrics

The API Gateway service metrics help you measure the connections to API gateways, and the quantity of data received and sent by API gateways. You can use metrics data to diagnose and troubleshoot API gateway and API deployment issues.

To view a default set of metrics charts in the Console, navigate to the API gateway you're interested in, and then click Metrics. You also can use the Monitoring service to create custom queries.

Prerequisites

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.
Available Metrics: oci_apigateway

The metrics listed in the following tables are automatically available for any API gateways you create. You do not need to enable monitoring on the resource to get these metrics.

API Gateway metrics include the following dimensions:

**RESOURCEID**

The *OCID* of the API gateway.

**DEPLOYMENTID**

The *OCID* of the API deployment.

**ROUTE**

The route path for API calls to the back-end service.

**HTTPMETHODTYPE**

The HTTP methods of incoming connections accepted by the back-end service (such as GET, HEAD, POST, PUT, DELETE).

**HTTPSTATUSCODE**

The HTTP response status code received from the API gateway (such as 200, 201, 502, 504).

**HTTPSTATUSCATEGORY**

The category of the HTTP response status code received from the API gateway (such as 2xx, 3xx, 4xx, 5xx).

**BACKENDTYPE**

The type of back end by which an API gateway routes requests to a back-end service (such as HTTP_BACKEND, ORACLE_FUNCTIONS_BACKEND, STOCK_RESPONSE_BACKEND).

**BACKENDHTTPSTATUSCODE**

The HTTP response status code received from the back end (such as 200, 201, 502, 504).

**BACKENDHTTPSTATUSCATEGORY**

The category of the HTTP response status code received from the back end (such as 2xx, 3xx, 4xx, 5xx).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BytesReceived</td>
<td>Bytes Received</td>
<td>Bytes</td>
<td>Number of bytes received by the API gateway from API clients.</td>
<td>resourceId deploymentId route</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>httpMethodType httpStatusCode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>httpStatusCategory backendType</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 479
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BytesSent</td>
<td>Bytes Sent</td>
<td>Bytes</td>
<td>Number of bytes sent by the API gateway to API clients.</td>
</tr>
<tr>
<td>HttpRequests</td>
<td>API Requests</td>
<td>count</td>
<td>Number of incoming API client requests to the API gateway.</td>
</tr>
<tr>
<td>HttpResponses</td>
<td>API Responses</td>
<td>count</td>
<td>Number of http responses that the API gateway has sent back.</td>
</tr>
<tr>
<td>BackendHttpResponses</td>
<td>Backend Responses</td>
<td>count</td>
<td>Count of the HTTP responses returned by the back-end services.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Latency</td>
<td>Gateway Latency</td>
<td>Seconds</td>
<td>Average time that it takes for a request to be processed and its response to be sent. This is calculated from the time the API gateway receives the first byte of an HTTP request to the time when the response send operation is completed.</td>
</tr>
<tr>
<td>IntegrationLatency</td>
<td>Backend Latency</td>
<td>Seconds</td>
<td>Time between the API gateway sending a request to the back-end service and receiving a response from the back-end service.</td>
</tr>
<tr>
<td>InternalLatency</td>
<td>Internal Latency</td>
<td>Seconds</td>
<td>Time spent internally in the API gateway to process the request.</td>
</tr>
</tbody>
</table>

**Using the Console**

To view default metric charts for a single API gateway

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click API Gateway.
2. Select the region you are using with API Gateway.
3. Select the compartment containing the API gateway for which you want to view metrics.
   
   The Gateways page shows all the API gateways in the compartment you selected.
4. Click the name of the API gateway for which you want to view metrics.
5. Under Resources, click Metrics.
   
   The Metrics page displays a chart for each metric that is emitted by the metric namespace for API Gateway. For more information about the emitted metrics, see Available Metrics: oci_apigateway on page 479.

   For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.
**Not seeing the API gateway metrics data you expect?**

If you don't see the metrics data for an API gateway that you expect, see the following possible causes and resolutions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>How to check</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I called an API deployed on an API gateway but the HTTP Requests chart doesn't show the API call.</td>
<td>You might have called the API outside the time period covered by the HTTP Requests chart.</td>
<td>Confirm the Start Time and End Time cover the period when you called the API.</td>
<td>Adjust the Start Time and End Time as necessary.</td>
</tr>
<tr>
<td>I called an API deployed on an API gateway but the HTTP Requests chart doesn't show the API call, even</td>
<td>Although you called the API between the Start Time and End Time, the x-axis (window of data display)</td>
<td>Confirm the x-axis (window of data display) covers the period when the API was called.</td>
<td>Adjust the x-axis (window of data display) as necessary.</td>
</tr>
<tr>
<td>though I called the API between the Start Time and End Time.</td>
<td>might be excluding the API call.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I want to see data in the charts as a continuous line over time, but the line has gaps in it.</td>
<td>This is expected behavior. If there is no metrics data to show in the selected interval, the data line is discontinuous.</td>
<td>Increase the Interval (for example, from 1 minute to 5 minutes, or from 1 minute to 1 hour).</td>
<td>Adjust the Interval as necessary.</td>
</tr>
</tbody>
</table>

**To view default metric charts for all the API gateways in a compartment**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. Select the region you are using with API Gateway
3. Select the compartment containing the API gateways for which you want to view metrics.
4. For Metric Namespace, select oci_apigateway.

The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace. For more information about the emitted metrics, see Available Metrics: oci_apigateway on page 479.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)
Chapter 7

Archive Storage

This chapter explains how to upload, manage, and access data using Archive Storage.

Overview of Archive Storage

The Archive Storage service is ideal for storing data that is seldom accessed, but requires long retention periods. Archive Storage is more cost effective than Object Storage for preserving cold data. Unlike Object Storage, Archive Storage data retrieval is not instantaneous.

Oracle Cloud Infrastructure supports multiple storage tiers that offer cost and performance flexibility. Archive is the default storage tier for Archive Storage buckets.

Archive Storage is Always Free eligible. For more information about Always Free resources, including capabilities and limitations, see Oracle Cloud Infrastructure Free Tier on page 140.

Using Archive Storage

Important:

You interact with the data stored in the Archive Storage using the same resources and management interfaces that you use for data stored in Object Storage. All Object Storage features are also supported in Archive Storage.

Use the following Object Storage resources to store and manage Archive Storage data.

Buckets

Buckets are logical containers for storing objects. A bucket is associated with a single compartment that has policies that determine what actions a user can perform on a bucket and on all the objects in the bucket.

When you initially create the bucket container for your data, you decide which default storage tier (Archive or Standard) is appropriate for your data. The default tier is automatically selected when you upload objects to the bucket, but you can instead select a different tier. Also, if objects meet the criteria of an object lifecycle policy rule, Object Storage can automatically move objects to Archive, while remaining in the Standard tier bucket.

Once set, you cannot change the default storage tier property for a bucket:

• An existing Standard tier bucket cannot be changed to an Archive tier bucket.
• An existing Archive tier bucket cannot be changed to a Standard tier bucket.

In addition to the inability to change the default storage tier designation of a bucket, there are other reasons why storage tier selection for buckets requires careful consideration:

• The minimum storage retention period for the Archive tier is 90 days. If you delete or overwrite objects from the Archive tier before the minimum retention requirements are met, you are charged the prorated cost of storing the data for the full 90 days.
• When you restore objects, you are returning those objects to the Standard tier for access. You are billed for the Standard class tier while the restored objects reside in that tier.
You can use object lifecycle policy rules to automatically delete objects in an Archive Storage bucket based on the age of the object. You cannot, however, use object lifecycle policy rules to automatically restore archived objects to the Standard tier. See Restoring and Downloading Objects for information on restoring objects.

See Managing Buckets on page 3398 for detailed instructions on creating an Archive Storage bucket.

## Objects

Any type of data, regardless of content type, is stored as an object. The object is composed of the object itself and metadata about the object. Each object is stored in a bucket.

You upload objects to an Archive Storage bucket the same way you upload objects to a standard Object Storage bucket. The difference is that when you upload an object to an Archive Storage bucket, the object is immediately archived. You must first restore the object before you can download it.

Archived objects are displayed in the object listing of a bucket. You can also display the details of each object. See Managing Objects on page 3419 for detailed instructions on uploading objects to an Archive Storage bucket.

## Restoring and Downloading Objects

To download an object from Archive Storage, you must first restore the object. Restoration takes at most an hour from the time an Archive Storage restore request is made, to the time the first byte of data is retrieved. The retrieval time metric is measured as Time To First Byte (TTFB). How long the full restoration takes, depends on the size of the object. You can determine the status of the restoration by looking at the object Details. Once the status shows as Restored, you can then download the object.

After an object is restored, you have a window of time to download the object. By default, you have 24 hours to download an object, but you can alternatively specify a time from 1 to 240 hours. You can find out how much of the download time is remaining by looking at Available for Download in object Details. After the allotted download time expires, the object returns to Archive Storage. You can always access the metadata for an object, regardless of whether the object is in an archived or restored state.

See Managing Objects on page 3419 for detailed instructions on restoring, checking status of, and downloading Archive Storage objects.

## Ways to Access Archive Storage

Archive Storage and Object Storage use the same management interfaces:

- The Console is an easy-to-use, browser-based interface. To access Archive Storage in the console, do the following:
  - Sign in to the Console.
  - Open the navigation menu. Under Core Infrastructure, click Object Storage. A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).
  - Click the name of the Archive Storage tier bucket you want to manage.
- The command line interface (CLI) provides both quick access and full functionality without the need for programming. For more information, see Command Line Interface (CLI) on page 4192.
- The REST API provides the most functionality, but requires programming expertise. API Reference and Endpoints provides endpoint details and links to the available API reference documents. For general information about using the API, see REST APIs on page 4368. Object Storage is accessible with the following APIs:
  - Object Storage Service
  - Amazon S3 Compatibility API
  - Swift API (for use with Oracle RMAN)
• Oracle Cloud Infrastructure provides SDKs that interact with Archive Storage and Object Storage without you having to create a framework. For general information about using the SDKs, see Software Development Kits and Command Line Interface on page 4225.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API). IAM also manages user credentials for things like API signing keys, auth tokens, and customer secret keys for Amazon S3 Compatibility API. See User Credentials on page 2360 for details.

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control things like who can create users, create and manage the cloud network, launch instances, create buckets, and download objects. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see the Policy Reference on page 2167. For specific details about writing policies for Archive Storage, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For administrators:

• The policy Let Object Storage admins manage buckets and objects on page 2149 lets the specified group do everything with buckets and objects.
• Users that need to restore archived objects require the OBJECT_RESTORE permission.

WORM Compliance

Use retention rules to achieve WORM compliance with Archive Storage so that after the data is written, the data cannot be overwitten. Retention rules are configured at the bucket level and are applied to all individual objects in the bucket. You cannot update, overwrite, or delete objects or object metadata until the retention rule is deleted (indefinite rule) or for the duration specified (time-bound rules). You can, however, always restore an object from Archive Storage.

For more information, see Using Retention Rules to Preserve Data on page 3458.

Limits on Archive Storage Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

Other limits include:

• Number of namespaces per root compartment: 1
• Maximum object size: 10 TiB
• Maximum object part size in a multipart upload: 50 GiB
• Maximum number of parts in a multipart upload: 10,000
• Maximum object size allowed by PutObject API: 50 GiB
• Maximum size of object metadata: 2 K
Chapter 8

Audit

This chapter explains how to work with audit logs.

Overview of Audit

The Oracle Cloud Infrastructure Audit service automatically records calls to all supported Oracle Cloud Infrastructure public application programming interface (API) endpoints as log events. Currently, all services support logging by Audit. Object Storage service supports logging for bucket-related events, but not for object-related events. Log events recorded by the Audit service include API calls made by the Oracle Cloud Infrastructure Console, Command Line Interface (CLI), Software Development Kits (SDK), your own custom clients, or other Oracle Cloud Infrastructure services. Information in the logs includes the following:

• Time the API activity occurred
• Source of the activity
• Target of the activity
• Type of action
• Type of response

Each log event includes a header ID, target resources, timestamp of the recorded event, request parameters, and response parameters. You can view events logged by the Audit service by using the Console, API, or the SDK for Java. Data from events can be used to perform diagnostics, track resource usage, monitor compliance, and collect security-related events.

Version 2 Audit Log Schema

On October 8, 2019, Oracle introduced the Audit version 2 schema, which provides the following benefits:

• Captures state changes of resources
• Better tracking of long running APIs
• Provides troubleshooting information in logs

The new schema is being implemented over time. Oracle continues to provide Audit logs in the version 1 format, but you cannot access version 1 format logs from the Console. The Console displays only the version 2 format logs. However, not all resources are emitting logs using the version 2 schema. For those services that are not emitting in the version 2 format, Oracle converts version 1 logs to version 2 logs, leaving fields blank if information for the version 2 schema cannot be determined.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:
Audit

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Administrators: For an example of policy that gives groups access to audit logs, see Required IAM Policy on page 494. To modify the Audit log retention period, you must be a member of the Administrators group. See The Administrators Group and Policy on page 2125.

Contents of an Audit Log Event

The following explains the contents of an Audit log event. Every audit log event includes two main parts:

- Envelopes that act as a container for all event messages
- Payloads that contain data from the resource emitting the event message

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

Event Envelope

These attributes for an event envelope are the same for all events. The structure of the envelope follows the CloudEvents industry standard format hosted by the Cloud Native Computing Foundation (CNCF).

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cloudEventsVersion</td>
<td>The version of the CloudEvents specification.</td>
</tr>
<tr>
<td>contentType</td>
<td>Set to application/json. The content type of the data contained in the data attribute.</td>
</tr>
<tr>
<td>data</td>
<td>The payload of the event. Information within data comes from the resource emitting the event.</td>
</tr>
<tr>
<td>eventID</td>
<td>The UUID of the event. This identifier is not an OCID, but just a unique ID for the event.</td>
</tr>
</tbody>
</table>
### Audit

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>eventTime</strong></td>
<td>The time of the event, expressed in RFC 3339 timestamp format.</td>
</tr>
<tr>
<td><strong>eventType</strong></td>
<td>The type of event that happened.</td>
</tr>
<tr>
<td><strong>eventTypeVersion</strong></td>
<td>The version of the event type. This version applies to the payload of the event, not the envelope. Use cloudEventsVersion to determine the version of the envelope.</td>
</tr>
<tr>
<td><strong>source</strong></td>
<td>The resource that produced the event. For example, an Autonomous Database or an Object Storage bucket.</td>
</tr>
</tbody>
</table>

#### Payload

The data in these fields depends on which service produced the event log and the event type it defines.

#### Data

The data object contains the following attributes.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.additionalDetails</td>
<td>A container object for attributes unique to the resource emitting the event.</td>
</tr>
<tr>
<td>data.availabilityDomain</td>
<td>The availability domain where the resource resides.</td>
</tr>
<tr>
<td>data.compartmentId</td>
<td>The OCID of the compartment of the resource emitting the event.</td>
</tr>
<tr>
<td>data.compartmentName</td>
<td>The name of the compartment of the resource emitting the event.</td>
</tr>
<tr>
<td>data.definedTags</td>
<td>Defined tags added to the resource emitting the event.</td>
</tr>
<tr>
<td>data.eventGroupingId</td>
<td>This value links multiple audit events that are part of the same API operation. For example, a long running API operation that emits an event at the start and the end of the operation.</td>
</tr>
<tr>
<td>data.eventName</td>
<td>Name of the API operation that generated this event. Example: LaunchInstance</td>
</tr>
<tr>
<td>data.freeformTags</td>
<td>Free-form tags added to the resource emitting the event.</td>
</tr>
<tr>
<td>data.identity</td>
<td>A container object for identity attributes. See Identity.</td>
</tr>
</tbody>
</table>
### Audit

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.request</td>
<td>A container object for request attributes. See Request.</td>
</tr>
<tr>
<td>data.resourceId</td>
<td>An OCID or an ID for the resource emitting the event.</td>
</tr>
<tr>
<td>data.resourceName</td>
<td>The name of the resource emitting the event.</td>
</tr>
<tr>
<td>data.response</td>
<td>A container object for response attributes. See Response.</td>
</tr>
<tr>
<td>data.stateChange</td>
<td>A container object for state change attributes. See State Change.</td>
</tr>
</tbody>
</table>

### Identity

The identity object contains the following attributes.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.identity.authType</td>
<td>The type of authentication used.</td>
</tr>
<tr>
<td>data.identity.callerId</td>
<td>The OCID of the caller. The caller that made a request on behalf of the principal.</td>
</tr>
<tr>
<td>data.identity.callerName</td>
<td>The name of the user or service issuing the request. This value is the friendly name associated with callerId.</td>
</tr>
<tr>
<td>data.identity.consoleSessionId</td>
<td>This value identifies any Console session associated with this request.</td>
</tr>
<tr>
<td>data.identity.credentials</td>
<td>The credential ID of the user.</td>
</tr>
<tr>
<td>data.identity.ipAddress</td>
<td>The IP address of the source of the request.</td>
</tr>
<tr>
<td>data.identity.principalId</td>
<td>The OCID of the principal.</td>
</tr>
<tr>
<td>data.identity.principalName</td>
<td>The name of the user or service. This value is the friendly name associated with principalId.</td>
</tr>
<tr>
<td>data.identity.tenantId</td>
<td>The OCID of the tenant.</td>
</tr>
<tr>
<td>data.identity.userAgent</td>
<td>The user agent of the client that made the request.</td>
</tr>
</tbody>
</table>

### Request

The request object contains the following attributes.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.request.action</td>
<td>The HTTP method of the request.</td>
</tr>
<tr>
<td></td>
<td>Example: GET</td>
</tr>
<tr>
<td>data.request.headers</td>
<td>The HTTP header fields and values in the request.</td>
</tr>
<tr>
<td>data.request.id</td>
<td>The unique identifier of a request.</td>
</tr>
<tr>
<td>data.request.parameters</td>
<td>All the parameters supplied by the caller during this operation.</td>
</tr>
<tr>
<td>data.request.path</td>
<td>The full path of the API request.</td>
</tr>
<tr>
<td></td>
<td>Example: /20160918/instances/ocid1.instance.ocl.phx.&lt;unique_ID&gt;</td>
</tr>
</tbody>
</table>
Response

The response object contains the following attributes.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.response.headers</td>
<td>The headers of the response.</td>
</tr>
<tr>
<td>data.response.message</td>
<td>A friendly description of what happened during the operation.</td>
</tr>
<tr>
<td>data.response.payload</td>
<td>This value is included for backward compatibility with the Audit version 1 schema, where it contained metadata of interest from the response payload.</td>
</tr>
<tr>
<td>data.response.responseTime</td>
<td>The time of the response to the audited request, expressed in RFC 3339 timestamp format.</td>
</tr>
<tr>
<td>data.response.status</td>
<td>The status code of the response.</td>
</tr>
</tbody>
</table>

State Change

The state change object contains the following attributes.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.stateChange.current</td>
<td>Provides the current state of fields that may have changed during an operation. To determine how the current operation changed a resource, compare the information in this attribute to data.stateChange.previous.</td>
</tr>
<tr>
<td>data.stateChange.previous</td>
<td>Provides the previous state of fields that may have changed during an operation. To determine how the current operation changed a resource, compare the information in this attribute to data.stateChange.current.</td>
</tr>
</tbody>
</table>

An Example Audit Log

The following is an example an event recorded by the Audit service.

```json
{
    "eventType": "com.oraclecloud.ComputeApi.GetInstance",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ComputeApi",
    "eventId": "<unique_ID>",
    "eventTime": "2019-09-18T00:10:59.252Z",
    "contentType": "application/json",
    "data": {
        "eventGroupingId": null,
        "eventName": "GetInstance",
        "compartmentId": "ocid1.tenancy.oc1..<unique_ID>",
        "compartmentName": "compartmentA",
        "resourceName": "my_instance",
        "resourceId": "ocid1.instance.oc1.phx.<unique_ID>",
        "availabilityDomain": "<availability_domain>",
        "freeformTags": null,
        "definedTags": null,
        "identity": {
            "principalName": "ExampleName",
            "principalId": "ocid1.user.oc1..<unique_ID>",
            "authType": "natv",
            "callerName": null,
```
Viewing Audit Log Events

Audit provides records of API operations performed against supported services as a list of log events. The service logs events at both the tenant and compartment level.

When viewing events logged by Audit, you might be interested in specific activities that happened in the tenancy or compartment and who was responsible for the activity. You will need to know that the approximate time and date something happened and the compartment in which it happened to display a list of log events that includes the activity in question. List log events by specifying a time range on the 24-hour clock in Greenwich Mean Time (GMT), calculating the offset for your local time zone, as appropriate. New activity is appended to the existing list, usually within 15 minutes of the API call, though processing time can vary.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.
Audit

For administrators: The following policy statement gives the specified group (Auditors) the ability to view all the Audit event logs in the tenancy:

Allow group Auditors to read audit-events in tenancy

To give the group access to the Audit event logs in a specific compartment only (ProjectA), write a policy like the following:

Allow group Auditors to read audit-events in compartment ProjectA

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more details about policies for the Audit, see Details for the Audit Service on page 2177.

Searching and Filtering in the Console

When you navigate to Audit in the Console, a list of results is generated for the current compartment. Audit logs are organized by compartment, so if you are looking for a particular event, you must know which compartment the event occurred in. You can filter the list in all the following ways:

- Date and time
- Request Action Types (operations)
- Keywords

For example, users begin to report that their attempts to log in are failing. You want to use Audit to research the problem. Adjust the date and time to search for corresponding failures during a window of time that starts a little before the events were reported. Look for corresponding failures and similar operations preceding the failures to correlate a reason for the failures.

Note:
The service logs events at the time they are processed. There can be a delay between the time an operation occurs and when it is processed.

You can filter results by request actions to zero in on only the events with operations that interest you. For example, say that you only want to know about instances that were deleted during a specific time frame. Select a delete request action filter to see only the events with delete operations.

You can also filter by keywords. Keyword filters are powerful when combined with the values from audit event fields. For example, say that you know the user name of an account and want a list of all activity by that account in a particular time frame. Do a search using the user name as a keyword filter.

Every audit event contains the same fields, so search for values from those fields. To get a better understanding of what values are available, see Contents of an Audit Log Event on page 489.

Using the Console

To search log events

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Audit.
   The list of events that occurred in the current compartment is displayed.

2. Click one of the compartments under Compartment.
   Audit organizes logs by compartment, so if you are looking for a particular event, you must know which compartment the event occurred in.

3. Click in the Start Date box to choose the start date and time for the range of results you want to see. You can click the arrows on either side of the month to go backward or forward.
4. (Optional) Specify a time by doing one of the following:
   a. Click Time and specify an exact start time in thirty-minute increments.
   b. Type an exact time in the Start Date box.

      The service uses a 24-hour clock, so you must provide a number between 0 and 23 for the hour. Also remember to calculate the offset between Greenwich Mean Time (GMT) and your local time.

5. Repeat step 3 and 4 to choose an end date and time.

6. (Optional) In Request Action Types, specify one or more operations with which to filter results.
   - GET
   - POST
   - PUT
   - PATCH
   - DELETE

7. (Optional) In the Keywords box, type the text you want to find and click Search.

   Tip: If you want to find log events with a specific status code, include quotes (") around the code to avoid results that have those numbers embedded in a longer string.

The results are updated to include only log events that were processed within the time range and filters you specified.

If an event occurred in the recent past, you might have to wait to see it in the list. The service typically requires up to 15 minutes for processing.

If there are more than 100 results for the specified time range, you can click the right arrow next to the page number at the bottom of the page to advance to the next page of log events.

Tip:

If you get fewer than 100 results on the last page of a results list, you might still have more results, which you can access by clicking the right arrow. If there are more results, Audit prompts you.

If you want to view all the key-value pairs in a log event, see To view the details of a log event on page 496.

To view the details of a log event

View the details of your event:
   - To see only the top-level details, click the down arrow to the right of an event.
   - To see lower-level details, click {...} to the right of the collapsed parameter.

To copy the details of a log event

The following assumes that you have expanded a row in your results.
   - To copy an entire event, click the clipboard icon to the right of the event parameter.
   - To copy a portion of an event, click the clipboard icon to the right of the nested parameter or value you want to copy.

The log event is copied to your clipboard. The Audit service logs events in JSON format. You can paste the log event details into a text editor to save and review later or to use with standard log analysis tools.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operation to list audit log events:
   - ListEvents
Audit

Note:
This API is not intended for bulk-export operations. For bulk export, see Bulk Export of Audit Log Events on page 497.

Bulk Export of Audit Log Events

You can request a bulk export of audit logs, and within 5-10 business days Oracle support will begin making copies of the logs and adding them to buckets in your tenancy. The export includes logs for the specified regions, beginning after you make the request and continuing into the future.

Highlights

• Administrators have full control of the buckets and can provide access to others with IAM policy statements.
• Exported logs remain available indefinitely.

Tip:
You can automatically manage archiving and deleting logs using Object Storage. See Using Object Lifecycle Management on page 3466.

• Specify all the regions you want exported in your request. If you only request some regions, then decide later you want to add other regions, you must make another request.
• To disable your bulk export, contact Oracle support. New logs will stop being added to the bucket, and audit logs will only be available through the Console, based on the retention period you have defined.

Required IAM Policy

To access the bucket where Oracle exports the audit logs, you must be a member of the Administrators group. See The Administrators Group and Policy on page 2125.

Requesting an Export of Audit Logs

A member of the Administrators group for your tenancy must create a ticket at My Oracle Support and provide the following information:

• Ticket name: Export Audit Logs - <your_company_name>
• Tenancy OCID
• Regions

For example:

• Ticket name: Export Audit Logs - ACME
• Tenancy OCID: ocid1.tenancy.oc1.<unique_ID>
• Regions: US East (Ashburn), region identifier= us-ashburn-1; (US West (Phoenix)), region identifier = us-phoenix-1

Note:
It can take 5-10 business days before your My Oracle Support ticket is complete and the logs are available to you.

Bucket and Object Details

This section specifies the naming conventions of the bucket and objects you receive.

Bucket Name Format

Oracle support creates buckets for audit log exports using the following naming format:

oci-logs.audit.<compartment_OCID>
• **oci-logs** identifies that Oracle created this bucket.
• **_audit** identifies that the bucket contains audit events.
• **<compartment_OCID>** identifies the compartment where the audit events were generated.

For example:

```plaintext
oci-logs._audit.ocid1compartment.oc1..<unique_ID>
```

**Important:**

If the OCID of the compartment that generated the audit log contains a colon, your bucket name will not match the OCID. To create a bucket, Oracle must substitute colon characters (:) from the OCID with dot characters (.) in the bucket name.

**Object Name Format**

Objects use the following naming format:

```plaintext
<region>/<ad>/<YYYY-MM-DDTHH:MMZ>[_<seqNum>].log.gz
```

- **<region>** identifies the region where the audit events were generated.
- **<ad>** identifies the availability domain where the audit events were generated.
- **<YYYY-MM-DDTHH:MMZ>** identifies the start time of the earliest audit event listed in the object.
- **[_<seqNum>]** identifies a conditional sequence number. If present, this number means that either an event came in late or the object became too large to write. Sequence numbers start at two. Apply multiple sequence numbers to the original object in the order listed.

For example:

```plaintext
us-phoenix-1/ad1/2019-03-21T00:00Z.log.gz
us-phoenix-1/ad1/2019-03-21T00:00Z_2.log.gz
```

**File Format**

Files list a single audit event per line. For more information, see [Contents of an Audit Log Event](#) on page 489.

**Note:**

Audit introduced a version 2 schema of Audit logs but bulk export is currently only available for version 1 schema logs.
Chapter 9

Block Volume

This chapter explains how to create storage volumes and attach them to instances.

Overview of Block Volume

The Oracle Cloud Infrastructure Block Volume service lets you dynamically provision and manage block storage volumes. You can create, attach, connect, and move volumes, as well as change volume performance, as needed, to meet your storage, performance, and application requirements. After you attach and connect a volume to an instance, you can use the volume like a regular hard drive. You can also disconnect a volume and attach it to another instance without the loss of data.

These components are required to create a volume and attach it to an instance:

- **Instance**: A bare metal or virtual machine (VM) host running in the cloud.
- **Volume attachment**: There are two types of volume attachments:
  - **iSCSI** on page 501: A TCP/IP-based standard used for communication between a volume and attached instance.
  - **Paravirtualized** on page 501: A virtualized attachment available for VMs.
- **Volume**: There are two types of volumes:
  - **Block volume**: A detachable block storage device that allows you to dynamically expand the storage capacity of an instance.
  - **Boot volume**: A detachable boot volume device that contains the image used to boot a Compute instance. See Boot Volumes on page 609 for more information.

For additional Oracle Cloud Infrastructure terms, see the Glossary.

Block Volume is Always Free eligible. For more information about Always Free resources, including capabilities and limitations, see Oracle Cloud Infrastructure Free Tier on page 140.

Typical Block Volume Scenarios

**Scenario A: Expanding an Instance's Storage**

A common usage of Block Volume is adding storage capacity to an Oracle Cloud Infrastructure instance. After you have launched an instance and set up your cloud network, you can create a block storage volume through the Console or API. Then, you attach the volume to an instance using a volume attachment. After the volume is attached, you connect to the volume from your instance's guest OS using iSCSI. The volume can then be mounted and used by your instance.

**Scenario B: Persistent and Durable Storage**

A Block Volume volume can be detached from an instance and moved to a different instance without the loss of data. This data persistence enables you to migrate data between instances and ensures that your data is safely stored, even when it is not connected to an instance. Any data remains intact until you reformat or delete the volume.
To move your volume to another instance, unmount the drive from the initial instance, terminate the iSCSI connection, and attach the volume to the second instance. From there, you connect and mount the drive from that instance's guest OS to have access to all of your data.

Additionally, Block Volume volumes offer a high level of data durability compared to standard, attached drives. All volumes are automatically replicated for you, helping to protect against data loss, see Block Volume Durability on page 505.

**Scenario C: Instance Scaling**

When you terminate an instance, you can keep the associated boot volume and use it to launch a new instance with a different instance type or shape. This allows you to easily switch from a bare metal instance to a VM instance and vice versa, or scale up or scale down the number of cores for an instance. See Creating an Instance on page 695 for steps to launch an instance based on a boot volume.

**Volume Attachment Types**

When you attach a block volume to a VM instance, you have two options for attachment type, iSCSI or paravirtualized. Paravirtualized attachments simplify the process of configuring your block storage by removing the extra commands that are required before connecting to an iSCSI-attached volume. The trade-off is that IOPS performance for iSCSI attachments is greater than that for paravirtualized attachments. You should consider your requirements when selecting a volume's attachment type.

### Important:

Connecting to Volumes on Linux Instances

When connecting to volumes on Linux instances, if you want to automatically mount these volumes on instance boot, you need to use some specific options in the `/etc/fstab` file, or the instance may fail to launch. See Traditional fstab Options on page 528 and fstab Options for Block Volumes Using Consistent Device Paths on page 527 for more information.

**iSCSI**

iSCSI attachments are the only option when connecting a block volume to any of the following types of instances:

- Bare metal instances
- VM instances based on Windows images that were published before February 2018
- VM instances based on Linux images that were published before December 2017

After the volume is attached, you need to log in to the instance and use the `iscsiadm` command-line tool to configure the iSCSI connection. For more information about the additional configuration steps required for iSCSI attachments, see iSCSI Commands and Information on page 505, Connecting to a Volume on page 524, and Disconnecting From a Volume on page 562.

IOPS performance is better with iSCSI attachments compared to paravirtualized attachments. For more information about iSCSI-attached volume performance, see Block Volume Performance on page 567.

**Paravirtualized**

Paravirtualized attachments are an option when attaching volumes to the following types of VM instances:

- For VM instances launched from Oracle-provided images, you can select this option for Linux-based images published in December 2017 or later, and Windows images published in February 2018 or later.
- For VM instances launched from custom images, the volume attachment type is based on the volume attachment type from the VM the custom image was created from.
After you attach a volume using the paravirtualized attachment type, it is ready to use, and you do not need to run any additional commands. However, because of the overhead of virtualization, this reduces the maximum IOPS performance for larger block volumes.

**Volume Access Types**

When you attach a block volume, you can specify one of the following options for access type:

- **Read/write**: This is the default option for volume attachments. With this option, an instance can read and write data to the volume.
- **Read/write, shareable**: With this option, you can attach a volume to more than one instance at a time and those instances can read and write data to the volume. To prevent data corruption from uncontrolled read/write operations with multiple instance volume attachments you must install and configure a cluster-aware solution for system before you can use the volume, see Configuring Multiple Instance Volume Attachments with Read/Write Access on page 521 for more information.
- **Read-only**: With this option, an instance can only read data on the volume. It cannot update data on the volume. Specify this option to safeguard data against accidental or malicious modifications.

To change the access type for a block volume, you need to detach the volume and specify the new access type when you reattach the volume. For more information, see Detaching a Volume on page 563 and Attaching a Volume on page 517.

The access type for boot volumes is always read/write. If you want to change the access type, you need to stop the instance and detach the boot volume. You can then reattach it to another instance as a block volume, with read-only specified as the access type. For more information, see Detaching a Boot Volume on page 623 and Attaching a Volume on page 517.

**Device Paths**

When you attach a block volume to a compatible Linux-based instance, you can select a device path that remains consistent between instance reboots. This enables you to refer to the volume using a consistent device path. For example, you can use the device path when you set options in the /etc/fstab file to automatically mount the volume on instance boot.

Consistent device paths are supported on instances when all of the following things are true:

- The instance was created using an Oracle-provided image.
- The image is a Linux-based image.
- The image was released in November 2018 or later. For specific version numbers, see Oracle-Provided Image Release Notes.
- The instance was launched after January 11, 2019.

For instances launched using the image OCID or an existing boot volume, if the source image supports consistent device paths, the instance supports device paths.

Consistent device paths are not supported on Linux-based partner images or custom images that are created from other sources. This feature does not apply to Windows-based images.

**Important:**

You must select a device path when you attach a volume using the Console, it is required. Specifying a device path is optional when you attach a volume using the CLI, REST APIs, or SDK.

For more information about consistent device paths, see Connecting to Volumes With Consistent Device Paths on page 518.

**Regions and Availability Domains**

Volumes are only accessible to instances in the same availability domain. You cannot move a volume between availability domains or regions, they are only accessible within the region or availability domain they were created in.
However volume backups are not limited to the availability domain of the source volume, you can restore them to any availability domain within that region, see Restoring a Backup to a New Volume on page 557. You can also copy a volume backup to a new region and restore the backup to a volume in any availability domain in the new region, for more information see Copying a Volume Backup Between Regions on page 558.

For more information, see Regions and Availability Domains on page 180.

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Monitoring Resources**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

**Moving Resources**

You can move Block Volume resources such as block volumes, boot volumes, volume backups, volume groups, and volume group backups from one compartment to another. For more information, see Move Block Volume Resources Between Compartments on page 564.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.
Creating Automation with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

The following Block Volume resources emit events:

- Block volumes and block volume backups
- Boot volumes and boot volume backups
- Volume groups and volume group backups

Note:
For troubleshooting, see Known Issues - Block Volume for a list of known issues related to Block Volume events.

Block Volume Encryption

The Oracle Cloud Infrastructure Block Volume service always encrypts all block volumes, boot volumes, and volume backups at rest by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. By default all volumes and their backups are encrypted using the Oracle-provided encryption keys. Each time a volume is cloned or restored from a backup the volume is assigned a new unique encryption key.

You have the option to encrypt all of your volumes and their backups using the keys that you own and manage using the Vault service, for more information see Overview of Vault on page 3952. If you do not configure a volume to use the Vault service or you later unassign a key from the volume, the Block Volume service uses the Oracle-provided encryption key instead. This applies to both encryption at-rest and in-transit encryption.

For how to use your own key for new volumes, see Creating a Volume on page 515. See To assign a key to an existing Block Volume on page 3972 for how to assign or change the key for an existing volume.

All the data moving between the instance and the block volume is transferred over an internal and highly secure network. If you have specific compliance requirements related to the encryption of the data while it is moving between the instance and the block volume, the Block Volume service provides the option to enable in-transit encryption for paravirtualized volume attachments on virtual machine (VM) instances.

Important:
In-transit encryption for boot and block volumes is only available for virtual machine (VM) instances launched from Oracle-provided images, it is not supported on bare metal instances. It is also not supported in most cases for instances launched from custom images imported for "bring your own image" (BYOI) scenarios. To confirm support for certain Linux-based custom images and for more information contact Oracle support, see Getting Help and Contacting Support on page 125.

Block Volume Data Eradication

The Oracle Cloud Infrastructure Block Volume service uses eventual-overwrite data eradication, which guarantees that block volumes you delete cannot be accessed by anyone else and that the deleted data is eventually overwritten. When you terminate a volume, its associated data is overwritten in the storage infrastructure before any future volume allocations.

Block Volume Performance

Block Volume performance varies with volume size, see Block Volume Performance on page 567 for more information.

The Block Volume service's elastic performance feature enables you to dynamically change the volume performance. You can select one of the following volume performance options for your block volumes:

- Balanced
• Higher Performance
• Lower Cost

For more information about this feature and the performance options, see Block Volume Elastic Performance on page 581 and Changing the Performance of a Volume on page 582

**Block Volume Durability**

The Oracle Cloud Infrastructure Block Volume service offers a high level of data durability compared to standard, attached drives. All volumes are automatically replicated for you, helping to protect against data loss. Multiple copies of data are stored redundantly across multiple storage servers with built-in repair mechanisms. For service level objective, the Block Volume service is designed to provide 99.99 percent annual durability for block volumes and boot volumes. However, we recommend that you make regular backups to protect against the failure of an availability domain.

**Block Volume Capabilities and Limits**

Block Volume volumes can be created in sizes ranging from **50 GB** to **32 TB** in **1 GB** increments. By default, Block Volume volumes are **1 TB**.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Additional limits include:

• **Attached block volumes per instance**: 32
• **Attached boot volumes per instance**: 1

**Note:**

Boot volumes attached to an instance as a data volume and not as the instance’s boot volume count towards the limit for attached block volumes.

• **Number of backups**
  • Monthly universal credits: 100,000
  • Pay-as-you-go: 100,000

**iSCSI Commands and Information**

Block volumes attached with the iSCSI on page 501 attachment type use the iSCSI protocol to connect a volume to an instance. See Volume Attachment Types on page 501 for more information about volume attachment options.

Once the volume is attached, you need to log on to the instance and use the iscsiadm command-line tool to configure the iSCSI connection. After you configure the volume, you can mount it and use it like a normal hard drive.

To enhance security, Oracle enforces an iSCSI security protocol called CHAP that provides authentication between the instance and volume.

**Accessing a Volume’s iSCSI Information**

When you successfully attach a volume to an instance, Block Volume provides a list of iSCSI information. You need the following information from the list when you connect the instance to the volume.

• IP address
• Port
• CHAP user name and password (if enabled)
• IQN
The CHAP credentials are auto-generated by the system and cannot be changed. They are also unique to their assigned volume/instance pair and cannot be used to authenticate another volume/instance pair.

The Console provides this information on the details page of the volume’s attached instance. Click the Actions icon (three dots) on your volume’s row, and then click **iSCSI Information**. The system also returns this information when the **AttachVolume** API operation completes successfully. You can re-run the operation with the same parameter values to review the information.

See **Attaching a Volume** on page 517 and **Connecting to a Volume** on page 524 for step-by-step instructions.

### Recommended iSCSI Initiator Parameters for Linux-based Images

iSCSI attached volumes for Linux-based images are managed by the Linux iSCSI initiator service, `iscsid`. Oracle Cloud Infrastructure images use iSCSI default settings for the `iscsid` service’s parameters, with the exception of the following parameters:

- `node.startup = automatic`
- `node.session.timeo.replacement_timeout = 6000`
- `node.conn[0].timeo.noop_out_interval = 0`
- `node.conn[0].timeo.noop_out_timeout = 0`
- `node.conn[0].iscsi.HeaderDigest = None`

If you are using custom images, you should update the `iscsid` service configuration by modifying the `/etc/iscsi/iscsid.conf` file.

### Additional Reading

There is a wealth of information on the internet about iSCSI and CHAP. If you need more information on these topics, try the following pages:

- [Oracle Linux 8 Managing Storage Devices - Working with iSCSI Devices](#)
- [Oracle Linux Administrator's Guide for Release 7 - About iSCSI Storage](#)
- [Oracle Linux Administrator's Guide for Release 6 - About iSCSI Storage](#)
- [Troubleshooting iSCSI Configuration Problems](#)

### Volume Groups

The Oracle Cloud Infrastructure Block Volume service provides you with the capability to group together multiple volumes in a volume group. A volume group can include both types of volumes, boot volumes, which are the system disks for your Compute instances, and block volumes for your data storage. You can use volume groups to create volume group backups and clones that are point-in-time and crash-consistent.

This simplifies the process to create time-consistent backups of running enterprise applications that span multiple storage volumes across multiple instances. You can then restore an entire group of volumes from a volume group backup.

Similarly, you can also clone an entire volume group in a time-consistent and crash-consistent manner. A deep disk-to-disk and fully isolated clone of a volume group, with all the volumes associated in it, becomes available for use within a matter of seconds. This speeds up the process of creating new environments for development, quality assurance, user acceptance testing, and troubleshooting.

For more information about Block Volume-backed system disks, see **Boot Volumes** on page 609. For more information about Block Volume backups see **Overview of Block Volume Backups** on page 540. See **Cloning a Volume** on page 560 for more information about Block Volume clones.

This capability is available using the Console, command line interface (CLI), SDKs, or REST APIs.
Volume groups and volume group backups are high-level constructs that allow you to group together multiple volumes. When working with volume groups and volume group backups, keep the following in mind:

- You can only add a volume to a volume group when the volume status is available.
- You can add up to 32 volumes in a volume group, up to a maximum size limit of 128 TB. For example, if you wanted to add 32 volumes of equal size to a volume group, the maximum size for each volume would be 4 TB. Or you could add volumes that vary in size, however the overall combined size of all the block and boot volumes in the volume group must be 128 TB or less. Make sure you account for the size of any boot volumes in your volume group when considering volume group size limits.

- Each volume may only be in one volume group.
- When you clone a volume group, a new group with new volumes are created. For example, if you clone a volume group containing three volumes, once this operation is complete, you will now have two separate volume groups and six different volumes with nothing shared between the volume groups.
- When you update a volume group using the CLI, SDKs, or REST APIs you need to specify all the volumes to include in the volume group each time you use the update operation. If you do not include a volume ID in the update call, that volume will be removed from the volume group.
- When you delete a volume group the individual volumes in the group are not deleted, only the volume group is deleted.
- When you delete a volume that is part of a volume group you must first remove it from the volume group before you can delete it.
- When you delete a volume group backup, all the volume backups in the volume group backup are deleted.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes, backups, and volume groups.

See the following policy examples for working with volume groups:

- Let users create a volume group on page 2147 lets the specified group create a volume group from a set of volumes.
- Let users clone a volume group on page 2148 lets the specified group clone a volume group from an existing volume group.
- Let users create a volume group backup on page 2148 lets the specified group create a volume group backup.
- Let users restore a volume group backup on page 2148 lets the specified group create a volume group by restoring a volume group backup.

**Tip:**

When users create a backup from a volume or restore a volume from a backup, the volume and backup don't have to be in the same compartment. However, users must have access to both compartments.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.
Managing Volume Groups

This section covers how to perform tasks related to managing your volume groups using the Console, command line interface (CLI), and REST APIs.

Using the Console

To create a volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. Click Create Volume Group.
3. Fill in the required volume information:
   - **Name**: A user-friendly name or description. Avoid entering confidential information.
   - **Compartment**: The compartment for the volume group.
   - **Availability Domain**: The availability domain for the volume group.
   - **Backup Policy**: The backup policy to use for scheduled backups. For more information, see Policy-Based Volume Group Backups on page 514.
   - **Volumes**: For each volume you want to add, select the compartment containing the volume and then the volume to add. Click + Volume to add additional volumes.
4. Click Create Volume Group.

To view the volumes in a volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. In the Volume Groups list, click the volume group you want to view the volumes for.
3. To view the block volumes for the volume group, in Resources, click Block Volumes.
4. To view the boot volumes for the volume group, in Resources, click Boot Volumes.

To add block volumes to an existing volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. In the Volume Groups list, click the volume group you want to add the volume to.
3. In Resources, click Block Volumes.
4. Click Add Block Volumes.
5. For each block volume you want to add, select the compartment containing the volume and then select the volume to add. Click + Volume to add additional volumes.
6. Once you have selected all the block volumes to add to the volume group, click Add.

To remove block volumes from an existing volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. In the Volume Groups list, click the volume group you want to add the volume to.
3. In Resources, click Block Volumes.
4. In Actions menu for the block volume you want to remove, click Remove.
5. In the Confirm dialog, click Remove.

**Note:**

You cannot add a volume with an existing backup policy assignment to a volume group with a backup policy assignment. You must first remove the backup policy assignment from the volume before you can add it to the volume group.

To add boot volumes to an existing volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. In the **Volume Groups** list, click the volume group you want to add the volume to.
3. In **Resources**, click **Boot Volumes**.
4. Click **Add Boot Volumes**.

   **Note:**
   You cannot add a volume with an existing backup policy assignment to a volume group with a backup policy assignment. You must first remove the backup policy assignment from the volume before you can add it to the volume group.

5. For each boot volume you want to add, select the compartment containing the volume and then select the volume to add. Click + **Volume** to add additional volumes.
6. Once you have selected all the boot volumes to add to the volume group, click **Add**.

**To remove boot volumes from an existing volume group**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Groups**.
2. In the **Volume Groups** list, click the volume group you want to add the volume to.
3. In **Resources**, click **Boot Volumes**.
4. In the **Actions** menu for the boot volume you want to remove, click **Remove**.
5. In the **Confirm** dialog, click **Remove**.

**To create a clone of the volume group**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Groups**.
2. In the **Volume Groups** list, click **Create Volume Group Clone** in the **Actions** menu for the volume group you want to clone.

**To delete the volume group**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Groups**.
2. In the **Volume Groups** list, click the volume group you want to delete.
3. On the **Volume Group Details** page, click **Terminate**.
4. On the **Terminate Volume Group** dialog, click **Terminate**.

   **Note:**
   When you delete a volume group the individual volumes in the group are not deleted, only the volume group is deleted.

**Using the CLI**

For information about using the CLI, see [Command Line Interface (CLI)](#) on page 4192.

**To retrieve information about the supported operations**

Open a command prompt and run the one of the following commands to retrieve the information.

- To retrieve the supported operations for volume groups:

  `oci bv volume-group --help`

- To retrieve the supported operations for volume group backups:

  `oci bv volume-group-backup --help`

- To retrieve help for a specific volume group operation:

  `oci bv volume-group <operation_name> --help`
• To retrieve help for a specific volume group backup operation:

```
oci bv volume-group-backup <operation_name> --help
```

**To list the volume groups in a specified compartment**

Open a command prompt and run:

```
oci bv volume-group list --compartment-id <compartment_ID>
```

For example:

```
oci bv volume-group list --compartment-id ocid1.compartment.oc1..<unique_ID>
```

**To create a volume group from existing volumes**

Open a command prompt and run:

```
oci bv volume-group create --compartment-id <compartment_ID> --availability-domain <external_AD> --source-details <Source_details_JSON>
```

Volume status must be available to add it to a volume group.

For example:

```
oci bv volume-group create --compartment-id ocid1.compartment.oc1..<unique_ID> --availability-domain ABbv:PHX-AD-1 --source-details '{"type": "volumeIds", "volumeIds": ["ocid1.volume.oc1.phx.<unique_ID_1>", "ocid1.volume.oc1.phx.<unique_ID_2>" ]}'
```

**To clone a volume group from another volume group**

Open a command prompt and run:

```
oci bv volume-group create --compartment-id <compartment_ID> --availability-domain <external_AD> --source-details <Source_details_JSON>
```

For example:

```
oci bv volume-group create --compartment-id ocid1.compartment.oc1..<unique_ID> --availability-domain ABbv:PHX-AD-1 --source-details '{"type": "volumeGroupId", "volumeGroupId": "ocid1.volumegroup.oc1.phx.<unique_ID>" }'
```

**To retrieve a volume group**

Open a command prompt and run:

```
oci bv volume-group get --volume-group-id <volume-group-ID>
```

For example:

```
oci bv volume-group get --volume-group-id ocid1.volumegroup.oc1.phx.<unique_ID>
```
To update display name or add/remove volumes from a volume group

Open a command prompt and run:

```
oci bv volume-group update --volume-group-id <volume-group_ID> --volume-ids <volume_ID_JSON>
```

You can update the volume group display name along with adding or removing volumes from the volume group. The volume group is updated to include only the volumes specified in the update operation. This means that you need to specify the volume IDs for all of the volumes in the volume group each time you update the volume group.

The following example changes the volume group's display name for a volume group with two volumes:

```
oci bv volume-group update --volume-group-id ocid1.volumegroup.oc1.phx.<unique_ID> --volume-ids '["ocid1.volume.oc1.phx.<unique_ID_1>","ocid1.volume.oc1.phx.<unique_ID_2>"]' --display-name "new display name"
```

If you specify volumes in the command that are not part of the volume group they are added to the group. Any volumes not specified in the command are removed from the volume group.

To delete a volume group

Open a command prompt and run:

```
oci bv volume-group delete --volume-group-id <volume-group_ID>
```

When you delete a volume group, the individual volumes in the group are not deleted, only the volume group is deleted.

For example:

```
oci bv volume-group delete --volume-group-id ocid1.volumegroup.oc1.phx.<unique_ID>
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations for working with volume groups:

- ListVolumeGroups
- CreateVolumeGroup
- DeleteVolumeGroup
- GetVolumeGroup
- UpdateVolumeGroup

Volume Group Backups

A volume group backup provides coordinated point-in-time-consistent backups of all the volumes in a volume group automatically. You can perform most of the same backup operations and tasks with volume groups that you can perform with individual block volumes and boot volumes. You can restore a volume group backup to a volume group, or you can restore individual volumes in the volume group from volume backups. With volume group backups, you can manage the backup settings for several volumes in one place, consistently. This simplifies the process to create time-consistent backups of running enterprise applications that span multiple storage volumes across multiple instances.

For a general overview of the Block Volume's service backup functionality, see Overview of Block Volume Backups on page 540.
**Source Region**

Volume group backups include a **Source Region** field. This specifies the region for the volume group that the backup was created from. For volume group backups copied from another region, this field will show the region the volume group backup was copied from.

**Manual Volume Group Backups**

Manual backups are on-demand one-off backups that you can launch immediately for volume groups by following the steps outlined in the procedures in this section. For general information about the manual backups feature for the Block Volume service, see **Manual Backups** on page 540.

*Using the Console*

To create a backup of the volume group

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Groups**.
2. In the **Volume Groups** list, click **Create Volume Group Backup** in the **Actions** menu for the volume group you want to create a backup for.

To restore a volume group from a volume group backup

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Group Backups**.
2. In the **Volume Group Backups** list, click the volume group backup you want to restore.
3. Click **Create Volume Group**.
4. Fill in the required volume information:
   - **Name**: A user-friendly name or description. Avoid entering confidential information.
   - **Compartment**: The compartment for the volume group.
   - **Availability Domain**: The availability domain for the volume group.
5. Click **Create Volume Group**.

*Using the CLI*

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192.

To list volume backup groups

Open a command prompt and run:

```
oci bv volume-group-backup list --compartment-id <compartment_ID>
```

For example:

```
oci bv volume-group-backup list --compartment-id ocid1.compartment.oc1..<unique_ID>
```

To create a volume group backup

Open a command prompt and run:

```
oci bv volume-group-backup create --volume-group-id <volume-group_ID>
```

For example:

```
oci bv volume-group-backup create --volume-group-id ocid1.volumegroup.oc1.phx.<unique_ID>
```

To retrieve a volume group backup
Open a command prompt and run:

```bash
oci bv volume-group-backup get --volume-group-backup-id <volume-group-backup_ID>
```

For example:

```bash
oci bv volume-group-backup get --volume-group-backup-id ocid1.volumegroupbackup.oc1.phx.<unique_ID>
```

To update display name for a volume group backup

Open a command prompt and run:

```bash
oci bv volume-group-backup update --volume-group-backup-id <volume-group-backup_ID> --display-name <new_display_name>
```

You can only update the display name for the volume group backup.

For example:

```bash
oci bv volume-group-backup update --volume-group-backup-id ocid1.volumegroupbackup.oc1.phx.<unique_ID> --display-name "new display name"
```

To restore a volume group from a volume group backup

Open a command prompt and run:

```bash
oci bv volume-group create --compartment-id <compartment_ID> --availability-domain <external_AD> --source-details <Source_details_JSON>
```

For example:

```bash
oci bv volume-group create --compartment-id ocid1.compartment.oc1..<unique_ID> --availability-domain ABby:PHX-AD-1 --source-details '{"type": "volumeGroupBackupId", "volumeGroupBackupId": "ocid1.volumegroup.oc1.sea.<unique_ID>"}'
```

To delete a volume group backup

Open a command prompt and run:

```bash
oci bv volume-group-backup delete --volume-group-backup-id <volume-group-backup_ID>
```

When you delete a volume group backup, all volume backups in the group are deleted.

For example:

```bash
oci bv volume-group-backup delete --volume-group-backup-id ocid1.volumegroupbackup.oc1.phx.<unique_ID>
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations for working with volume group backups:

- ListVolumeGroupBackups
- CreateVolumeGroupBackup
• DeleteVolumeGroupBackup
• GetVolumeGroupBackup
• UpdateVolumeGroupBackup

Policy-Based Volume Group Backups

These are automated scheduled backups as defined by the backup policy assigned to the volume group. Policy-based backups for volume groups are essentially the same as policy-based backups for block volumes, the main difference is that the backup policy is applied to all the volumes in the volume group instead of a single volume. For general information about policy-based backups, see Policy-Based Backups on page 547. The process to create and configure user defined backup policies are the same for volume groups as they are for volumes, see Creating and Configuring User Defined Backup Policies on page 552 for these procedures.

Note:
Oracle defined backup policies are not supported for scheduled volume group backups.

Caution:
Vault encryption keys for volumes are not copied to the destination region for scheduled volume and volume group backups enabled for cross region copy. For more information, see Vault encryption keys not copied to destination region for scheduled cross region backup copies.

Managing Backup Policy Assignments to Volume Groups

The backup policy assigned to a volume group defines the frequency and schedule for volume group backups. This section covers how to perform tasks related to managing the backup policy assignments for your volume groups using the Console, command line interface (CLI), and REST APIs.

If a volume group has an assigned backup policy, you must remove any backup policy assignments from volumes before you can add them to the volume group.

Before you can assign a backup policy to an existing volume group containing one or more volumes with assigned backup policies, you must remove those policy assignments from the individual volumes before you can assign the policy to the volume group.

Using the Console

To assign a backup policy to a volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. Click the volume group for which you want to assign a backup policy to.
3. On the Volume Group Details page click Edit.
4. In the BACKUP POLICIES section, select the compartment containing the backup policies.
5. Select the appropriate backup policy for your requirements.
6. Click Save Changes.

To change a backup policy assigned to a volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. Click the volume group for which you want to change the backup policy for.
3. On the Volume Group Details page click Edit.
4. In the BACKUP POLICIES section, select the compartment containing the backup policy.
5. Select the backup policy you want to switch to.
6. Click Save Changes.

To remove a backup policy assigned to a volume group

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Volumes Groups.
2. Click the volume group for which you want to remove the backup policy for.
3. On the Volume Group Details page click Edit.
4. In the **BACKUP POLICIES** section, select **None** from the list, and then click **Save Changes**.

**Using the CLI**

For information about using the CLI, see [Command Line Interface (CLI)] on page 4192.

**To assign a backup policy to a volume group**

Open a command prompt and run:

```bash
oci bv volume-backup-policy-assignment create --asset-id <volume_group_ID> --policy-id <policy_ID>
```

For example:

```bash
oci bv volume-backup-policy-assignment create --asset-id ocid1.volumegroup.oc1..<unique_ID> --policy-id ocid1.volumebackuppolicy.oc1..<unique_ID>
```

**To get the backup policy assigned to a volume group**

Open a command prompt and run:

```bash
oci bv volume-backup-policy-assignment get-volume-backup-policy-asset-assignment --asset-id <volume_group_ID>
```

For example:

```bash
oci bv volume-backup-policy-assignment get-volume-backup-policy-asset-assignment --asset-id ocid1.volumegroup.oc1..<unique_ID>
```

**To retrieve a specific backup policy assignment**

Open a command prompt and run:

```bash
oci bv volume-backup-policy-assignment get --policy-assignment-id <backup-policy-ID>
```

For example:

```bash
oci bv volume-backup-policy-assignment get --policy-assignment-id ocid1.volumebackuppolicyassignment.oc1.phx.<unique_ID>
```

**Using the API**

Use the following operations to manage backup policy assignments to volume groups:

- CreateVolumeBackupPolicyAssignment
- DeleteVolumeBackupPolicyAssignment
- GetVolumeBackupPolicyAssetAssignment
- GetVolumeBackupPolicyAssignment

For information about using the API and signing requests, see [REST APIs] on page 4368 and [Security Credentials] on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface] on page 4225.

**Creating a Volume**

You can create a volume using Block Volume.
**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

For administrators: The policy in *Let volume admins manage block volumes, backups, and volume groups* on page 2146 lets the specified group do everything with block volumes and backups.

If you’re new to policies, see *Getting Started with Policies* on page 2135 and *Common Policies* on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see *Details for the Core Services* on page 2181.

**Monitoring Resources**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see *Monitoring Overview* on page 2660 and *Notifications Overview* on page 3350.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see *Resource Tags* on page 211.

**Using the Console**

1. Open the navigation menu. Under *Core Infrastructure*, go to *Block Storage* and click *Block Volumes*.
2. Click *Create Block Volume*.
3. Fill in the required volume information:
   - **Name**: A user-friendly name or description. Avoid entering confidential information.
   - **Domain**: Must be in the same *availability domain* as the instance.
   - **Size**: Must be between 50 GB and 32 TB. You can choose in 1 GB increments within this range. The default is 1024 GB. If you choose a size outside of your service limit, you may be prompted to request an increase. For more information, see *Service Limits* on page 215.
   - **Backup Policy**: Optionally, you can select the appropriate backup policy for your requirements. See *Policy-Based Backups* on page 547 for more information about backup policies.
   - **Volume Performance**: Optionally, you can select the appropriate performance setting for your requirements. See *Block Volume Elastic Performance* on page 581 for more information about volume performance options. The default option is *Balanced*.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see *Resource Tags* on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
   - **Encryption**: Optionally, you can encrypt the data in this volume using your own Vault encryption key. To use Vault for your encryption needs, select the *Encrypt using customer-managed keys* radio button. Then, select the *Vault compartment* and *Vault* that contain the master encryption key you want to use. Also select the *Master encryption key compartment* and *Master encryption key*. For more information about encryption, see *Overview of Vault* on page 3952.
4. Click *Create Block Volume*.

   The volume will be ready to attach once its icon no longer lists it as *PROVISIONING* in the volume list. For more information, see *Attaching a Volume* on page 517.
Using the API

To create a volume, use the following operation:

- CreateVolume

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Attaching a Volume

You can attach a volume to an instance in order to expand the available storage on the instance. If you specify iSCSI on page 501 as the volume attachment type, you must also connect and mount the volume from the instance for the volume to be usable. For more information, see Volume Attachment Types on page 501 and Connecting to a Volume on page 524.

You can attach volumes to more than one instance at a time, see Attaching a Volume to Multiple Instances on page 520. To prevent data corruption from uncontrolled read/write operations with multiple instance volume attachments you must install and configure a clustered file system before you can use the volume, see Configuring Multiple Instance Volume Attachments with Read/Write Access on page 521 for more information.

Note:
You should only attach Linux volumes to Linux instances and Windows volumes to Windows instances.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to attach/detach existing block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Security Zones

Security Zones ensure that your cloud resources comply with Oracle security principles. If any operation on a resource in a security zone compartment violates a policy for that security zone, then the operation is denied.

The following security zone policies affect your ability to attach block volumes to Compute instances.

- All block volumes attached to a Compute instance in a security zone must themselves be in a security zone.
- Block volumes in a security zone cannot be attached to a Compute instance that is not in a security zone.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the Instances list, click the instance that you want to attach a volume to.
3. In the Resources section, click Attached Block Volumes.
4. Click Attach Block Volume.
5. Select the volume attachment type, iSCSI, Paravirtualized, or Let Oracle Cloud Infrastructure choose the best attachment type.

For more information, see Volume Attachment Types on page 501.
6. In the **Block Volume Compartment** drop-down list, select the compartment.
7. Specify the volume you want to attach to. To use the volume name, choose **SELECT VOLUME** and then select the volume from the **Block Volume** drop-down list. To specify the volume OCID, choose **ENTER VOLUME OCID** and then enter the OCID into the **Block Volume OCID** field.
8. If the instance supports consistent device paths, and the volume you are attaching is not a boot volume, select a path from the **Device Path** drop-down list when attaching. This is required and enables you to specify a device path for the volume attachment that remains consistent between instance reboots.

   For more information about this feature and the instances that support it, see **Connecting to Volumes With Consistent Device Paths** on page 518

   Tip:
   
   You must select a device path when you attach a volume from the Console, it is not optional. Specifying a device path is optional when you attach a volume using the CLI, REST APIs, or SDK.

9. Select the access type, **Read/Write** or **Read-only**.

   For more information, see **Volume Access Types** on page 502.

10. For paravirtualized volume attachments on virtual machine (VM) instances, you can optionally encrypt data that is transferred between the instance and the Block Volume service storage servers. To do this, select the **Use in-transit encryption** check box. If you configured the volume to use an encryption key that you manage using the Vault service, this key is used for in-transit encryption. Otherwise, the Oracle-provided encryption key is used. See **Block Volume Encryption** on page 504 for more information.

11. Click **Attach**.

    When the volume's icon no longer lists it as **Attaching**, if the attachment type is **Paravirtualized** on page 501, you can use the volume. If the attachment type is **iSCSI** on page 501, you need to connect to the volume first. For more information, see **Connecting to a Volume** on page 524.

    On Linux-based instances, if you want to automatically mount volumes on instance boot, you need to set some specific options in the **/etc/fstab** file, or the instance may fail to launch. This applies to both iSCSI and paravirtualized attachment types. For volumes using consistent device paths, see **fstab Options for Block Volumes Using Consistent Device Paths** on page 527. For all other volumes, see **Traditional fstab Options** on page 528.

**Using the API**

To attach a volume to an instance, use the following operation:

- **AttachVolume**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

**Connecting to Volumes With Consistent Device Paths**

Oracle Cloud Infrastructure supports consistent device paths for block volumes that are attached to compatible Linux-based instances. When you attach a block volume to an instance, you must select a device path that remains consistent between instance reboots. This enables you to use a consistent device path when you refer to the volume to perform tasks such as:

- Creating partitions.
- Creating file systems.
- Mounting file systems.
- Specifying options in the **/etc/fstab** file to ensure that volumes are mounted properly when automatically mounting volumes on instance boot. For more information, see **fstab Options for Block Volumes Using Consistent Device Paths** on page 527.
When you use consistent device paths on compatible Linux-based instances, the boot volume’s device path is:

```
/dev/oracleoci/oraclevda
```

**Note:**
Device paths are not available when you attach a boot volume as a data volume to a second instance.

**Images that Support Consistent Device Paths**

Consistent device paths are supported on instances when all of the following things are true:

- The instance was created using an Oracle-provided image.
- The image is a Linux-based image.
- The image was released in November 2018 or later. For specific version numbers, see Oracle-Provided Image Release Notes.
- The instance was launched after January 11, 2019.

For instances launched using the image OCID or an existing boot volume, if the source image supports consistent device paths, the instance supports device paths.

Consistent device paths are not supported on Linux-based partner images or custom images that are created from other sources. This feature does not apply to Windows-based images.

**Important:**
You must select a device path when you attach a volume using the Console, it is required. Specifying a device path is optional when you attach a volume using the CLI, REST APIs, or SDK.

**Device Paths in the Console**

You select a device path when you attach a block volume to an instance.

If you specify a device path, the path appears in the Attached Block Volumes list for an instance, in the Device Path field. An example is shown in the following screenshot.

**Device Paths on the Instance**

Use the following sample commands to perform various configuration tasks on the attached volume. Commands are provided for volumes that use consistent device paths and for volumes that don’t.

**Creating a partition with fdisk**

- No device path specified:
  ```
  fdisk /dev/sdb
  ```

- Device path specified:
  ```
  fdisk /dev/oracleoci/oraclevdb
  ```

**Creating an ext3 file system**

- No device path specified:
  ```
  /sbin/mkfs.ext3 /dev/sdb1
  ```
• Device path specified:
  
  
  ```bash
/sbin/mkfs.ext3 /dev/oracleoci/oraclevdb1
  ```

**Updating the /etc/fstab file**

• No device path specified:
  
  ```bash
UUID=84dc162c-43dc-429c-9ac1-b511f3f0e23c /oradiskvdb1 xfs
defaults,_netdev,noatime 0 2
  ```

• Device path specified:
  
  ```bash
/dev/oracleoci/oraclevdb1 /oradiskvdb1 xfs
defaults,_netdev,noatime 0 2
  ```

**Mounting the file system**

• No device path specified:
  
  ```bash
mount /dev/sdb1 /oradiskvdb1
  ```

• Device path specified:
  
  ```bash
mount /dev/oracleoci/oraclevdb1 /oradiskvdb1
  ```

### Attaching a Volume to Multiple Instances

The Oracle Cloud Infrastructure Block Volume service provides the capability to attach a block volume to multiple Compute instances. With this feature, you can share block volumes across instances in read/write or read-only mode. Attaching block volumes as read/write and shareable enables you to deploy and manage your cluster-aware solutions.

This topic describes how to attach block volumes as shareable, along with the limits and considerations for this feature.

See [Volume Access Types](#) on page 502 for more information about the available access type options. For attaching volumes to single instances, see [Attaching a Volume](#) on page 517.

### Limits and Considerations

• The Block Volume service does not provide coordination for concurrent write operations to block volumes attached to multiple instances, so if you configure the block volume as read/write and shareable you must deploy a cluster aware system or solution on top of the shared storage, see [Configuring Multiple Instance Volume Attachments with Read/Write Access](#) on page 521.

• Once you attach a block volume to an instance as read-only, it can only be attached to other instances as read-only. If you want to attach the block volume to an instance as read/write, you need to detach the block volume from all instances and then you can reattach the block volume to instances as read/write.

• If the block volume is already attached to an instance as read/write non-shareable you can't attach it to another instance until you detach it from the first instance. You can then reattach it to both the first and second instances as read/write shareable.

• You can't delete a block volume until it has been detached from all instances it was attached to. When viewing the instances attached to the block volume from the Resources section of the Volume Details page, you should note that only instances in the selected compartment will be displayed. You may need to change the compartment to list additional instances that are attached to the volume.

• You can attach a block volume as read/write shareable or read-only shareable up to a maximum of eight instances.

• Block volumes attached as read-only are configured as shareable by default.

• Performance characteristics described in [Block Volume Performance](#) on page 567 are per volume, so when a block volume is attached to multiple instances the performance is shared across all the attached instances.
Configuring Multiple Instance Volume Attachments with Read/Write Access

The Block Volume service does not provide coordination for concurrent write operations to volumes attached to multiple instances. To prevent data corruption from uncontrolled read/write operations you must install and configure a cluster aware system or solution such as Oracle Cluster File System version 2 (OCFS2) on top of the shared storage before you can use the volume.

You can see an sample walkthrough of scenario using OCFS2 described in Using the Multiple-Instance Attach Block Volume Feature to Create a Shared File System on Oracle Cloud Infrastructure. The summary of the required steps for this scenario are:

1. Attach the block volume to an instance as Read/Write-Shareable using the Console, CLI, or API.
2. Set up your OCFS2/O2CB cluster nodes.
3. Create your OCFS2 file system and mount point.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to attach/detach existing block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

To attach a volume to multiple instances from the Instance details page

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the Instances list, click the instance that you want to attach a volume to.
3. In the Resources section, click Attached Block Volumes.
4. Click Attach Block Volume.
5. Select the volume attachment type, iSCSI or Paravirtualized.
   For more information, see Volume Attachment Types on page 501.
6. Select the volume access type. Select Read/Write-Shareable if you want to enable read/write attachments to multiple instances or Read-only-Shareable for read-only attachments to multiple instances.
   For more information, see Volume Access Types on page 502.
7. In the Block Volume Compartment drop-down list, select the compartment.
8. Specify the volume you want to attach to. To use the volume name, choose SELECT VOLUME and then select the volume from the Block Volume drop-down list. To specify the volume OCID, choose ENTER VOLUME OCID and then enter the OCID into the Block Volume OCID field.
9. If the instance supports consistent device paths select a path from the Device Path drop-down list when attaching. This is required and enables you to specify a device path for the volume attachment that remains consistent between instance reboots.
   For more information about this feature and the instances that support it, see Connecting to Volumes With Consistent Device Paths on page 518

Tip:

You must select a device path when you attach a volume from the Console, it is not optional. Specifying a device path is optional when you attach a volume using the CLI, REST APIs, or SDK.
For paravirtualized volume attachments on virtual machine (VM) instances, you can optionally encrypt data that is transferred between the instance and the Block Volume service storage servers. To do this, select the Use in-transit encryption check box. If you configured the volume to use an encryption key that you manage using the Vault service, this key is used for in-transit encryption. Otherwise, the Oracle-provided encryption key is used. See Block Volume Encryption on page 504 for more information.

Click Attach.

When the volume's icon no longer lists it as Attaching, if the attachment type is Paravirtualized on page 501, you can use the volume. If the attachment type is iSCSI on page 501, you need to connect to the volume first. For more information, see Connecting to a Volume on page 524.

On Linux-based instances, if you want to automatically mount volumes on instance boot, you need to set some specific options in the /etc/fstab file, or the instance may fail to launch. This applies to both iSCSI and paravirtualized attachment types. For volumes using consistent device paths, see fstab Options for Block Volumes Using Consistent Device Paths on page 527. For all other volumes, see Traditional fstab Options on page 528.

To attach a volume to multiple instances from the Block Volume details page

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. In the Block Volumes list, click the block volume that you want to attach to an instance.
3. In the Resources section, click Attached Instances.
4. Click Attach to Instance.
5. Select the volume attachment type, iSCSI or Paravirtualized.
6. Select the volume access type. Select Read/Write-Shareable if you want to enable read/write attachments to multiple instances or Read-only-Shareable for read-only attachments to multiple instances.
7. In the Choose Instance drop-down list, select the instance. Click Change Compartment if the instance is in a different compartment than the default one listed. If you want to specify the instance using the OCID, select the ENTER INSTANCE OCID option and then copy the OCID in the textbox.
8. If the instance supports consistent device paths select a path from the Device Path drop-down list when attaching. This is required and enables you to specify a device path for the volume attachment that remains consistent between instance reboots.

For more information about this feature and the instances that support it, see Connecting to Volumes With Consistent Device Paths on page 518

Tip:
You must select a device path when you attach a volume from the Console, it is not optional. Specifying a device path is optional when you attach a volume using the CLI, REST APIs, or SDK.

9. For paravirtualized volume attachments on virtual machine (VM) instances, you can optionally encrypt data that is transferred between the instance and the Block Volume service storage servers. To do this, select the Use in-transit encryption check box. If you configured the volume to use an encryption key that you manage using the Vault service, this key is used for in-transit encryption. Otherwise, the Oracle-provided encryption key is used. See Block Volume Encryption on page 504 for more information.

10. Click Attach.

When the volume's icon no longer lists it as Attaching, if the attachment type is Paravirtualized on page 501, you can use the volume. If the attachment type is iSCSI on page 501, you need to connect to the volume first. For more information, see Connecting to a Volume on page 524.

On Linux-based instances, if you want to automatically mount volumes on instance boot, you need to set some specific options in the /etc/fstab file, or the instance may fail to launch. This applies to both iSCSI and paravirtualized attachment types. For volumes using consistent device paths, see fstab Options for Block Volumes Using Consistent Device Paths.
Using Consistent Device Paths on page 527. For all other volumes, see Traditional fstab Options on page 528.

To view the instances attached to a volume from the Volume details page

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. In the Block Volumes list, click the block volume that you want to view the attached instances for.
3. In the Resources section, click Attached Instances.

All the attached instances in the selected compartment will be displayed in the list. To view attached instances in other compartments, change the compartment in the COMPARTMENT drop down list.

To view the volumes attached to an instance from the Instance details page

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the Instances list, click the instance that you want to view the attached volumes for.
3. In the Resources section, click Attached Block Volumes.

All the block volumes attached to the instance will be displayed in the list, regardless of the compartment the block volumes are in.

Using the CLI

For information about using the CLI, see Command Line Interface (CLI) on page 4192.

To attach a volume to an instance as shareable, read/write

Open a command prompt and run:

```
oci compute volume-attachment attach --instance-id <instance_ID> --type <attachment_type> --volume-id <volume_ID> --read-only true/false --is-shareable true
```

For example:

```
oci compute volume-attachment attach --instance-id ocid1.instance.oc1..<unique_ID> --type iscsi --volume-id ocid1.volume.oc1..<unique_ID> --read-only false --is-shareable true
```

To list all the instances attached to a volume

Open a command prompt and run:

```
oci compute volume-attachment list --compartment-id <compartment_ID> --volume-id <volume_ID>
```

For example:

```
oci compute volume-attachment attach --compartment-id ocid1.compartment.oc1..<unique_ID> --volume-id ocid1.volume.oc1..<unique_ID>
```

Note:

This operation will only return the attached instances that are in the specified compartment. You need to run this operation for every compartment that may contain instances that are attached to the specified volume.

Using the API

Use the following APIs to attach volumes and work with volume attachments to instances:
Block Volume

- **AttachVolume**
  
  Set the `isShareable` attribute of `AttachVolumeDetails` to `true`.

- **GetVolumeAttachment**

- **ListVolumeAttachments**

  The `ListVolumeAttachments` operation will only return the attached instances that are in compartment you specify. You need to run this operation for every compartment that may contain instances that are attached to the specified volume.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

**Additional Resources**

See the following links for example deployments of shared file systems on Oracle Cloud Infrastructure.

- GitHub project for automated terraform deployment of BeeGFS: `oci-beegfs`
- GitHub project for automated terraform deployment of Lustre: `oci-lustre`
- GitHub project for automated terraform deployments of IBM Spectrum Scale (GPFS) distributed parallel file system on Oracle Cloud Infrastructure: `oci-ibm-spectrum-scale`
- Refer to page 8 of Deploying Microsoft SQL Server Always On Availability Groups for an example of setting up shared access.

**Connecting to a Volume**

For volumes attached with Paravirtualized on page 501 as the volume attachment type, you do not need to perform any additional steps after Attaching a Volume on page 517, the volumes are connected automatically. However, for Linux-based images, if you want to mount these volumes on instance boot, you need to perform additional configuration steps. If you specified a device path when you attached the volume, see Fstab Options for Block Volumes Using Consistent Device Paths on page 527. If you did not specify a device path or if your instance was created from an image that does not support device paths, see Traditional Fstab Options on page 528.

For volumes attached with iSCSI on page 501 as the volume attachment type, you need to connect and mount the volume from the instance for the volume to be usable. For more information about attachment type options, see Volume Attachment Types on page 501. In order to connect the volume, you must first `attach` the volume to the instance, see Attaching a Volume on page 517.

**Connecting to iSCSI-Attached Volumes**

**Required IAM Policy**

Connecting a volume to an instance does not require a specific IAM policy. However, you may need permission to run the necessary commands on the instance's guest OS. Contact your system administrator for more information.

**Prerequisites**

You must attach the volume to the instance before you can connect the volume to the instance's guest OS. For details, see Attaching a Volume.

To connect the volume, you need the following information:

- iSCSI IP Address
- iSCSI Port numbers
- `CHAP` credentials (if you enabled CHAP)
- IQN

The Console provides the commands required to configure, authenticate, and log on to iSCSI.
Connecting to a Volume on a Linux Instance

1. Use the Console to obtain the iSCSI data you need to connect the volume:
   a. Log on to Oracle Cloud Infrastructure.
   b. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
   c. Click the name of the instance to display the instance details.
   d. In the Resources section on the Instance Details page, click Attached Block Volumes to view the attached block volume.
   e. Click the Actions icon (three dots) next to the volume you’re interested in, and then click iSCSI Commands and Information.
   
   The iSCSI Commands and Information dialog box displays specific identifying information about your volume and the iSCSI commands you’ll need. The commands are ready to use with the appropriate information included. You can copy and paste the commands into your instance session window for each of the following steps.

2. Log on to your instance’s guest OS.
3. Register the volume with the iscsiadm tool.

   ```
   iscsiadm -m node -o new -T <volume IQN> -p <iSCSI IP address>:<iSCSI port>
   ```

   A successful registration response resembles the following:

   ```
   New iSCSI node [tcp:[hw=,ip=,net_if=,iscsi_if=default] 169.254.0.2,3260,-1
   ign.2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418] added
   ```

4. Configure iSCSI to automatically connect to the authenticated block storage volumes after a reboot:

   ```
   iscsiadm -m node -T <volume IQN> -o update -n node.startup -v automatic
   ```

   **Note:** All command arguments are essential. Success returns no response.

5. Skip this step if CHAP is not enabled. If you enabled CHAP when you attached the volume, authenticate the iSCSI connection by providing the volume's CHAP credentials as follows:

   ```
   iscsiadm -m node -T <volume IQN> -p <iSCSI IP address>:<iSCSI port> -o update -n node.session.auth.authmethod -v CHAP
   ```

   ```
   iscsiadm -m node -T <volume IQN> -p <iSCSI IP address>:<iSCSI port> -o update -n node.session.auth.username -v <CHAP user name>
   ```

   ```
   iscsiadm -m node -T <volume's IQN> -p <iSCSI IP address>:<iSCSI port> -o update -n node.session.auth.password -v <CHAP password>
   ```

   Success returns no response.

6. Log in to iSCSI:

   ```
   iscsiadm -m node -T <volume's IQN> -p <iSCSI IP Address>:<iSCSI port> -l
   ```

   A successful login response resembles the following:

   ```
   Logging in to [iface: default, target:
   ign.2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418, portal:
   169.254.0.2,3260] (multiple)
   ```

7. You can now format (if needed) and mount the volume. To get a list of mountable iSCSI devices on the instance, run the following command:

```
fdisk -l
```

The connected volume listing resembles the following:

```
Disk /dev/sdb: 274.9 GB, 274877906944 bytes, 536870912 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Tip:

If you have multiple volumes that do not have CHAP enabled, you can log in to them all at once by using the following commands:

```
iscsiadm -m discovery -t sendtargets -p <iSCSI IP address>:<iSCSI port>
iscsiadm -m node -l
iscsiadm -m node -l
```

Connecting to a Volume on a Windows Instance

Caution:

When connecting to a Windows boot volume as a data volume from a second instance, you need to append -IsMultipathEnabled $True to the Connect-IscsiTarget command. See Attaching a Windows boot volume as a data volume to another instance fails for more information.

1. Use the Console to obtain the iSCSI data you need to connect the volume:
   a. Log on to Oracle Cloud Infrastructure.
   b. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
   c. Click your instance's name to display the instance details.
   d. In the Resources section on the Instance Details page, click Attached Block Volumes to view the attached block volume.
   e. Click the Actions icon (three dots) next to the volume you're interested in, and then click iSCSI Commands and Information.

   The iSCSI Commands and Information dialog box displays your volume’s IP address and port, which you’ll need to know later in this procedure.

2. Log in to your instance using a Remote Desktop client.
3. On your Windows instance, open the iSCSI Initiator. The steps to open the iSCSI Initiator may vary depending on the version of Windows.

   For example: Open Server Manager, click Tools, and then select iSCSI Initiator.
4. In the iSCSI Initiator Properties dialog box, click the Discovery tab, and then click Discover Portal.
5. Enter the block volume IP Address and Port, and then click OK.
6. Click the Targets tab.
7. Under Discovered targets, select the volume IQN.
8. Click Connect.
9. Make sure that the Add this connection to the list of favorite targets check box is selected, and then click OK.
You can now format (if needed) and mount the volume. To view a list of mountable iSCSI devices on your instance, in Server Manager, click File and Storage Services, and then click Disks.

The disk is displayed in the list.

**fstab Options for Block Volumes Using Consistent Device Paths**

On Linux instances, if you want to automatically mount volumes on instance boot, you need to set some specific options in the /etc/fstab file, or the instance may fail to launch.

**Note:**

These steps are for block volumes that are attached with consistent device paths enabled. If the block volume does not have consistent device paths enabled, use the legacy etc/fstab options instead.

**Prerequisites**

Before using a consistent device path, you should confirm that the instance supports consistent device paths and is correctly configured.

To verify that the volume is attached to a supported instance, connect to the instance and run the following command:

```
ll /dev/oracleoci/oraclevd*
```

The output will look similar to the following:

```
lrwxrwxrwx. 1 root root 6 Feb  7 21:02 /dev/oracleoci/oraclevda -> ../sda
lrwxrwxrwx. 1 root root 7 Feb  7 21:02 /dev/oracleoci/oraclevda1 -> ../sda1
lrwxrwxrwx. 1 root root 7 Feb  7 21:02 /dev/oracleoci/oraclevda2 -> ../sda2
lrwxrwxrwx. 1 root root 7 Feb  7 21:02 /dev/oracleoci/oraclevda3 -> ../sda3
```

If you don't see this output and instead see the following error message:

```
cannot access /dev/oracleoci/oraclevd*: No such file or directory
```

there may be a problem with the instance configuration for device paths. For assistance with this, contact Support.

**Use the _netdev and nofail Options**

By default, the /etc/fstab file is processed before the initiator starts. To configure the mount process to initiate before the volumes are mounted, specify the _netdev option on each line of the /etc/fstab file.

When you create a custom image of an instance where the volumes, excluding the root volume, are listed in the /etc/fstab file, instances will fail to launch from the custom image. To prevent this issue, specify the nofail option in the /etc/fstab file.

In the example scenario with three volumes, the /etc/fstab file entries for the volumes with the _netdev and nofail options are as follows:

```
/dev/oracleoci/oraclevdb /mnt/vol1 xfs defaults,_netdev,nofail 0 2
/dev/oracleoci/oraclevdc /mnt/vol2 xfs defaults,_netdev,nofail 0 2
/dev/oracleoci/oraclevdd /mnt/vol3 xfs defaults,_netdev,nofail 0 2
```

After you have updated the /etc/fstab file, use the following command to mount the volumes:

```
bash-4.2$ sudo mount -a
```

Reboot the instance to confirm that the volumes are mounted properly on reboot with the following command:

```
bash-4.2$ sudo reboot
```
**Troubleshooting Issues with the /etc/fstab File**

If the instance fails to reboot after you update the /etc/fstab file, you may need to undo the changes to the /etc/fstab file. To update the file, first connect to the serial console for the instance. When you have access to the instance using the serial console connection, you can remove, comment out, or fix the changes that you made to the /etc/fstab file.

**Traditional fstab Options**

On Linux instances, if you want to automatically mount volumes on instance boot, you need to set some specific options in the /etc/fstab file, or the instance may fail to launch.

**Note:**

These steps are for block volumes that do not have **consistent device paths** enabled. If consistent device paths are enabled for the block volume, use the /etc/fstab options for block volumes using consistent device paths instead.

**Volume UUIDs**

On Linux operating systems, the order in which volumes are attached is non-deterministic, so it can change with each reboot. If you refer to a volume using the device name, such as /dev/sdb, and you have more than one non-root volume, you can't guarantee that the volume you intend to mount for a specific device name will be the volume mounted.

To prevent this issue, specify the volume UUID in the /etc/fstab file instead of the device name. When you use the UUID, the mount process matches the UUID in the superblock with the mount point specified in the /etc/fstab file. This process guarantees that the same volume is always mounted to the same mount point.

**Determining the UUID for a Volume**

1. Follow the steps to attach a volume and connect to the volume.
2. After the volumes are connected, create the file system of your choice on each volume using standard Linux tools.
   
   The remaining steps assume that three volumes were connected, and that an XFS file system was created on each volume.
3. Run the following command to use the blkid utility to get the UUIDs for the volumes:

```
sudo blkid
```

The output will look similar to the following:

```
{{ /dev/sda3: UUID="1701c7e0-7527-4338-ae9f-672fd8d24ec7" TYPE="xfs" PARTUUID="82d2ba4e-4d6e-4a33-9c4d-ba52db57ea61"}}
{{ /dev/sdal: UUID="5750-10A1" TYPE="vfat" PARTLABEL="EFI System Partition" PARTUUID="082c26fd-85f5-4db2-9f4e-9288a3f3e784"}}
{{ /dev/sda2: UUID="1aad7aca-689d-4f4f-afff-e0d46fc1b89f" TYPE="swap" PARTUUID="94ee5675-a805-49b2-aaf5-2fa15aade8d5"}}
{{ /dev/sdb: UUID="699a776a-3d8e-4c88-8f46-209101f318b6" TYPE="xfs"}}
{{ /dev/sdd: UUID="85566369-7148-4ff0-bf97-50954caee7854" TYPE="xfs"}}
{{ /dev/sdc: UUID="ba0ac1d3-58cf-4ff0-bd28-f2df532f7de9" TYPE="xfs"}}
```

The root volume in this output is /dev/sda*. The additional remote volumes are:

- /dev/sdb
- /dev/sdc
- /dev/sdd

4. To automatically attach the volumes at /mnt/vol1, /mnt/vol2, and /mnt/vol3 respectively, create the three directories using the following commands:

```
bash-4.2$ sudo mkdir /mnt/vol1
```
{% bash-4.2$ sudo mkdir /mnt/vol2 %}
{% bash-4.2$ sudo mkdir /mnt/vol3 %}

**Use the _netdev and nofail Options**

By default, the `/etc/fstab` file is processed before the initiator starts. To configure the mount process to initiate before the volumes are mounted, specify the `_netdev` option on each line of the `/etc/fstab` file.

When you create a custom image of an instance where the volumes, excluding the root volume, are listed in the `/etc/fstab` file, instances will fail to launch from the custom image. To prevent this issue, specify the `nofail` option in the `/etc/fstab` file.

In the example scenario with three volumes, the `/etc/fstab` file entries for the volumes with the `_netdev` and `nofail` options are as follows:

```
UUID=699a776a-3d8d-4c88-8f46-209101f318b6 /mnt/vol1 xfs defaults,_netdev,nofail 0 2
UUID=ba0ac1d3-58cf-4ff0-bd28-f2df532f7de9 /mnt/vol2 xfs defaults,_netdev,nofail 0 2
UUID=85566369-7148-4ffc-bf97-50954cae7854 /mnt/vol3 xfs defaults,_netdev,nofail 0 2
```

After you have updated the `/etc/fstab` file, use the following command to mount the volumes:

```
bash-4.2$ sudo mount -a
```

Reboot the instance to confirm that the volumes are mounted properly on reboot with the following command:

```
bash-4.2$ sudo reboot
```

**Troubleshooting Issues with the `/etc/fstab` File**

If the instance fails to reboot after you update the `/etc/fstab` file, you may need to undo the changes to the `/etc/fstab` file. To update the file, first connect to the serial console for the instance. When you have access to the instance using the serial console connection, you can remove, comment out, or fix the changes that you made to the `/etc/fstab` file.

**Listing Volumes**

You can list all Block Volume volumes in a specific compartment, as well as detailed information on a single volume.

**Required IAM Service Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a `policy` by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which `compartment` you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to list volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Using the Console**

Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes. A detailed list of volumes in your current compartment is displayed.
• To view the volumes in a different compartment, change the compartment in the Compartment drop-down menu.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

List Volumes:
Get a list of volumes within a compartment.
• ListVolumes

Get a Single Volume:
Get detailed information on a single volume:
• GetVolume

Listing Volume Attachments

You can use the API to list all Block Volume volume attachments in a specific compartment, as well as detailed information on a single volume attachment.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to list volume attachments. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

List Attachments:
Get information on all volume attachments in a specific compartment.
• ListVolumeAttachments

Get a Single Attachment:
Get detailed information on a single attachment.
• GetVolumeAttachment

Renaming a Volume

You can use the API to change the display name of a Block Volume volume.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to rename block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the API

To update a volume's display name, use the following operation:

- UpdateVolume

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Editing a Volume's Settings

The Oracle Cloud Infrastructure Block Volume service enables you to edit the following settings for block volumes and boot volumes:

- Expand the volume size.
- Change the volume performance.
- Enable performance auto-tune.
- Assigning a volume backup policy.

You can edit these settings when volumes are online and attached to instances or while they’re detached from instances. See the applicable sections in this topic for links to tasks describing the steps to edit these settings, along with additional information about working with these settings.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to attach/detach existing block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Resizing Volumes

The Block Volume service's online resizing feature enables you to expand the size of an existing volume in place. After you resize an online volume, you need to rescan the disk and extend the partition. For more information, see:

- Resizing a Volume on page 532
- Rescanning the Disk for a Block Volume or Boot Volume on page 535
Changing the Volume Performance

The elastic performance feature of the Block Volume service allows you to dynamically change the volume performance, see Block Volume Elastic Performance on page 581 for more information. You can change volume performance for your block volumes and boot volumes while they are online, without any downtime, see Changing the Performance of a Volume on page 582. For specific information about this task in the Console, see Using the Console on page 582.

Enabling Performance Auto-tune for a Volume

With the performance auto-tune feature of the Block Volume service, you can configure your volumes to optimize cost with performance. When auto-tune is enabled, a volume’s performance it automatically adjusted to the lower cost option when the volume is detached from all instances. The performance is then automatically reset to the default performance option when you reattach the volume to an instance. For details, see Auto-tune Volume Performance on page 583.

Assigning a Backup Policy to a Volume

The Block Volume service provides you with the capability to perform volume backups automatically on a schedule and retain them based on the selected backup policy.

There are two kinds of backup policies:

- **User defined**: Custom backup policies that you create and configure schedules for. With user defined policies, you can also enable scheduled cross-region backups, so that scheduled volume backups are automatically copied to a second region, see Scheduling Volume Backup Copies Across Regions on page 548.
- **Oracle defined**: Predefined backup policies that have a set backup frequency and retention period. You cannot modify these policies.

For more information about scheduling volume backups, see Policy-Based Backups. For task-based procedures, see Managing Backup Policy Assignments to Volumes.

Resizing a Volume

The Oracle Cloud Infrastructure Block Volume service lets you expand the size of block volumes and boot volumes. You have several options to increase the size of your volumes:

- Expand an existing volume in place with online resizing. See Online Resizing of Block Volumes Using the Console on page 533 for the steps to do this.
- Restore from a volume backup to a larger volume. See Restoring a Backup to a New Volume on page 557 and Restoring a Boot Volume on page 618.
- Clone an existing volume to a new, larger volume. See Cloning a Volume on page 560 and Cloning a Boot Volume on page 621.
- Expand an existing volume in place with offline resizing. See Offline Resizing of Block Volumes Using the Console on page 534 for the steps to do this.

For more information about the Block Volume service, see the Block Volume FAQ.

You can only increase the size of the volume, you cannot decrease the size.

**Note:**

Resizing IDE type boot volumes is not supported. This applies to both offline and online resizing. To workaround this limitation, you can do one of the following:

- Terminate the VM instance, ensuring that you keep the boot volume when you terminate the instance. Resize the boot volume that you have kept,
and then launch a new VM instance, using the resized boot volume as the image source.
• Create a clone of the boot volume, resize the boot volume clone, and then launch a new VM instance using the resized boot volume clone as the image source.

Caution:
Before you resize a boot or block volume, you should create a backup of the volume.

Note:
After a volume has been resized, the first backup on the resized volume will be a full backup. See Volume Backup Types on page 541 for more information about full versus incremental volume backups.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to attach/detach existing block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Online Resizing of Block Volumes Using the Console
With online resizing, you can expand the volume size without detaching the volume from an instance.

To resize a block volume attached to a Linux-based instance
1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. In the Block Volumes list, click the block volume you want to resize.
3. Click Edit Size or Performance.
4. Specify the new size in VOLUME SIZE (IN GB). You must specify a larger value than the block volume's current size.
5. Click Save Changes. This opens a dialog that lists the commands to rescan the disk that you need to run after the volume is provisioned. You need to run these commands so that the operating system identifies the expanded volume size. Click the Copy link to copy the commands, and then click Close to close the dialog.
6. Log on to your instance's OS and then paste and run the rescan commands you copied in the previous step into your instance session window. The rescan commands are also provided in Rescanning the Disk for Volumes Attached to Linux-Based Instances on page 535.
7. Extend the partition, see Extending the Partition for a Block Volume on page 536.

To resize a block volume attached to a Windows instance
This procedure describes the process for online resizing for block volumes attached to Windows instances, or other instance types that are not Linux-based.
1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. In the Block Volumes list, click the block volume you want to resize.
3. Click Edit Size or Performance.
4. Specify the new size in **VOLUME SIZE (IN GB)**. You must specify a larger value than the block volume's current size.
5. Click **Save Changes**.
6. Rescan the disk, see **Rescanning the Disk for Volumes Attached to Windows Instances** on page 536.
7. Extend the partition, see **Extending the Partition for a Block Volume** on page 536.

**To resize a boot volume for a Linux-based Instance**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. In the **Boot Volumes** list, click the boot volume you want to resize.
3. Click **Edit Size or Performance**.
4. Specify the new size in **VOLUME SIZE (IN GB)**. You must specify a larger value than the boot volume's current size.
5. Click **Save Changes**. This opens a dialog that lists the commands to rescan the disk that you need to run after the volume is provisioned. You need to run these commands so that the operating system identifies the expanded volume size. Click the **Copy** link to copy the commands, and then click **Close** to close the dialog.
6. Log on to your instance's OS and then paste and run the rescan commands you copied in the previous step into your instance session window. The rescan commands are also provided in **Rescanning the Disk for Volumes Attached to Linux-Based Instances** on page 535.
7. Extend the partition and grow the file system using the **oci-growfs** command from **OCI Utilities** on page 642.

**Resizing a Boot Volume for a Windows Instance**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. In the **Boot Volumes** list, click the boot volume you want to resize.
3. Click **Resize**.
4. Click **Save Changes**.
5. Rescan the disk, see **Rescanning the Disk for Volumes Attached to Windows Instances** on page 536.
6. Extend the partition, see **Extending the System Partition on a Windows-Based Image** on page 612.

**Offline Resizing of Block Volumes Using the Console**
With offline resizing, you detach the volume from an instance before you expand the volume size. Once the volume is resized and reattached, you need to extend the partition, but you do not need to rescan the disk.

**Considerations When Resizing an Offline Volume**
Whenever you detach and reattach volumes, there are complexities and risks for both Linux-based and Windows-based instances. This applies to both paravirtualized and iSCSI attachment types. You should keep the following in mind when resizing volumes:

- When you reattach a volume to an instance after resizing, if you are not using consistent device paths, or the instance does not support consistent device paths, device order and path may change. If you are using a tool such as Logical Volume Manager (LVM), you may need to fix the device mappings. For more information about consistent device paths, see **Connecting to Volumes With Consistent Device Paths** on page 518.
- When you detach and then reattach an iSCSI-attached volume to an instance, the volume's IP address will increment.
- Before you resize a volume, you should create a full backup of the volume.

**To resize a block volume attached to a Linux-based instance**
1. Detach the block volume, see **Detaching a Volume** on page 563.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
3. In the **Block Volumes** list, click the block volume you want to resize.
4. Click **Edit Size or Performance**.
5. Specify the new size in **VOLUME SIZE (IN GB)**. You must specify a larger value than the block volume's current size.
6. Click **Save Changes**. This opens a dialog that lists the required steps to complete the volume resize. For offline resizing, you need to extend the partition after you reattach the volume. Click **Close** to close the dialog.
7. Reattach the volume, see **Attaching a Volume** on page 517.
8. Extend the partition, see **Extending the Partition for a Block Volume** on page 536.

### Resizing a Boot Volume for a Windows Instance

1. Stop the instance, see **Stopping and Starting an Instance** on page 779.
2. Detach the boot volume, see **Detaching a Boot Volume** on page 623.
3. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
4. In the **Boot Volumes** list, click the boot volume you want to resize.
5. Click **Edit Size or Performance**.
6. Specify the new size in **VOLUME SIZE (IN GB)**. You must specify a larger value than the block volume's current size.
7. Reattach the boot volume, see **Attaching a Boot Volume** on page 613.
8. Restart the instance, see **Stopping and Starting an Instance** on page 779.
9. Extend the partition, see **Extending the System Partition on a Windows-Based Image** on page 612.

### Resizing a Boot Volume for a Linux Instance

1. Stop the instance, see **Stopping and Starting an Instance** on page 779.
2. Detach the boot volume, see **Detaching a Boot Volume** on page 623.
3. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
4. In the **Boot Volumes** list, click the boot volume you want to resize.
5. Click **Edit Size or Performance**.
6. Specify the new size in **VOLUME SIZE (IN GB)**. You must specify a larger value than the block volume's current size.
7. Attach the boot volume to a second instance as a data volume. See **Attaching a Volume** on page 517 and **Connecting to a Volume** on page 524.
8. Extend the partition and grow the file system, see **Extending the Root Partition on a Linux-Based Image** on page 612.
9. Reattach the boot volume, see **Attaching a Boot Volume** on page 613.
10. Restart the instance, see **Stopping and Starting an Instance** on page 779.

### Rescanning the Disk for a Block Volume or Boot Volume

The Oracle Cloud Infrastructure Block Volume service lets you expand the size of block volumes and boot volumes while they are online and attached to instances, for more information, see **Online Resizing of Block Volumes Using the Console** on page 533. After the volume is provisioned, you need to run commands to rescan the disk, so that the operating system identifies the expanded volume size. You will need to run different rescan commands depending on the operating system of the attached instance. This topic describes some procedures you can use to rescan the disk.

#### Required IAM Policy

Rescanning the disk does not require a specific IAM policy. However, you may need permission to run the necessary commands on the instance's guest OS. Contact your system administrator for more information.

### Rescanning the Disk for Volumes Attached to Linux-Based Instances

For volumes attached to Linux-based instances, run the following commands rescan the disk for a block volume:

```bash
sudo dd iflag=direct if=/dev/<device_name> of=/dev/null count=1
echo "1" | sudo tee /sys/class/block/<device_name>/device/rescan
```

These commands are also displayed in the dialog that opens after you click **Save Changes** in the **Edit Size or Performance** dialog, and you can copy them from that dialog.
Next Steps

After you've rescanned the disk, you need to extend the partition. See Extending the Partition for a Block Volume on a Linux-Based Image on page 537 for block volumes. For boot volumes, use the oci-growfs operation from OCI Utilities on page 642.

Rescanning the Disk for Volumes Attached to Windows Instances

Using Disk Management or diskpart

For volumes formatted as FAT32 or NTFS, you can rescan the disk using the Windows interface, in Disk Management, or you can use the diskpart utility's rescan command from the command line.

Rescanning the disk using the command line with DISKPART

1. Open a command prompt as administrator on the instance.
2. Run the following command to start the diskpart utility:
   ```bash
diskpart
   ```
3. At the DISKPART prompt, run the following command:
   ```bash
   rescan
   ```

Rescanning the disk using the Windows interface

1. Open the Disk Management system utility on the instance.
2. Click Action, and then click Rescan Disks.

Update disk information.

Using Cygwin

For volumes formatted with a non-native Windows file system, such as volumes formatted using Oracle Automatic Storage Management (Oracle ASM), you can't use the Windows interface or the diskpart utility. Instead, you can use the dd process from a Cygwin terminal to rescan the disk. You can also use this for native Windows file systems. For more information, see Cygwin.

Next Steps

After you've rescanned the disk, you need to extend the partition. See Extending the Partition for a Block Volume on a Windows-Based Image on page 539 for block volumes, see Extending the System Partition on a Windows-Based Image on page 612 for boot volumes.

Extending the Partition for a Block Volume

The Oracle Cloud Infrastructure Block Volume service lets you expand the size of block volumes with offline volume resizing. For more information, see Resizing a Volume on page 532. In order to take advantage of the larger volume size, you need to extend the partition for the block volume. For boot volumes, see Extending the Partition for a Boot Volume on page 612.

Note:

After a volume has been resized, the first backup on the resized volume will be a full backup. See Volume Backup Types on page 541 for more information about full versus incremental volume backups.

Required IAM Policy

Extending a partition on an instance does not require a specific IAM policy. However, you may need permission to run the necessary commands on the instance's guest OS. Contact your system administrator for more information.
Extending the Partition for a Block Volume on a Linux-Based Image

On Linux-based images, use the following steps to extend the partition for a block volume.

Prerequisites

After you have resized a volume, you need to attach it to an instance before you can extend the partition and grow the file system. See Attaching a Volume on page 517 and Connecting to a Volume on page 524 for more information.

Extending the Linux Partition

Extending a partition

1. To identify the volume that you want to extend the partition for, run the following command to list the attached block volumes:

   `lsblk`

2. Run the following command to edit the volume's partition table with `parted`:

   `parted <volume_id>`

   `<volume_id>` is the volume identifier, for example `/dev/sdc`.

3. When you run `parted`, you may encounter the following error message:

   Warning: Not all of the space available to `<volume_id>` appears to be used, you can fix the GPT to use all of the space (an extra `volume_size` blocks)
or continue with the current setting?

You are then prompted to fix the error or ignore the error and continue with the current setting. Specify the option to fix the error.

4. Run the following command to change the display units to sectors so that you can see the precise start position for the volume:

\[(parted)\ unit\ s\]

5. Run the following command to display the current partitions in the partition table:

\[(parted)\ print\]

Make note of the values in the **Number**, **Start**, and **File system** columns for the root partition.

6. Run the following command to remove the existing root partition:

\[(parted)\ rm\ <partition_number>\]

\(<partition_number>\) is the value from the **Number** column.

7. Run the following command to recreate the partition:

\[(parted)\ mkpart\]

At the **Start?** prompt, specify the value from the **Start** column. At the **File system type?** prompt, specify the value from the **File system** column. Specify 100% for the **End?** prompt.

8. Run the following command to exit parted:

\[(parted)\ quit\]

This command forces a rewrite of the partition table with the new partition settings that you specified.

9. To verify that the root partition was extended, run the following command to list the attached block volumes:

\[lsblk\]

After you extend the root partition you need to grow the file system. The steps in the following procedure apply only to xfs file systems.

**Growing the file system for a partition**

1. Before you grow the file system, repair any issues with the file system on the extended partition by running the following command:

\[xfs\_repair\ <partition\_id>\]

\(<partition\_id>\) is the partition identifier, for example /dev/sdc1. See Checking and Repairing an XFS File System for more information.

2. After you have confirmed that there are no more issues to repair, you need to create a mount point to run the xfs_growfs against. To do this, create a directory and mount the partition to that directory by running the following commands:

\[mkdir\ <directory\_name>\]

\[mount\ <device>\ <directory\_name>\]

\(<device>\) is the device path to the file system, for example /dev/sdc1.
3. After you have created the mount point run the following command to grow the file system:

```
mount <partition_id> <directory_name> -o nouuid
```

<partition_id> is the partition identifier, for example /dev/sdc1, and <directory_name> is the directory name, for example data.

4. To verify that the file system size is correct, run the following command to display the file system details:

```
xfs_growfs -d <directory_name>
```

<directory_name> is the name for the directory you created in the previous step, for example data.

---

**Extending the Partition for a Block Volume on a Windows-Based Image**

On Windows-based images, you can extend a partition using the Windows interface or from the command line using the DISKPART utility.

**Windows Server 2012 and Later Versions**

The steps to extend a partition for a block volume attached to an instance running Windows Server 2012, Windows Server 2016, or Windows Server 2019 are the same, and are described in the following procedures.

**Extending a partition using the Windows interface**

1. Open the Disk Management system utility on the instance.
2. Right-click the expanded block volume and select **Extend Volume**.
3. Follow the instructions in the **Extend Volume Wizard**:
   a. Select the disk that you want to extend, enter the size, and then click **Next**.
   b. Confirm that the disk and size settings are correct, and then click **Finish**.
4. Verify that the block volume's disk has been extended in Disk Management.

**Extending a partition using the command line with DISKPART**

1. Open a command prompt as administrator on the instance.
2. Run the following command to start the DISKPART utility:

```
diskpart
```

3. At the DISKPART prompt, run the following command to display the instance's volumes:

```
list volume
```

4. Run the following command to select the expanded block volume:

```
select volume <volume_number>
```

<volume_number> is the number associated with the block volume that you want to extend the partition for.

5. Run the following command to extend the partition:

```
extend size=<increased_size_in_MB>
```

<increased_size_in_MB> is the size in MB that you want to extend the partition to.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When using the DISKPART utility, do not overextend the partition beyond the current available space. Overextending the partition could result in data loss.</td>
</tr>
</tbody>
</table>

6. To confirm that the partition was extended, run the following command and verify that the block volume's partition has been extended:

```
list volume
```

---

**Overview of Block Volume Backups**

The backups feature of the Oracle Cloud Infrastructure Block Volume service lets you make a point-in-time snapshot of the data on a block volume. You can make a backup of a volume when it is attached to an instance or while it is detached. These backups can then be restored to new volumes either immediately after a backup or at a later time that you choose.

Backups are encrypted and stored in Oracle Cloud Infrastructure Object Storage, and can be restored as new volumes to any availability domain within the same region they are stored. This capability provides you with a spare copy of a volume and gives you the ability to successfully complete disaster recovery within the same region.

There are two ways you can initiate a backup, either by manually starting the backup, or by assigning a policy which defines a set backup schedule.

**Manual Backups**

These are on-demand one-off backups that you can launch immediately by following the steps described in Backing Up a Volume on page 546. When launching a manual backup, you can specify whether an incremental or a full backup should be performed. See Volume Backup Types for more information about backup types.

**Policy-Based Backups**

These are automated scheduled backups as defined by the backup policy assigned to the volume.

There are two kinds of backup policies:

- **Oracle defined**: Predefined backup policies that have a set backup frequency and retention period. You cannot modify these policies. For more information, see Oracle Defined Backup Policies on page 550.
- **User defined**: Custom backup policies that you create and configure schedules and retention periods for. You can also enable scheduled cross-region automated backups with user defined policies, see Scheduling Volume Backup Copies Across Regions on page 548. For more information, see User Defined Backup Policies on page 547.
Tags
When a volume backup is created, the source volume's tags are automatically included in the volume backup. This also includes volumes with custom backup policies applied to create backups on a schedule. Source volume tags are automatically assigned to all backups when they are created. You can also apply additional tags to volume backups as needed.

When a volume backup is copied to a new region, tags are also automatically copied with the volume backup. When the volume is restored from a backup, the volume is restored with the source volume's tags.

Volume Backup Types
There are two backup types available in the Block Volume service:

- **Incremental**: This backup type includes only the changes since the last backup.
- **Full**: This backup type includes all changes since the volume was created.

For data recovery purposes, there is no functional difference between an incremental backup and a full backup. You can restore a volume from any of your incremental or full volume backups. Both backup types enable you to restore the full volume contents to the point-in-time snapshot of the volume when the backup was taken. You don't need to keep the initial full backup or subsequent incremental backups in the backup chain and restore them in sequence, you only need to keep the backups taken for the times you care about.

Backup Details
For incremental backups, they are a record of all the changes since the last backup. If the first backup on a volume is created as incremental, it is effectively a full backup. For full backups, they are a record of all the changes since the volume was created.

For example, in a scenario where you create a 16 TB block volume, modify 40 GB on the volume, and then launch a full backup of the volume, upon completion, the volume backup size is 40 GB. If you then modify an additional 4 GB and create an incremental backup, the unique size of the incremental backup will be 4 GB. If the full backup is deleted, the incremental backup will retain the full 44 GB necessary to restore the volume contents. In this example, if there was a third incremental backup of non-overlapping blocks, with a size of 1 GB, created after the second incremental backup, and then the full backup is deleted, the third backup would stay at a 1 GB size, and the second incremental backup size would be updated to 44 GB. The blocks are accounted for in the earliest backup that references them.

**Note:**

After a volume has been resized, the first backup on the resized volume will be a full backup. See [Resizing a Volume](https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/block-volumes.htm#resize) on page 532 for more information about volume resizing.

Planning Your Backup
The primary use of backups is to support business continuity, disaster recovery, and long-term archiving requirements. When determining a backup schedule, your backup plan and goals should consider the following:

- **Frequency**: How often you want to back up your data.
- **Recovery time**: How long you can wait for a backup to be restored and accessible to the applications that use it. The time for a backup to complete varies on several factors, but it will generally take a few minutes or longer, depending on the size of the data being backed up and the amount of data that has changed since your last backup.
- **Number of stored backups**: How many backups you need to keep available and the deletion schedule for those you no longer need. You can only create one backup at a time, so if a backup is underway, it will need to complete before you can create another one. For details about the number of backups you can store, see [Block Volume Capabilities and Limits](https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/block-volumes.htm#lim) on page 505.
The common use cases for using backups are:

- Needing to create multiple copies of the same volume. Backups are highly useful in cases where you need to create many instances with many volumes that need to have the same data formation.
- Taking a snapshot of your work that you can restore to a new volume at a later time.
- Ensuring you have a spare copy of your volume in case something goes wrong with your primary copy.

**Volume Backup Size**

Volume backup size may be larger than the current volume usage. Some of the reasons for this could include the following:

- Any part of a volume that has been written to is considered initialized, so will always be part of a volume backup.
- Many operating systems write or zero out the content, which results in these blocks marked as used. The Block Volume service considers these blocks updated and includes them in the volume backup.
- Volume backups also include metadata, which can be up to 1 GB in additional data. For example, in a full backup of a 256 GB Windows boot disk, you may see a backup size of 257 GB, which includes an additional 1 GB of metadata.

**Copying Block Volume Backups Across Regions**

You can copy block volume backups between regions using the Console, command line interface (CLI), SDKs, or REST APIs. For steps, see Copying a Volume Backup Between Regions on page 558. This capability enhances the following scenarios:

- **Disaster recovery and business continuity:** By copying block volume backups to another region at regular intervals, it makes it easier for you to rebuild applications and data in the destination region if a region-wide disaster occurs in the source region.
- **Migration and expansion:** You can easily migrate and expand your applications to another region.

You can also enable scheduled cross-region automated backups with user defined policies, see Scheduling Volume Backup Copies Across Regions on page 548.

To copy volume backups between regions, you must have permission to read and copy volume backups in the source region, and permission to create volume backups in the destination region. For more information see Required IAM Policy on page 620.

Once you have copied the volume backup to the new region you can then restore from that backup by creating a new volume from the backup using the steps described in Restoring a Backup to a New Volume on page 557.

**Volume Backup Encryption**

The Oracle Cloud Infrastructure Block Volume service always encrypts all block volumes, boot volumes, and volume backups at rest by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption.

The Oracle Cloud Infrastructure Vault service enables you to bring and manage your own keys to use for encrypting volumes and their backups. When you create a volume backup, the encryption key used for the volume is also used for the volume backup. When you restore the backup to create a new volume you configure a new key, see Restoring a Backup to a New Volume on page 557. See also Overview of Vault on page 3952.

If you do not configure a volume to use the Vault service, the Block Volume service uses the Oracle-provided encryption key instead. This applies to both encryption at-rest and in-transit encryption.

**Best Practices When Creating Block Volume Backups**

When creating and restoring from backups, keep in mind the following:

- Before creating a backup, you should ensure that the data is consistent: Sync the file system, unmount the file system if possible, and save your application data. Only the data on the disk will be backed up. When creating a backup, after the backup state changes from REQUEST_RECEIVED to CREATING, you can return to writing data to the volume. While a backup is in progress, the volume that is being backed up cannot be deleted.
• If you want to attach a restored volume that has the original volume attached, be aware that some operating systems do not allow you to restore identical volumes. To resolve this, you should change the partition IDs before restoring the volume. The steps to change an operating system's partition ID vary by operating system. For instructions, see your operating system's documentation.

• You should not delete the original volume until you have verified that the backup you created of it completed successfully.

See Backing Up a Volume on page 546 and Restoring a Backup to a New Volume on page 557 for more information.

**Differences Between Block Volume Backups and Clones**

Consider the following criteria when you decide whether to create a backup or a clone of a volume.

<table>
<thead>
<tr>
<th></th>
<th>Volume Backup</th>
<th>Volume Clone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Creates a point-in-time backup of data on a volume. You can restore multiple new volumes from the backup later in the future.</td>
<td>Creates a single point-in-time copy of a volume without having to go through the backup and restore process.</td>
</tr>
<tr>
<td><strong>Use case</strong></td>
<td>Retain a backup of the data in a volume, so that you can duplicate an environment later or preserve the data for future use. Meet compliance and regulatory requirements, because the data in a backup remains unchanged over time. Support business continuity requirements. Reduce the risk of outages or data mutation over time.</td>
<td>Rapidly duplicate an existing environment. For example, you can use a clone to test configuration changes without impacting your production environment.</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Slower (minutes or hours)</td>
<td>Faster (seconds)</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Lower cost</td>
<td>Higher cost</td>
</tr>
<tr>
<td><strong>Storage location</strong></td>
<td>Object Storage</td>
<td>Block Volume</td>
</tr>
<tr>
<td><strong>Retention policy</strong></td>
<td>Policy-based backups expire, manual backups do not expire</td>
<td>No expiration</td>
</tr>
<tr>
<td><strong>Volume groups</strong></td>
<td>Supported. You can back up a volume group.</td>
<td>Supported. You can clone a volume group.</td>
</tr>
</tbody>
</table>

For background information and steps to clone a block volume, see Cloning a Volume on page 560.

**Using the CLI or REST APIs to Customize and Manage the Lifecycle of Volume Backups**

You can use the CLI, REST APIs, or the SDKs to automate, script, and manage volume backups and their lifecycle.

**Using the CLI**

This section provides basic sample CLI commands that you can use in a script, such as a cron job run by the cron utility on Linux-based operating systems, to perform automatic backups at specific times. For information about using the CLI, see Command Line Interface (CLI) on page 4192.
To create a manual backup of the specified block volume

Open a command prompt and run:

```
oci bv backup create --volume-id <block_volume_OCID> --display-name <Name> --type <FULL|INCREMENTAL>
```

For example:

```
oci bv backup create --volume-id ocid1.volume.oc1..<unique_ID> --display-name "backup display name" --type FULL
```

To delete a block volume backup

Open a command prompt and run:

```
oci bv backup delete --volume-backup-id <volume_backup_OCID>
```

For example:

```
oci bv backup delete --volume-backup-id ocid1.volume.oc1..<unique_ID>
```

To create a manual backup of the specified boot volume

Open a command prompt and run:

```
oci bv boot-volume-backup create --volume-id <boot_volume_OCID> --display-name <Name> --type <FULL|INCREMENTAL>
```

For example:

```
oci bv boot-volume-backup create --volume-id ocid1.volume.oc1..<unique_ID> --display-name "backup display name" --type FULL
```

To delete a boot volume backup

Open a command prompt and run:

```
oci bv backup delete --boot-volume-backup-id <boot_volume_backup_OCID>
```

For example:

```
oci bv backup delete --boot-volume-backup-id ocid1.volume.oc1..<unique_ID>
```

To list the Oracle-defined backup policies

Open a command prompt and run:

```
oci bv volume-backup-policy list
```

To assign an Oracle-defined backup policy to a boot or block volume

Open a command prompt and run:

```
oci bv volume-backup-policy-assignment create --asset-id <volume_OCID> --policy-id <policy_OCID>
```
For example:

```bash
oci bv volume-backup-policy-assignment create --asset-id ocid1.volume.oc1..<unique_ID> --policy-id ocid1.volumebackuppolicy.oc1..<unique_ID>
```

**To un-assign an Oracle-defined backup policy from a boot or block volume**

Open a command prompt and run:

```bash
oci bv volume-backup-policy-assignment delete --policy-assignment-id <policy_assignment_OCID>
```

For example:

```bash
oci bv volume-backup-policy-assignment delete --policy-assignment-id ocid1.volumebackuppolicyassign.oc1..<unique_ID>
```

**To retrieve the backup policy assignment ID for a boot or block volume**

Open a command prompt and run:

```bash
oci bv volume-backup-policy-assignment get-volume-backup-policy-asset-assignment --asset-id <volume_OCID>
```

For example:

```bash
oci bv volume-backup-policy-assignment get-volume-backup-policy-asset-assignment --asset-id ocid1.volume.oc1..<unique_ID>
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations for working with block volume backups, boot volume backups, and backup policies.

**Block Volume Backups**

- CreateVolumeBackup
- DeleteVolumeBackup
- GetVolumeBackup
- ListVolumeBackups
- UpdateVolumeBackup

**Boot Volume Backups**

- CreateBootVolumeBackup
- DeleteBootVolumeBackup
- GetBootVolumeBackup
- ListBootVolumeBackups
- UpdateBootVolumeBackup

**Volume Backup Policies and Policy Assignments**

- GetVolumeBackupPolicy
- ListVolumeBackupPolicies
- CreateVolumeBackupPolicyAssignment
- DeleteVolumeBackupPolicyAssignment
Block Volume

- GetVolumeBackupPolicyAssetAssignment
- GetVolumeBackupPolicyAssignment

**Backing Up a Volume**

You can create a backup of a volume using Block Volume. Volume backups are point-in-time snapshots of volume data. For more information about volume backups, see Overview of Block Volume Backups on page 540.

For information to help you decide whether to create a backup or a clone of a boot volume, see Differences Between Block Volume Backups and Clones on page 543.

**Note:**

Volume backup size may be larger than the current volume usage. See Volume Backup Size on page 542 for more information.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups. The policy in Let boot volume backup admins manage only backups on page 2147 further restricts access to just creating and managing backups.

**Tip:**

When users create a backup from a volume or restore a volume from a backup, the volume and backup don't have to be in the same compartment. However, users must have access to both compartments.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. Click the block volume that you want to create a backup for.
3. Click Create Manual Backup.
4. Enter a name for the backup. Avoid entering confidential information.
5. Select the backup type, either incremental or full. See Volume Backup Types on page 541 for information about backup types.
6. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click Create Backup.

The backup will be completed once its icon no longer lists it as CREATING in the volume list.

**Using the API**

To back up a volume, use the following operation:

- CreateVolumeBackup

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
For more information about backups, see Overview of Block Volume Backups on page 540 and Restoring a Backup to a New Volume on page 557.

**Policy-Based Backups**

The Oracle Cloud Infrastructure Block Volume service provides you with the capability to perform volume backups and volume group backups automatically on a schedule and retain them based on the selected backup policy.

With user defined policies, you can also enable scheduled cross-region backups, so that scheduled volume backups are automatically copied to a second region, see Scheduling Volume Backup Copies Across Regions on page 548. These features allow you to adhere to your data compliance and regulatory requirements.

Caution:

Deleting Block Volumes with Policy-Based Backups

All policy-based backups will eventually expire, so if you want to keep a volume backup indefinitely, you need to create a manual backup.

Volume backups are point-in-time snapshots of volume data. For more information about volume backups, see Overview of Block Volume Backups on page 540.

There are two kinds of backup policies:

- **User defined**: Custom backup policies that you create and configure schedules for.
- **Oracle defined**: Predefined backup policies that have a set backup frequency and retention period. You cannot modify these policies.

Note:

Timing for Scheduled Backups

Scheduled volume backups are not guaranteed to start at the exact time specified by the backup schedule. You may see up to several hours of delay between the scheduled start time and the actual start time for the volume backup in scenarios where the system is overloaded. This applies to both user defined and Oracle defined backup policies.

Caution:

Full Backups and Oracle Defined Policies

Starting November 3, 2021, Oracle defined policies will no longer include full backups. See Full backups removed from Oracle defined backup policies.

**User Defined Backup Policies**

Oracle Cloud Infrastructure enables you to customize your backup schedules with user defined policies. These are backup policies that you define the backup frequency and retention period for. There are two parts to user defined backup policies, the backup policy itself, and then one or more schedules in the policy.

To get started with user defined backup policies, you need to first create the backup policy, see To create a user defined backup policy on page 552. After this step, you have an empty backup policy, so the next step is to define and add schedules to the policy.

**Schedules**

Schedules define the backup frequency and retention period for a user defined backup policy, just like Oracle defined backup policies. The difference is that you can customize the schedules associated with user defined policies. This gives you control over the backup frequency and retention period.

When defining a schedule for a user defined backup policy, the first thing you configure is the schedule type, this specifies the backup frequency. Oracle Cloud Infrastructure provides the following schedule types:
Block Volume

- **Daily**: Backups are generated daily. You specify the hour of the day for the backup.
- **Weekly**: Backups are generated weekly. You specify the day of the week, and the hour of that day for the backup.
- **Monthly**: Backups are generated monthly. You specify the day of the month, and the hour of that day for the backup.
- **Yearly**: Backups are generated yearly. You specify the month, the day of that month, and the hour of that day for the backup.

In addition to frequency, you also configure the following:

- **Retention time**: The amount of time to keep the backup, in days, weeks, months, or years. The time period is based on the schedule type.
- **Backup type** Options are full or incremental, see Volume Backup Types on page 541 for more information.
- **Timezone** The time zone to use for the backup schedule. Options are UTC or the regional data center time zone.

For more information, see To add a schedule to a user defined backup policy on page 552.

You can also edit or remove schedules for a user defined policy at any time, see To edit a schedule for a user defined backup policy on page 553 and To delete a schedule for a user defined backup policy on page 553.

**Duplicating Existing Backup Policies**

You can create a new backup policy by duplicating any of the existing backup policies.

If one of the Oracle defined policies is close to meeting your volume backup requirements, but with some changes, you can create a new backup policy by duplicating the Oracle defined policy. This creates a new user defined backup policy with schedules already assigned, enabling you to use the Oracle defined policy’s settings as a starting point to save time and simplify the process.

You can also duplicate an existing user defined policy. For more information, see To duplicate a backup policy on page 553. You can then add, edit, or delete schedules for the new backup policy.

**Scheduling Volume Backup Copies Across Regions**

The Block Volume service enables you to copy volume backups from one region to another for business continuity and disaster recovery scenarios, for more information, see Copying Block Volume Backups Across Regions on page 542. With user-defined policies, you can automate this process, so that volume backups are copied to another region on a schedule. Enabling the automatic copying of scheduled volume backups is only supported with user-defined policies, so if you need to use this feature for a volume currently configured with an Oracle defined policy, you need to duplicate the policy and then enable cross region copy. The volume backup copy in the target region has the same retention period as the volume backup in the source region.

**Caution:**

Vault encryption keys for volumes are not copied to the destination region for scheduled volume and volume group backups enabled for cross region copy.

For more information, see Vault encryption keys not copied to destination region for scheduled cross region backup copies.

**Note:**

It may take up to 24 hours for daily scheduled volume backups to be copied to the target region. You can verify that the volume backup was copied by switching to the target region and checking the list of volume backups for that region. If the volume backup has not been copied yet, you can perform a manual copy of that volume backup to the target region using the steps described in Copying a Volume Backup Between Regions on page 558.

**Cost**

Once this feature is enabled, your bill will include charges for storing volume backups in both the source region and the destination region. You may also see an increase in network costs. For pricing details, see Oracle Storage Cloud Pricing. The Object Storage price applies to backup storage. Outbound Data Transfer price will be applicable for network costs with cross-region backup copies.
Regions Pairs

When you enable cross region copy for a backup policy, the default target region is based on the source region for the backup.

**Note:**

You can change the default target region using the CLI, see Configuring a Custom Target Region on page 549. This capability is not available in the Console.

The following table lists the source and target region pairs for cross region copy. To copy a volume backup to a region not paired with the backup's source region, you must manually copy the volume backup, see Copying a Volume Backup Between Regions on page 558.

<table>
<thead>
<tr>
<th>Source Region</th>
<th>Target Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>US West (Phoenix)</td>
<td>US East (Ashburn)</td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td>US West (Phoenix)</td>
</tr>
<tr>
<td>US West (San Jose)</td>
<td>US West (Phoenix)</td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>US West (Phoenix)</td>
</tr>
<tr>
<td>Chile (Santiago)</td>
<td>Brazil East (Sao Paulo)</td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>Canada Southeast (Montreal)</td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>Canada Southeast (Toronto)</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>Japan East (Tokyo)</td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td>Japan Central (Osaka)</td>
</tr>
<tr>
<td>India South (Hyderabad)</td>
<td>India West (Mumbai)</td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>India South (Hyderabad)</td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>Switzerland North (Zurich)</td>
</tr>
<tr>
<td>UK South (London)</td>
<td>Germany Central (Frankfurt)</td>
</tr>
<tr>
<td>UK West (Newport)</td>
<td>UK South (London)</td>
</tr>
<tr>
<td>Australia East (Sydney)</td>
<td>Australia Southeast (Melbourne)</td>
</tr>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td>Australia East (Sydney)</td>
</tr>
<tr>
<td>Netherlands Northwest (Amsterdam)</td>
<td>Germany Central (Frankfurt)</td>
</tr>
<tr>
<td>Saudi Arabia West (Jeddah)</td>
<td>Germany Central (Frankfurt)</td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td>South Korea North (Chuncheon)</td>
</tr>
<tr>
<td>South Korea North (Chuncheon)</td>
<td>South Korea Central (Seoul)</td>
</tr>
</tbody>
</table>

Configuring a Custom Target Region

You can change the default target region for the scheduled cross region backup copy feature using the CLI. You can do this when you create a new backup policy or you can update the target region for an existing backup policy. When you create a new policy, specify the custom target region using the destination-region parameter. If you're updating an existing policy, you need to ensure that you include all the existing backup policy settings that you want to keep when you update the policy with the custom target region. To do this:

1. Use the get operation to retrieve the existing policy settings.
2. Save those settings.
3. Use the settings you saved from the previous step in the **update** operation, along with the custom target region specified in the **destination-region** parameter.

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192.

**Note:**
This capability is not available in the Console.

**To create a volume backup policy with a custom target region:**

Open a command prompt and run:

```bash
oci bv volume-backup-policy create --compartment-id <compartment_ID> --display-name <display_name> --destination-region <region_ID> --schedules file//<path>/<scheduleJSON>.json
```

For example:

```bash
oci bv volume-backup-policy create --compartment-id ocid1.compartment.oc1..<unique_ID> --display-name MyPolicyName --destination-region us-sanjose-1 --schedules file//~/input.json
```

When you update an existing policy, you need to specify all the policy's settings in the update operation, including the existing settings that you want to keep. To ensure that you include all the settings, you should first retrieve those settings using the **get** operation.

**To get the volume backup policy:**

Open a command prompt and run:

```bash
oci bv volume-backup-policy get --policy-id <backup_policy_ID>
```

For example:

```bash
oci bv volume-backup-policy get --policy-id ocid1.volumebackuppolicy.oc1..<unique_ID>
```

Save these settings and then use them when you call the **update** operation.

**To update the volume backup policy with a custom target region:**

Open a command prompt and run:

```bash
oci bv volume-backup-policy update --policy-id <backup_policy_ID> --display-name <display_name> --destination-region <region_ID> --schedules file//<path>/<scheduleJSON>.json
```

For example:

```bash
oci bv volume-backup-policy create --policy-id ocid1.volumebackuppolicy.oc1..<unique_ID> --display-name MyPolicyName --destination-region us-sanjose-1 --schedules file//~/input.json
```

**Oracle Defined Backup Policies**

There are three Oracle defined backup policies, Bronze, Silver, and Gold. Each backup policy is comprised of schedules with a set backup frequency and a retention period that you cannot modify. If the backup policy settings for Oracle defined policies don't meet your requirements, you should use **User Defined Backup Policies** on page 547 instead. With user defined backup policies you define and control the schedules. You can also enable the automatic copying of volume backups to a second region, which is not supported with Oracle defined policies.
Note:
Oracle defined backup policies are not supported for scheduled volume group backups.

Caution:
Full Backups and Oracle Defined Policies
Starting November 3, 2021, Oracle defined policies will no longer include full backups. See Full backups removed from Oracle defined backup policies.

Bronze Policy
The bronze policy includes monthly incremental backups, run on the first day of the month. These backups are retained for twelve months. This policy also includes a full backup, run yearly during the first part of January. This backup is retained for five years.

Silver Policy
The silver policy includes weekly incremental backups that run on Sunday. These backups are retained for four weeks. This policy also includes monthly incremental backups, run on the first day of the month and are retained for twelve months. Also includes a full backup, run yearly during the first part of January. This backup is retained for five years.

Gold Policy
The gold policy includes daily incremental backups, retained for seven days, along with weekly incremental backups, run on Sunday and retained for four weeks. Includes monthly incremental backups, run on the first day of the month, retained for twelve months. Also include a full backup, run yearly, during the first part of January. This backup is retained for five years.

Working with Backup Policies
There are two types of tasks when working with backup policies:

- Creating and Configuring User Defined Backup Policies on page 552
- Managing Backup Policy Assignments to Volumes on page 555

The linked sections listed above provide information for working with backup policies using the Console, CLI, and REST APIs.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

Important:
To view or work with backup policies, you need access to the root compartment, which is where the predefined backup policies are located.

For administrators: The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups. The policy in Let volume backup admins manage only backups on page 2146 further restricts access to just creating and managing backups.
Tip:

When users create a backup from a volume or restore a volume from a backup, the volume and backup don't have to be in the same compartment. However, users must have access to both compartments.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

Creating and Configuring User Defined Backup Policies

Using the Console

You can use the Console to create and update user defined backup policies.

To create a user defined backup policy

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Backup Policies.
2. Click Create Backup Policy.
3. Specify a name for the backup policy. Avoid entering confidential information.
4. Select the compartment to create the backup policy in.

   While you select a compartment for the backup policy, it is accessible across your tenancy.
5. Optionally, you can enable cross region copy to the specified region. This automates the copying of the volume backup to a second region after each backup is created. The target region specified for the backup copy is based on the region pair for the policy's source region and cannot be changed. For more information, see Regions Pairs on page 549.
6. Click Create Backup Policy to create the backup policy.

To add a schedule to a user defined backup policy

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Backup Policies.
2. Click the backup policy you want to add the schedule to.
3. Click Add Schedule.
4. Specify the backup frequency by selecting from the Schedule Type options: Daily, Weekly, Monthly, or Yearly, and then configure the additional schedule options. Depending on the schedule type, the additional schedule options will include one or more of the following:
   - Hour of the day
   - Day of the week
   - Day of the month
   - Month of the year
5. Specify the Retention Time, which will be in days, weeks, months, or years, depending on the schedule type you selected in the previous step.
6. Select Full or Incremental for Backup Type.
7. Select the Timezone to base the schedule settings on, either UTC or Regional Data Center Time.
8. Click Add Schedule.

To enable cross region copy for a user defined backup policy

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Backup Policies.
2. Click the backup policy that you want to enable cross region copy for.
3. On the details page, for Cross Region Copy Target, click Enable.
4. Click **Enable** in the confirmation dialog.

**To disable cross region copy for a user defined backup policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Backup Policies**.
2. Click the backup policy that you want to disable cross region copy for.
3. On the details page, for **Cross Region Copy Target**, click **Disable**.
4. Click **Disable** in the confirmation dialog.

**To duplicate a backup policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Backup Policies**.
2. Click the backup policy that you want to duplicate. Both Oracle defined and user defined backup policies can be duplicated.
3. Click **Duplicate**.
4. Specify a name for the policy. Avoid entering confidential information.
5. Select the compartment to create the backup policy in. It does not need to be the same compartment as the backup policy you are duplicating.
6. Optionally, you can enable cross region copy to the specified region. This automates the copying of the volume backup to a second region after each backup is created. The default target region specified for the backup copy is based on the region pair for the policy’s source region. For more information, see **Regions Pairs** on page 549.
7. Click **Duplicate Backup Policy**.

**To edit a schedule for a user defined backup policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Backup Policies**.
2. Click the backup policy that you want to edit a schedule for.
3. In **Schedules**, for the schedule you want to edit, click the Actions icon (three dots), and then click **Edit**.
4. After making your changes to the schedule, click **Update**.

**To delete a schedule for a user defined backup policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Backup Policies**.
2. Click the user defined backup policy that you want to delete a schedule for.
3. In **Schedules**, for the schedule you want to delete, click the Actions icon (three dots), and then click **Delete**.
4. Click **Delete** in the confirmation dialog.

**To delete a user defined backup policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Backup Policies**.
2. Click the user defined backup policy you want to delete.
3. Click **Delete**.
4. Enter the name of the backup policy and click **Delete**.

**Using the CLI**

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192.

Use the following operations to work with backup policies:

**To create a user defined backup policy**

Open a command prompt and run:

```
oci bv volume-backup-policy create --compartment-id <compartment_ID> --schedules file://<path>/<scheduleJSON>.json
```

For example:

```
oci bv volume-backup-policy create --compartment-id ocid1.compartment.oc1..<unique_ID> --schedules file://~/input.json
```
To list the backup policies in a specified compartment

Open a command prompt and run:

```
oci bv volume-backup-policy list --compartment-id <compartment_ID>
```

For example:

```
oci bv volume-backup-policy list --compartment-id ocid1.compartment.oc1..<unique_ID>
```

To retrieve a specific backup policy

Open a command prompt and run:

```
oci bv volume-backup-policy get --backup-policy-id <backup-policy-ID>
```

For example:

```
oci bv volume-backup-policy get --backup-policy-id ocid1.volumebackuppolicy.oc1.phx.<unique_ID>
```

To update the display name for a user defined backup policy

Open a command prompt and run:

```
oci bv volume-backup-policy update --backup-policy-id <backup-policy_ID> --display-name <backup-policy_name>
```

For example:

```
oci bv volume-backup-policy update --backup-policy-id ocid1.volumebackuppolicy.oc1.phx.<unique_ID> --display-name "new display name"
```

To update the schedules for a user defined backup policy

Open a command prompt and run:

```
oci bv volume-backup-policy update --backup-policy-id <backup-policy_ID> --schedules file//<path>/scheduleJSON.json
```

For example:

```
oci bv volume-backup-policy update --volume-group-id ocid1.volumebackuppolicy.oc1.phx.<unique_ID> --schedules file//~/input.json
```

To delete a user defined backup policy

Open a command prompt and run:

```
oci bv volume-backup-policy delete --backup-policy-id <backup-policy_ID>
```

You can only delete a user defined backup policy if it is not assigned to any volumes. You cannot delete Oracle defined backup policies.

For example:

```
oci bv volume-backup-policy delete --backup-policy-id ocid1.volumebackuppolicy.oc1.phx.<unique_ID>
```
**Using the API**

Use the following operations to work with backup policies:

- `CreateVolumeBackupPolicy`
- `DeleteVolumeBackupPolicy`
- `UpdateVolumeBackupPolicy`
- `ListVolumeBackupPolicies`
- `GetVolumeBackupPolicy`

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For more information about backups, see Overview of Block Volume Backups on page 540 and Restoring a Backup to a New Volume on page 557.

**Managing Backup Policy Assignments to Volumes**

If a volume is part of a volume group with a backup policy assignment, the backup policy assignment is managed by the volume group. In this scenario, to update the backup policy assigned you must change the assignment for the volume group or remove the volume from the group.

**To assign a backup policy to a volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click the volume for which you want to assign a backup policy to.
3. On the **Block Volume Information** tab, in **Scheduled Backups**, check the **Managed By** field.

**Using the Console**

You can use the Console to assign, change, or remove both user defined and Oracle defined backup policies for existing volumes.

**To assign a backup policy to a volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click the volume for which you want to assign a backup policy to.
3. On the **Block Volume Information** tab click **Edit**.
4. In the **BACKUP POLICIES** section, select the compartment containing the backup policies.
5. Select the appropriate backup policy for your requirements.
6. Click **Save Changes**.

**To change a backup policy assigned to a volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click the volume for which you want to change the backup policy for.
3. On the **Block Volume Information** tab click **Edit**.
4. In the **BACKUP POLICIES** section, select the compartment containing the backup policy.
5. Select the backup policy you want to switch to.
6. Click **Save Changes**.

**To remove a backup policy assigned to a volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click the volume for which you want to remove the backup policy for.
3. On the **Block Volume Information** tab click **Edit**.
4. In the **BACKUP POLICIES** section, select **None** from the list, and then click **Save Changes**.

**Using the CLI**

For information about using the CLI, see Command Line Interface (CLI) on page 4192.

Use the following operations to work with volume backup policy assignments to volumes:
To assign a backup policy to a volume

Open a command prompt and run:

```
oci bv volume-backup-policy-assignment create --asset-id <volume_ID> --policy-id <policy_ID>
```

For example:

```
oci bv volume-backup-policy-assignment create --asset-id ocid1.volume.oc1..<unique_ID> --policy-id ocid1.volumebackuppolicy.oc1..<unique_ID>
```

To get the backup policy assigned to a volume

Open a command prompt and run:

```
oci bv volume-backup-policy-assignment get-volume-backup-policy-asset-assignment --asset-id <volume_ID>
```

For example:

```
oci bv volume-backup-policy-assignment get-volume-backup-policy-asset-assignment --asset-id ocid1.volume.oc1..<unique_ID>
```

To retrieve a specific backup policy assignment

Open a command prompt and run:

```
oci bv volume-backup-policy-assignment get --policy-assignment-id <backup-policy-ID>
```

For example:

```
oci bv volume-backup-policy-assignment get --policy-assignment-id ocid1.volumebackuppolicyassignment.oc1.phx.<unique_ID>
```

To delete a backup policy assignment

Open a command prompt and run:

```
oci bv volume-backup-policy-assignment delete --policy-assignment-id <backup-policy_ID>
```

You can only delete a user defined backup policy if it is not assigned to any volumes. You cannot delete Oracle defined backup policies.

For example:

```
oci bv volume-backup-policy-assignment delete --policy-assignment-id ocid1.volumebackuppolicyassignment.oc1.phx.<unique_ID>
```

Using the API

Use the following operations to manage backup policy assignments to volumes:

- CreateVolumeBackupPolicyAssignment
- DeleteVolumeBackupPolicyAssignment
- GetVolumeBackupPolicyAssetAssignment
- GetVolumeBackupPolicyAssignment
Restoring a Backup to a New Volume

You can restore a backup of a volume as a new volume using Block Volume.

You can restore a volume from any of your incremental or full volume backups. Both backup types enable you to restore the full volume contents to the point-in-time snapshot of the volume when the backup was taken. You don't need to keep the initial full backup or subsequent incremental backups in the backup chain and restore them in sequence, you only need to keep the backups taken for the times you care about. See Volume Backup Types on page 541 for information about full and incremental backup types.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups.

Tip:

When users create a backup from a volume or restore a volume from a backup, the volume and backup don't have to be in the same compartment. However, users must have access to both compartments.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

1. Open the navigation menu. Under Block Storage, click Block Volume Backups.
   
   A list of the block volume backups in the compartment you're viewing is displayed. If you don’t see the one you're looking for, make sure you’re viewing the correct compartment (select from the list on the left side of the page).
2. Click the Actions icon (three dots) for the block volume backup you want to restore.
3. Click Create Block Volume.
4. Enter a name for the block volume and choose the availability domain in which you want to restore it. Avoid entering confidential information.
5. You can restore a block volume backup to a larger volume size. To do this, check Custom Block Volume Size (GB), and then specify the new size. You can only increase the size of the volume, you cannot decrease the size. If you restore the block volume backup to a larger size volume, you need to extend the volume's partition, see Extending the Partition for a Block Volume on page 536 for more information.
6. Optionally, you can select the appropriate backup policy for your requirements. See Policy-Based Backups on page 547 for more information about backup policies.
7. Optionally, you can encrypt the data in this volume using your own Vault encryption key. To use Vault for your encryption needs, select the Encrypt using Vault check box. Then, select the Vault compartment and Vault that contain the master encryption key you want to use. Also select the Master encryption key compartment and Master encryption key. For more information about encryption, see Overview of Vault on page 3952.
8. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
9. Click Create. The volume will be ready to attach once its icon no longer lists it as **PROVISIONING** in the volume list. For more information, see **Attaching a Volume** on page 517.

**Caution:**

If you want to attach a restored volume that has the original volume attached, be aware that some operating systems do not allow you to restore identical volumes. To resolve this, you should change the partition IDs before restoring the volume. How to change an operating system's partition ID varies by operating system; for instructions, see your operating system's documentation.

**Using the API**

The API used to restore a backup is **CreateVolume**. The API has an optional volumeBackupId parameter that you can use to define the backup from which the data should be restored on the newly created volume. For details, see **CreateVolumeDetails Reference**.

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

For more information about backups, see **Overview of Block Volume Backups** on page 540 and **Backing Up a Volume** on page 546.

**Copying a Volume Backup Between Regions**

You can copy volume backups from one region to another region using the Oracle Cloud Infrastructure Block Volume service. For more information, see **Copying Block Volume Backups Across Regions** on page 542. You can also enable scheduled cross-region automated backups with user defined policies, see **Scheduling Volume Backup Copies Across Regions** on page 548.

**Note:**

When copying block volume backups across regions in your tenancy, you can copy up to five concurrent backups per tenancy at a time from a specific source region.

**Volume Backup Type Considerations**

When volume backups are copied to another region, the volume backup type in the destination region will always match the source **volume backup types**, except for certain scenarios for incremental backups.

Incremental backups will be copied as full volume backups in the following scenarios:

- When the volume backup being copied is the first volume backup taken after a volume has been resized. This applies to volume backups copied on a schedule and volume backups copied manually.
- Volume backups that were the result of a cross region copy, if they are then copied back to their source region. This applies to volume backups copied on a schedule and volume backups copied manually.
- When the volume backup is being copied to a destination region where the previous incremental backup copy is not in the **AVAILABLE** state. This applies to volume backups copied on a schedule and volume backups copied manually.
- When the volume backup is copied out of order. For example, in the scenario where you have incremental volume backups #1 through #5, and you copy volume backup #3 and then volume backup #1, the volume backups may be copied as full backups to the destination region. This only applies to volume backups that are copied manually. This does not apply to volume backups created and copied using backup policies, as scheduled volume backups are always copied in sequential order.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message
For administrators: The first two statements listed in the Let volume admins manage block volumes, backups, and volume groups on page 2146 policy lets the specified group do everything with block volumes and backups with the exception of copying volume backups across regions. The aggregate resource type volume-family does not include the VOLUME_BACKUP_COPY permission, so to enable copying volume backups across regions you need to ensure that you include the third statement in that policy, which is:

```
Allow group VolumeAdmins to use volume-backups in tenancy where request.permission='VOLUME_BACKUP_COPY'
```

To restrict access to just creating and managing volume backups, including copying volume backups between regions, use the policy in Let boot volume backup admins manage only backups on page 2147. The individual resource type volume-backups includes the VOLUME_BACKUP_COPY permission, so you do not need to specify it explicitly in this policy.

If you are copying volume backups encrypted using Vault between regions or you want the copied volume backup to use Vault for encryption in the destination region, you need to use a policy that allows the Block Volume service to perform cryptographic operations with keys in the destination region. For a sample policy showing this, see Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools on page 2153.

### Restricting Access

The specific permissions needed to copy volume backups across regions are:

- **Source region**: VOLUME_BACKUP_READ, VOLUME_BACKUP_COPY
- **Destination region**: VOLUME_BACKUP_CREATE

### Sample Policies

#### To restrict a group to specific source and destination regions for copying volume backups

In this example, the group is restricted to copying volume backups from the UK South (London) region to the Germany Central (Frankfurt) region.

```
Allow group MyTestGroup to read volume-backups in tenancy where all 
{request.region='lhr'}
Allow group MyTestGroup to use volume-backups in tenancy where all 
{request.permission='VOLUME_BACKUP_COPY', request.region = 'lhr'},
Allow group MyTestGroup to manage volume-backups in tenancy where all 
{request.permission='VOLUME_BACKUP_CREATE', request.region = 'fra'}
```

#### To restrict some source regions to specific destination regions while enabling all destination regions for other source regions

In this example, the following is enabled for the group:

- Manage volume backups in all regions.
- Copy volume backups from the US West (Phoenix) and US East (Ashburn) regions to any destination regions.
- Copy volume backups from the Germany Central (Frankfurt) and UK South (London) regions only to the Germany Central (Frankfurt) or UK South (London) regions.

```
Allow group MyTestGroup to read volume-backups in tenancy where all 
{request.region='lhr'}
Allow group MyTestGroup to manage volume-backups in tenancy where any 
{request.permission!=VOLUME_BACKUP_COPY'}
Allow group MyTestGroup to use volume-backups in tenancy where all 
{request.permission='VOLUME_BACKUP_COPY', any {request.region='lhr', request.region='fra'}, any{target.region='fra', target.region='lhr'}}
```
If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Using the Console**

1. Open the navigation menu. Under Block Storage, click Block Volume Backups.

   A list of the block volume backups in the compartment you're viewing is displayed. If you don't see the one you're looking for, make sure you're viewing the correct compartment (select from the list on the left side of the page).

2. Click the Actions icon (three dots) for the block volume backup you want to copy to another region.

3. Click Copy to Another Region.

4. Enter a name for the backup and choose the region to copy the backup to. Avoid entering confidential information.

5. In the Encryption section select whether you want the volume backup to use the Oracle-provided encryption key or your own Vault encryption key. If you select the option to use your own key, paste the OCID for encryption key from the destination region.

6. Click Copy Block Volume Backup.

7. Confirm that the source and destination region details are correct in the confirmation dialog and then click OK.

**Using the API**

To copy a volume backup to another region, use the following operation:

- CopyVolumeBackup

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

**Next Steps**

After copying the block volume backup, switch to the destination region in the Console and verify that the copied backup appears in the list of block volume backups for that region. You can then restore the backup by creating a new block volume from it using the steps in Restoring a Backup to a New Volume on page 557.

For more information about backups, see Overview of Block Volume Backups on page 540.

**Cloning a Volume**

You can create a clone from a volume using the Block Volume service. Cloning enables you to make a copy of an existing block volume without needing to go through the backup and restore process.

A cloned volume is a point-in-time direct disk-to-disk deep copy of the source volume, so all the data that is in the source volume when the clone is created is copied to the clone volume. Any subsequent changes to the data on the source volume are not copied to the clone. Since the clone is a copy of the source volume it will be the same size as the source volume unless you specify a larger volume size when you create the clone.

The clone operation occurs immediately, and you can attach and use the cloned volume as a regular volume as soon as the state changes to available. At this point, the volume data is being copied in the background, and can take up to thirty minutes depending on the size of the volume.

There is a single point-in-time reference for a source volume while it is being cloned, so if the source volume is attached when a clone is created, you need to wait for the first clone operation to complete from the source volume before creating additional clones. If the source volume is detached, you can create up to ten clones from the same source volume simultaneously.

You can only create a clone for a volume within the same region, availability domain and tenant. You can create a clone for a volume between compartments as long as you have the required access permissions for the operation.

For more information about the Block Volume service and cloned volumes, see the Block Volume FAQ.
### Differences Between Block Volume Clones and Backups

Consider the following criteria when you decide whether to create a backup or a clone of a volume.

<table>
<thead>
<tr>
<th>Description</th>
<th>Volume Backup</th>
<th>Volume Clone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a point-in-time backup of data on a volume. You can restore multiple new volumes from the backup later in the future.</td>
<td>Creates a single point-in-time copy of a volume without having to go through the backup and restore process.</td>
<td></td>
</tr>
</tbody>
</table>

| Use case                                  | Retain a backup of the data in a volume, so that you can duplicate an environment later or preserve the data for future use. Meet compliance and regulatory requirements, because the data in a backup remains unchanged over time. Support business continuity requirements. Reduce the risk of outages or data mutation over time. | Rapidly duplicate an existing environment. For example, you can use a clone to test configuration changes without impacting your production environment. |

<table>
<thead>
<tr>
<th>Speed</th>
<th>Slower (minutes or hours)</th>
<th>Faster (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>Lower cost</td>
<td>Higher cost</td>
</tr>
<tr>
<td>Storage location</td>
<td>Object Storage</td>
<td>Block Volume</td>
</tr>
<tr>
<td>Retention policy</td>
<td>Policy-based backups expire, manual backups do not expire</td>
<td>No expiration</td>
</tr>
<tr>
<td>Volume groups</td>
<td>Supported. You can back up a volume group.</td>
<td>Supported. You can clone a volume group.</td>
</tr>
</tbody>
</table>

For more information about block volume backups, see [Overview of Block Volume Backups](#) on page 540 and [Backing Up a Volume](#) on page 546.

### Using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. In the **Block Volumes** list, click the volume that you want to clone.
3. In **Resources**, click **Clones**.
4. Click **Create Clone**.
5. Specify a name for the clone. Avoid entering confidential information.
6. If you want to clone the block volume to a larger size volume, check **Custom Block Volume Size (GB)** and then specify the new size. You can only increase the size of the volume, you cannot decrease the size. If you clone the block volume to a larger size volume, you need to extend the volume's partition. See [Extending the Partition for a Block Volume](#) on page 536 for more information.
7. If you want to change the elastic performance setting when cloning the volume, check **Custom Block Volume Performance** and select the elastic performance setting you want the volume clone to use. See [Block Volume Elastic Performance](#) on page 581 for more information. You can also change the elastic performance setting after you have cloned the volume, see [Block Volume Elastic Performance](#) on page 581. If you leave **Custom Block Volume Performance** unchecked, the cloned volume will use the same elastic performance setting as the source volume.
8. Click **Create Clone**.
The volume is ready use when its icon lists it as **AVAILABLE** in the volume list. At this point, you can perform various actions on the volume such as creating a clone from the volume, attaching it to an instance, or deleting the volume.

**Using the API**

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

To create a clone from a volume, use the `CreateVolume` operation and specify `VolumeSourceFromVolumeDetails` for `CreateVolumeDetails`.

**Disconnecting From a Volume**

For volumes attached with **iSCSI** on page 501 as the volume attachment type you need to disconnect the volume from an instance before you detach the volume. For more information about attachment type options, see [Volume Attachment Types](#) on page 501.

**Required IAM Policy**

Disconnecting a volume from an instance does not require a specific IAM policy. Don't confuse this with detaching a volume (see [Detaching a Volume](#) on page 563).

**Disconnecting from a Volume on a Linux Instance**

Caution: We recommend that you unmount and disconnect the volume from the instance using `iscsiadm` before you detach the volume. Failure to do so may lead to loss of data.

1. Log on to your instance's guest OS and unmount the volume.
2. Run the following command to disconnect the instance from the volume:

   ```
   iscsiadm -m node -T <IQN> -p <Iscsi IP ADDRESS>:<Iscsi PORT> -u
   ```

   A successful logout response resembles the following:

   ```
   Logging out of session [sid: 2, target:
   iqn.2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418, portal:
   169.254.0.2,3260]
   Logout of [sid: 2, target:
   iqn.2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418, portal:
   169.254.0.2,3260] successful.
   ```

3. You can now detach the volume without the risk of losing data.

**Disconnecting from a Volume on a Windows Instance**

1. Use a Remote Desktop client to log on to your Windows instance, and then open Disk Management.
2. Right-click the volume you want to disconnect, and then click Offline.
3. Open iSCSI Initiator, select the target, and then click Disconnect.
4. Confirm the session termination. The status should show as Inactive.
5. In iSCSI Initiator, click the Favorite Targets tab, select the target you are disconnecting, and then click Remove.
6. Click the Volumes and Devices tab, select the volume from the Volume List, and then click Remove.
7. You can now detach the volume without the risk of losing data.
Detaching a Volume

When an instance no longer needs access to a volume, you can detach the volume from the instance without affecting the volume's data.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to attach/detach existing block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

Caution:

For volumes attached using iSCSI on page 501, we recommend that you unmount and disconnect the volume from the instance using iscsiadm before you detach the volume. Failure to do so may lead to loss of data. See Disconnecting From a Volume on page 562 for more information.

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the Instance list locate the instance. Click its name to display the instance details.
3. In the Resources section on the Instance Details page, click Attached Block Volumes
4. Click the Actions icon (three dots) next to the volume you want to detach, and then click Detach. Confirm when prompted.

Using the API

To delete an attachment, use the following operation:

- DetachVolume

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Deleting a Volume

You can delete a volume that is no longer needed.

Caution:

- You cannot undo this operation. Any data on a volume will be permanently deleted once the volume is deleted.
- All policy-based backups will eventually expire, so if you want to keep a volume backup indefinitely, you need to create a manual backup. See Overview of Block Volume Backups on page 540 for information about policy-based and manual backups.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message
that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and
which **compartment** you should work in.

For administrators: The policy in *Let volume admins manage block volumes, backups, and volume groups* on page
2146 lets the specified group do everything with block volumes and backups.

If you're new to policies, see *Getting Started with Policies* on page 2135 and *Common Policies* on page 2142. For
reference material about writing policies for instances, cloud networks, or other Core Services API resources, see
*Details for the Core Services* on page 2181.

**Using the Console**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. In the **Block Volumes** list, find the volume you want to delete.
3. Click **Terminate** next to the volume you want to delete and confirm the selection when prompted.

**Using the API**

To delete a volume, use the following operation:

- **DeleteVolume**

For information about using the API and signing requests, see *REST APIs* on page 4368 and *Security Credentials* on
page 179. For information about SDKs, see *Software Development Kits and Command Line Interface* on page 4225.

**Move Block Volume Resources Between Compartments**

You can move Block Volume resources such as block volumes, boot volumes, volume backups, volume groups,
and volume group backups from one compartment to another. When you move a Block Volume resource to a
new compartment, associated resources are not moved. After you move the resource to the new compartment,
inherent policies apply immediately and affect access to the resource through the Console. For more information, see
*Managing Compartments* on page 2431.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When moving Block Volume resources between compartments you need to ensure that the resource users have sufficient access permissions on the compartment the resource is being moved to.</td>
</tr>
</tbody>
</table>

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access
is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message
that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and
which **compartment** you should work in.

For administrators: The following policies allow users to move Block Volume resources to a different compartment:

- **Allow group BlockCompartmentMovers to manage volume-family in tenancy**

If you're new to policies, see *Getting Started with Policies* on page 2135 and *Common Policies* on page 2142.

**Security Zones**

**Security Zones** ensure that your cloud resources comply with Oracle security principles. If any operation on a
resource in a security zone compartment violates a **policy for that security zone**, then the operation is denied.

The following security zone policies affect your ability to move Block Volume resources from one compartment to
another:

- You can't move a block volume or boot volume from a security zone to a standard compartment.
• You can't move a block volume or boot volume from a standard compartment to a compartment that is in a security zone if the volume violates any security zone policies.

**Using the Console**

**To move a block volume to a new compartment**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. In the **Scope** section, select a compartment.
3. Find the block volume in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To move a block volume backup to a new compartment**

1. Open the navigation menu. Under **Block Storage**, click **Block Volume Backups**.
2. In the **Scope** section, select a compartment.
3. Find the block volume backup in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To move a volume group to a new compartment**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Groups**.
2. In the **Scope** section, select a compartment.
3. Find the volume group in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To move a volume group backup to a new compartment**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Volumes Group Backups**.
2. In the **Scope** section, select a compartment.
3. Find the volume group backup in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To move a boot volume to a new compartment**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. In the **Scope** section, select a compartment.
3. Find the boot volume in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To move a boot volume backup to a new compartment**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volume Backups**.
2. In the **Scope** section, select a compartment.
3. Find the boot volume backup in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**Using the CLI**

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192.
To move a block volume to a new compartment
Open a command prompt and run:

```bash
oci bv volume change-volume-compartment --volume-id <volume OCID> --compartment-id <destination_compartment OCID>
```

To move a block volume backup to a new compartment
Open a command prompt and run:

```bash
oci bv volume-backup change-volume-backup-compartment --volume-backup-id <volume_backup OCID> --compartment-id <destination_compartment OCID>
```

To move a volume group to a new compartment
Open a command prompt and run:

```bash
oci bv volume-group change-volume-group-compartment --volume-group-id <volume_group OCID> --compartment-id <destination_compartment OCID>
```

To move a volume group backup to a new compartment
Open a command prompt and run:

```bash
oci bv volume-group-backup change-volume-group-backup-compartment --volume-group-backup-id <volume_group_backup OCID> --compartment-id <destination_compartment OCID>
```

To move a boot volume to a new compartment
Open a command prompt and run:

```bash
oci bv boot-volume change-boot-volume-compartment --boot-volume-id <boot_volume OCID> --compartment-id <destination_compartment OCID>
```

To move a boot volume backup to a new compartment
Open a command prompt and run:

```bash
oci bv boot-volume-backup change-boot-volume-backup-compartment --boot-volume-backup-id <boot_volume_backup OCID> --compartment-id <destination_compartment OCID>
```

Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations for moving Block Volume resources between compartments:

- ChangeVolumeCompartment
- ChangeVolumeBackupCompartment
- ChangeVolumeGroupCompartment
- ChangeVolumeGroupBackupCompartment
- ChangeBootVolumeCompartment
- ChangeBootVolumeBackupCompartment
Block Volume Performance

The content in the sections below apply to **Category 7** and **Section 2.7.1.8.1** (Oracle Cloud Infrastructure - Block Volume subsection) of the Oracle PaaS and IaaS Public Cloud Services Pillar documentation.

The Oracle Cloud Infrastructure Block Volume service lets you dynamically provision and manage block storage volumes. You can create, attach, connect and move volumes as needed to meet your storage and application requirements. The Block Volume service uses NVMe-based storage infrastructure, and is designed for consistency. You just need to provision the capacity needed and performance scales with the performance characteristics of the elastic performance option selected up to the service maximums. See Block Volume Elastic Performance on page 581 for specific details about the elastic performance options.

The Block Volume service supports creating volumes sized from 50 GB to a maximum size of 32 TB, in 1 GB increments. You can attach up to 32 block volumes to an instance, with a maximum of 1 PB of attached volumes per instance. The instance's boot volume does not count towards this limit.

Latency performance is independent of the instance shape or volume size, and is always sub-millisecond at the 95th percentile for the **Balanced** and **Higher Performance** elastic performance options. Per instance performance is up to 700,000 IOPS, see Host Maximum on page 573.

---

**Note:**

The throughput and IOPS performance results described in this topic are for unformatted iSCSI-attached data volumes, attached to bare metal Compute instances. Performance results may be lower for different scenarios, such as Windows-formatted data volumes, volumes using paravirtualized attachments, boot volumes, among other types of volume scenarios. For more information, see Performance Limitations and Considerations on page 569.

---

**Note:**

You should perform benchmark analysis during proof of concept testing to verify that your environment's configuration will have adequate performance for your application requirements, for more information, see Metrics and Performance Testing on page 569.

---

Higher Performance

The **Higher Performance** elastic performance option is recommended for workloads with the highest I/O requirements, requiring the best possible performance, such as large databases. This option provides the best linear performance scale with 75 IOPS/GB up to a maximum of 35,000 IOPS per volume. Throughput also scales at the highest rate at 600 KBPS/GB up to a maximum of 480 MBPS per volume.

The following table lists the Block Volume service’s throughput and IOPS performance numbers based on volume size for this option. IOPS and KPBS performance scales linearly per GB volume size up to the service maximums so you can predictably calculate the performance numbers for a specific volume size. If you're trying to achieve certain performance targets for volumes configured to use the **Higher Performance** elastic performance option you can provision a minimum volume size using this table as a reference.

<table>
<thead>
<tr>
<th>Volume Size</th>
<th>Max Throughput (1 MB block size)</th>
<th>Max Throughput (8 KB block size)</th>
<th>Max IOPS (4 KB block size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 GB</td>
<td>30 MB/s</td>
<td>30 MB/s</td>
<td>3750</td>
</tr>
<tr>
<td>100 GB</td>
<td>60 MB/s</td>
<td>60 MB/s</td>
<td>7500</td>
</tr>
<tr>
<td>200 GB</td>
<td>120 MB/s</td>
<td>96 MB/s</td>
<td>15,000</td>
</tr>
<tr>
<td>300 GB</td>
<td>180 MB/s</td>
<td>180 MB/s</td>
<td>22,500</td>
</tr>
<tr>
<td>400 GB</td>
<td>240 MB/s</td>
<td>240 MB/s</td>
<td>30,000</td>
</tr>
</tbody>
</table>
### Balanced Performance

The **Balanced** elastic performance option provides a good balance between performance and cost savings for most workloads, including those that perform random I/O such as boot volumes. This option provides linear performance scaling with 60 IOPS/GB up to 25,000 IOPS per volume. Throughput scales at 480 KBPS/GB up to a maximum of 480 MBPS per volume.

The following table lists the Block Volume service's throughput and IOPS performance numbers based on volume size for this option. IOPS and KPBS performance scales linearly per GB volume size up to the service maximums so you can predictably calculate the performance numbers for a specific volume size. If you're trying to achieve certain performance targets for volumes configured to use the **Balanced** elastic performance option you can provision a minimum volume size using this table as a reference.

<table>
<thead>
<tr>
<th>Volume Size</th>
<th>Max Throughput (1 MB block size)</th>
<th>Max Throughput (8 KB block size)</th>
<th>Max IOPS (4 KB block size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 GB</td>
<td>24 MB/s</td>
<td>24 MB/s</td>
<td>3000</td>
</tr>
<tr>
<td>100 GB</td>
<td>48 MB/s</td>
<td>48 MB/s</td>
<td>6000</td>
</tr>
<tr>
<td>200 GB</td>
<td>96 MB/s</td>
<td>96 MB/s</td>
<td>12,000</td>
</tr>
<tr>
<td>300 GB</td>
<td>144 MB/s</td>
<td>144 MB/s</td>
<td>18,000</td>
</tr>
<tr>
<td>400 GB</td>
<td>192 MB/s</td>
<td>192 MB/s</td>
<td>24,000</td>
</tr>
<tr>
<td>500 GB</td>
<td>240 MB/s</td>
<td>200 MB/s</td>
<td>25,000</td>
</tr>
<tr>
<td>750 GB</td>
<td>360 MB/s</td>
<td>200 MB/s</td>
<td>25,000</td>
</tr>
<tr>
<td>1 TB - 32 TB</td>
<td>480 MB/s</td>
<td>200 MB/s</td>
<td>25,000</td>
</tr>
</tbody>
</table>

### Lower Cost

The **Lower Cost** elastic performance option is recommended for throughput intensive workloads with large sequential I/O, such as streaming, log processing, and data warehouses. This option gives you linear scaling 2 IOPS/GB up to a maximum of 3000 IOPS per volume.

The following table lists the Block Volume service's throughput and IOPS performance numbers based on volume size for this option. IOPS and KPBS performance scales linearly per GB volume size up to the service maximums so you can predictably calculate the performance numbers for a specific volume size. If you're trying to achieve certain performance targets for volumes configured to use the **Lower Cost** elastic performance option you can provision a minimum volume size using this table as a reference.

<table>
<thead>
<tr>
<th>Volume Size</th>
<th>Max Throughput (1 MB block size)</th>
<th>Max Throughput (8 KB block size)</th>
<th>Max IOPS (4 KB block size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 GB</td>
<td>12 MB/s</td>
<td>0.8 MB/s</td>
<td>100</td>
</tr>
<tr>
<td>100 GB</td>
<td>24 MB/s</td>
<td>1.6 MB/s</td>
<td>200</td>
</tr>
<tr>
<td>200 GB</td>
<td>48 MB/s</td>
<td>3.2 MB/s</td>
<td>400</td>
</tr>
</tbody>
</table>
## Performance Limitations and Considerations

- Block Volume performance SLA for IOPS per volume and IOPS per instance applies to the **Balanced** and **Higher Performance** elastic performance settings only, not to the **Lower Cost** setting.

- The performance results described in this topic are for unformatted data volumes. Performance is lower for Windows-formatted data volumes. Linux-formatted data volume performance will be similar to performance for unformatted data volumes.

- The throughput performance results are for bare metal Compute instances. Throughput performance on virtual machine (VM) Compute instances is dependent on the network bandwidth that is available to the instance, and further limited by that bandwidth for the volume. For details about the network bandwidth available for VM shapes, see the **Network Bandwidth** column in the VM Shapes on page 658 table.

- IOPS performance is independent of the instance type or shape, so is applicable to all bare metal and VM shapes, for iSCSI attached volumes.

- Block Volume performance SLA for IOPS per volume and IOPS per instance applies to raw, unformatted volumes, with iSCSI volume attachments only, not to paravirtualized volume attachments, at the Block Volume service level.

Paravirtualized attachments simplify the process of configuring your block storage by removing the extra commands needed before accessing a volume. However, due to the overhead of virtualization, this reduces the maximum IOPS performance for larger block volumes. The performance of paravirtualized-attached volumes is 90% of the performance for iSCSI-attached volumes. If storage IOPS performance is of paramount importance for your workloads, you can continue to experience the guaranteed performance Oracle Cloud Infrastructure Block Volume offers by using iSCSI attachments.

Boot volumes are paravirtualized-attached volumes, so the volume performance will reflect this.

- For the **Lower Cost** option you may not see the same latency performance that you see with the **Balanced** or **Higher Performance** elastic performance options. You may also see a greater variance in latency with the **Lower Cost** option.

- Windows Defender Advanced Threat Protection (Windows Defender ATP) is enabled by default on all Oracle-provided Windows images. This tool has a significant negative impact on disk I/O performance. The IOPS performance characteristics described in this topic are valid for Windows bare metal instances with Windows Defender ATP disabled for disk I/O. Customers must carefully consider the security implications of disabling Windows Defender ATP. See Windows Defender Advanced Threat Protection.

- Block volume performance is per volume, so when a block volume is attached to multiple instances the performance is shared across all the attached instances. See Attaching a Volume to Multiple Instances on page 520.

## Metrics and Performance Testing

See Using Block Volumes Service Metrics to Calculate Block Volume Throughput and IOPS for a walkthrough of a performance testing scenario with FIO that shows how you can use Block Volume metrics to determine the performance characteristics of your block volume.

### Performance Table

<table>
<thead>
<tr>
<th>Volume Size</th>
<th>Max Throughput (1 MB block size)</th>
<th>Max Throughput (8 KB block size)</th>
<th>Max IOPS (4 KB block size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>300 GB</td>
<td>72 MB/s</td>
<td>4.8 MB/s</td>
<td>600</td>
</tr>
<tr>
<td>400 GB</td>
<td>96 MB/s</td>
<td>6.4 MB/s</td>
<td>800</td>
</tr>
<tr>
<td>500 GB</td>
<td>120 MB/s</td>
<td>8 MB/s</td>
<td>1000</td>
</tr>
<tr>
<td>750 GB</td>
<td>180 MB/s</td>
<td>12 MB/s</td>
<td>1500</td>
</tr>
<tr>
<td>1 TB</td>
<td>240 MB/s</td>
<td>16 MB/s</td>
<td>2000</td>
</tr>
<tr>
<td>1.5 TB - 32 TB</td>
<td>480 MB/s</td>
<td>23 MB/s</td>
<td>3000</td>
</tr>
</tbody>
</table>
For more information about FIO command samples you can use for performance testing see Sample FIO Commands for Block Volume Performance Tests on Linux-based Instances on page 575.

Testing Methodology and Performance for Balanced Elastic Performance Option

Caution:

- Before running any tests, protect your data by making a backup of your data and operating system environment to prevent any data loss.
- Do not run FIO tests directly against a device that is already in use, such as /dev/sdX. If it is in use as a formatted disk and there is data on it, running FIO with a write workload (readwrite, randrw, write, trimwrite) will overwrite the data on the disk, and cause data corruption. Run FIO only on unformatted raw devices that are not in use.

This section describes the setup of the test environments, the methodology, and the observed performance for the Balanced elastic performance configuration option. Some of the sample volume sizes tested were:

- 50 GB volume - 3,000 IOPS @ 4K
- 1 TB volume - 25,000 IOPS @ 4K
- Host maximum, Ashburn (IAD) region, twenty 1 TB volumes - 400,000 IOPS @ 4K

These tests used a wide range of volume sizes and the most common read and write patterns and were generated with the Gartner Cloud Harmony test suite. To show the throughput performance limits, 256k or larger block sizes should be used. For most environments, 4K, 8K, or 16K blocks are common depending on the application workload, and these are used specifically for IOPS measurements.

In the observed performance images in this section, the X axis represents the volume size tested, ranging from 4KB to 1MB. The Y axis represents the IOPS delivered. The Z axis represents the read/write mix tested, ranging from 100% read to 100% write.

Note:

Performance Notes for Instance Types

- The throughput performance results are for bare metal instances. Throughput performance on VM instances is dependent on the network bandwidth that is available to the instance, and further limited by that bandwidth for the volume. For details about the network bandwidth available for VM shapes, see the Network Bandwidth column in the VM Shapes table.
- IOPS performance is independent of the instance type or shape, so is applicable to all bare metal and VM shapes, for iSCSI attached volumes.

1 TB Block Volume

A 1 TB volume was mounted to a bare metal instance running in the Phoenix region. The instance shape was dense, workload was direct I/O with 10GB working set. The following command was run for the Gartner Cloud Harmony test suite:

```
~/block-storage/run.sh --nopurge --noprecondition --fio_direct\=1 --fio_size=10g --target /dev/sdb --test iops --skip_blocksize 512b
```

The results showed that for 1 TB, the bandwidth limit for the larger block size test occurs at 320MBS.

The following images show the observed performance for 1 TB:
Steep State Determination Data

<table>
<thead>
<tr>
<th>Steep State Determination Data</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Average IOPS</td>
<td>22152</td>
</tr>
<tr>
<td>Allowed Maximum Data Excursion</td>
<td>5096.497</td>
</tr>
<tr>
<td>Measured Maximum Data Excursion</td>
<td>4106.5521</td>
</tr>
<tr>
<td>Allowed Maximum Slope Excursion</td>
<td>2529.2485</td>
</tr>
<tr>
<td>Measured Maximum Slope Excursion</td>
<td>159.9</td>
</tr>
<tr>
<td>Least Squares Linear Fit Formula</td>
<td>-39.97 + X + 23412.410</td>
</tr>
</tbody>
</table>

Plot A.3 - IOPS Steady State Measurement Window - RNDV4KIB
**50 GB Block Volume**

A 50 GB volume was mounted to a bare metal instance running in the Phoenix region. The instance shape was dense, workload was direct I/O with 10GB working set. The following command was run for the Gartner Cloud Harmony test suite:

```
~/block-storage/run.sh --nopurge --noprecondition --fio_direct=1 --fio_size=10g --target /dev/sdb --test iops --skip_blocksize 512b
```

The results showed that for the 50 GB volume, the bandwidth limit is confirmed as 24,000 KBPS for the larger block size tests (256 KB or larger block sizes), and the maximum of 3,000 IOPS at 4K block size is delivered. For small volumes, a 4K block size is common.

The following images show the observed performance for 50 GB:
 Depending on the instance shape, a single instance with multiple attached volumes can achieve performance of up to 700,000 IOPS when the elastic performance settings for the attached volumes are set to balanced or higher performance.

To test performance, run the following command for the Gartner Cloud Harmony test suite using thirty 800 GB higher performance volumes:

```
sudo ./run.sh --savefio --nopurge --noprecondition --nozerofill --nosecureerase --notrim -v --fio_direct=1 --fio_size=10g --target /dev/sdy, /dev/sdf, /dev/sda, /dev/sdaa, /dev/sdc, /dev/sda, /dev/sde, /dev/sdaa, /dev/sdc, /dev/sda, /dev/sde, /dev/sdaa, /dev/sdc, /dev/sda, /dev/sde, /dev/sdaa, /dev/sdc, --test iops --skip_blocksize 512b&
```

The following images show the observed performance:
Sample FIO Commands for Block Volume Performance Tests on Linux-based Instances

This topic describes sample FIO commands you can use to run performance tests for the Oracle Cloud Infrastructure Block Volume service on instances created from Linux-based images.

Installing FIO

To install and configure FIO on your instances with Linux-based operating systems, run the commands applicable to the operating system version for your instance.

**Oracle Linux and CentOS**

Run the following command to install and configure FIO for your Oracle Linux or CentOS systems.

- Oracle Linux 8:
  ```bash
  sudo dnf install fio -y
  ```
- Oracle Autonomous Linux 7.x, Oracle Linux 6.x, Oracle Linux 7.x, CentOS 7.x, and CentOS 8.x:
  ```bash
  sudo yum install fio -y
  ```

**Ubuntu**

Run the following commands to install and configure FIO for your Ubuntu systems:

```bash
sudo apt-get update & & sudo apt-get install fio -y
```

This applies to Ubuntu 16.04, 18.04, and Ubuntu Minimal 16.04, 18.04.
**FIO Commands**

**IOPS Performance Tests**

Use the following FIO example commands to test IOPS performance. You can run the commands directly or create a job file with the command and then run the job file.

**Test random reads**

Run the following command directly to test random reads:

```
sudo fio --filename=device name --direct=1 --rw=randread --bs=4k --
ioengine=libaio --iodepth=256 --runtime=120 --numjobs=4 --time_based --
group_reporting --name=iops-test-job --eta-newline=1 --readonly
```

In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fiorandomread.fio, with the following:

   ```
   [global]
   bs=4K
   iodepth=256
   direct=1
   ioengine=libaio
   group_reporting
   time_based
   runtime=120
   numjobs=4
   name=raw-randread
   rw=randread
   
   [job1]
   filename=device name
   ```

2. Run the job using the following command:

   ```
fio randomread.fio
   ```

**Test file random read/writes**

Run the following command against the mount point to test file read/writes:

```
sudo fio --filename=/custom mount point/file --size=500GB --direct=1 --
rw=randrw --bs=4k --ioengine=libaio --iodepth=256 --runtime=120 --numjobs=4
--time_based --group_reporting --name=iops-test-job --eta-newline=1
```

Add both the read IOPS and the write IOPS returned.

**Test random read/writes**

**Caution:**

Do not run FIO tests with a write workload (readwrite, randrw, write, trimwrite) directly against a device that is in use.

Run the following command to test random read/writes:

```
sudo fio --filename=device name --direct=1 --rw=randrw --bs=4k --
ioengine=libaio --iodepth=256 --runtime=120 --numjobs=4 --time_based --
group_reporting --name=iops-test-job --eta-newline=1
```

Add both the read IOPS and the write IOPS returned.
In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fiorandomreadwrite.fio, with the following:

```
[globals]
bs=4K
iodepth=256
direct=1
ioengine=libaio
group_reporting
time_based
runtime=120
numjobs=4
name=raw-randomreadwrite
rw=randrw

[job1]
filename=device name
```

2. Run the job using the following command:

```
fio randomreadwrite.fio
```

**Test sequential reads**

For workloads that enable you to take advantage of sequential access patterns, such as database workloads, you can confirm performance for this pattern by testing sequential reads.

Run the following command to test sequential reads:

```
sudo fio --filename=device name --direct=1 --rw=read --bs=4k --
ioengine=libaio --iodepth=256 --runtime=120 --numjobs=4 --time_based --
group_reporting --name=iops-test-job --eta-newline=1 --readonly
```

In some cases you may see more consistent results if you use a job file instead of running the command directly. Use the following instructions for this approach:

1. Create a job file, fioread.fio, with the following:

```
[globals]
bs=4K
iodepth=256
direct=1
ioengine=libaio
group_reporting
time_based
runtime=120
numjobs=4
name=raw-read
rw=read

[job1]
filename=device name
```

2. Run the job using the following command:

```
fio read.fio
```

**Throughput Performance Tests**

Use the following FIO example commands to test throughput performance.
**Test random reads**

Run the following command to test random reads:

```
sudo fio --filename=device name --direct=1 --rw=randread --bs=64k --
ioengine=libaio --iodepth=64 --runtime=120 --numjobs=4 --time_based --
group_reporting --name=throughput-test-job --eta-newline=1 --readonly
```

In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fiorandomread.fio, with the following:

   ```
   [global]
   bs=64K
   iodepth=64
   direct=1
   ioengine=libaio
   group_reporting
   time_based
   runtime=120
   numjobs=4
   name=raw-randread
   rw=randread
   
   [job1]
   filename=device name
   ```

2. Run the job using the following command:

   ```
fio randomread.fio
   ```

**Test file random read/writes**

Run the following command against the mount point to test file read/writes:

```
sudo fio --filename=/custom mount point/file --size=500GB --direct=1 --
wtrandrw --bs=64k --ioengine=libaio --iodepth=64 --runtime=120 --numjobs=4
--time_based --group_reporting --name=throughput-test-job --eta-newline=1
```

Add both the read MBPs and the write MBPs returned.

**Test random read/writes**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not run FIO tests with a write workload (readwrite, randrw, write, trimwrite) directly against a device that is in use.</td>
</tr>
</tbody>
</table>

Run the following command to test random read/writes:

```
sudo fio --filename=device name --direct=1 --rw=randrw --bs=64k --
ioengine=libaio --iodepth=64 --runtime=120 --numjobs=4 --time_based --
group_reporting --name=throughput-test-job --eta-newline=1
```

Add both the read MBPs and the write MBPs returned.

In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fiorandomread.fio, with the following:

   ```
   [global]
   bs=64K
   ```
iodepth=64
direct=1
ioengine=libaio
group_reporting
time_based
runtime=120
numjobs=4
name=raw-randreadwrite
rw=randrw

[job1]
filename=device name

2. Run the job using the following command:

fio randomreadwrite.fio

Test sequential reads

For workloads that enable you to take advantage of sequential access patterns, such as database workloads, you can confirm performance for this pattern by testing sequential reads.

Run the following command to test sequential reads:

```
sudo fio --filename=device name --direct=1 --rw=read --bs=64k --
ioengine=libaio --iodepth=64 --runtime=120 --numjobs=4 --time_based --
group_reporting --name=throughput-test-job --eta-newline=1 --readonly
```

In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fioread.fio, with the following:

```
[global]
bs=64K
iodepth=64
direct=1
ioengine=libaio
group_reporting
time_based
runtime=120
numjobs=4
name=raw-read
rw=read

[job1]
filename=device name
```

2. Run the job using the following command:

```
fio read.fio
```

Latency Performance Tests

Use the following FIO example commands to test latency performance. You can run the commands directly or create a job file with the command and then run the job file.
**Test random reads for latency**

Run the following command directly to test random reads for latency:

```
sudo fio --filename=device name --direct=1 --rw=randread --bs=4k --
ioengine=libaio --iodepth=1 --numjobs=1 --time_based --group_reporting --
name=readlatency-test-job --runtime=120 --eta-newline=1 --readonly
```

In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fiorandomreadlatency.fio, with the following:

```
[global]
bs=4K
iodepth=1
direct=1
ioengine=libaio
group_reporting
time_based
runtime=120
numjobs=1
name=readlatency-test-job
rw=randread

[job1]
filename=device name
```

2. Run the job using the following command:

```
fio fiorandomreadlatency.fio
```

**Test random read/writes for latency**

```
Caution:
Do not run FIO tests with a write workload (readwrite, randrw, write, trimwrite) directly against a device that is in use.
```

Run the following command directly to test random read/writes for latency:

```
sudo fio --filename=device name --direct=1 --rw=randrw --bs=4k --
ioengine=libaio --iodepth=1 --numjobs=1 --time_based --group_reporting --
name=rwlatency-test-job --runtime=120 --eta-newline=1 --readonly
```

In some cases you might see more consistent results if you use a job file instead of running the command directly. Use the following steps for this approach.

1. Create a job file, fiorandomrwlatency.fio, with the following:

```
[global]
bs=4K
iodepth=1
direct=1
ioengine=libaio
group_reporting
time_based
runtime=120
numjobs=1
name=rwlatency-test-job
rw=randrw

[job1]
```
2. Run the job using the following command:

```
filename=device name
```

```
fio fioradomrwlateny.fio
```

## Block Volume Elastic Performance

The elastic performance feature of the Oracle Cloud Infrastructure Block Volume service allows you to dynamically change the volume performance, along with enabling you to pay for the performance characteristics you require independently from the size of your block volumes and boot volumes.

This feature includes the concept of volume performance units (VPUs). You can purchase more VPUs to allocate more resources to a volume, increasing IOPS/GB and throughput per GB. You also have the flexibility to purchase fewer VPUs, which reduces the performance characteristics for a volume, however it can also provide cost savings. You can also choose not to purchase any VPUs which can provide significant cost savings for volumes that don’t require the increased performance characteristics.

For specific pricing details, see [Oracle Storage Cloud Pricing](#).

### Elastic Performance Configuration Options

There are three elastic performance configuration options, as described below.

- **Balanced**: This is the default setting for new and existing block and boot volumes. It provides a good balance between performance and cost savings for most workloads, including those that perform random I/O such as boot volumes. This option provides linear performance scaling with 60 IOPS/GB up to 25,000 IOPS per volume. Throughput scales at 480 KBPS/GB up to a maximum of 480 MBPS per volume. With this option you are purchasing 10 VPUs per GB/month.

- **Higher Performance**: Recommended for workloads with the highest I/O requirements, requiring the best possible performance, such as large databases. This option provides the best linear performance scale with 75 IOPS/GB up to a maximum of 35,000 IOPS per volume. Throughput also scales at the highest rate at 600 KBPS/GB up to a maximum of 480 MBPS per volume. With this option you are purchasing 20 VPUs per GB/month.

- **Lower Cost**: Recommended for throughput intensive workloads with large sequential I/O, such as streaming, log processing, and data warehouses. The cost is only the storage cost, there is no additional VPU cost. This option gives you linear scaling 2 IOPS/GB up to a maximum of 3000 IOPS per volume. This option is only available for block volumes, it is not available for boot volumes.

The following table lists the performance characteristics for each elastic performance level.

<table>
<thead>
<tr>
<th>Performance Level</th>
<th>IOPS/GB</th>
<th>Max IOPS/Volume</th>
<th>Throughput/GB (KB/s per GB)</th>
<th>Max Throughput/Volume (MB/s per volume)</th>
<th>VPUs/GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower Cost</td>
<td>2</td>
<td>3000</td>
<td>240</td>
<td>Up to 480</td>
<td>0</td>
</tr>
<tr>
<td>Balanced</td>
<td>60</td>
<td>25,000</td>
<td>480</td>
<td>480</td>
<td>10</td>
</tr>
<tr>
<td>Higher Performance</td>
<td>75</td>
<td>35,000</td>
<td>600</td>
<td>480</td>
<td>20</td>
</tr>
</tbody>
</table>

See [Block Volume Performance](#) on page 567 for additional performance details for the Block Volume service.

VPUs refer to volume performance units, see [Oracle Storage Cloud Pricing](#) for specific pricing details.

### Configuring Volume Performance

You can configure the volume performance for a block volume when you create a volume, see [Creating a Volume](#) on page 515. You can also change the volume performance for an existing block volume, see [To change the volume performance for an existing block volume](#) on page 582.
When you create a Compute instance, the volume performance for the instance's boot volume is set to Balanced by default. You can change this setting after the instance has launched, see To change the volume performance for an existing boot volume on page 582.

### Changing the Performance of a Volume

The Block Volume service's elastic performance feature enables you to dynamically configure the volume performance for block volumes and boot volumes, for more information, see Block Volume Elastic Performance on page 581.

#### Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

#### Limitations

- You can only change the elastic performance configuration on three volumes concurrently per tenancy.
- When changing volume performance for boot volumes, you can only select the Balanced or Higher Performance options.

#### Using the Console

The default volume performance setting for existing block volumes or when you create a new block volume is Balanced. You can change the default setting when you create a new block volume, see Creating a Volume on page 515. You can also change the volume performance setting for an existing block volume using the steps in the following procedure.

To change the volume performance for an existing block volume

1. Open the navigation menu. Under Core Infrastructure, go to Block Storage and click Block Volumes.
2. Click the block volume that you want to change the performance for.
3. Click Edit Size or Performance.
4. Click the volume performance option you want to change to.
5. Click Save Changes.

When you create an instance, the volume performance setting for the instance's boot volume is set to Balanced. You can change this setting to Higher Performance after the instance has been launched.

To change the volume performance for an existing boot volume

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Boot Volumes.
2. Click the boot volume that you want to change the performance for.
3. Click Edit Size or Performance.
4. Click the volume performance option you want to change to.
5. Click Save Changes.

#### Using the CLI

For information about using the CLI, see Command Line Interface (CLI) on page 4192.

Use the `volume update` operation or the `boot-volume update` operation with `vpus-per-gb` parameter to update a block volume's elastic performance setting. The `vpus-per-gb` parameter is where you specify the volume performance units (VPUs). VPUs represent the volume performance settings, with the following allowed values:
### Block Volume

- **0**: Represents **Lower Cost** setting, applies to block volumes only.
- **10**: Represents **Balanced** setting, applies to both block volumes and boot volumes.
- **20**: Represents **Higher Performance** setting, applies to both block volumes and boot volumes.

For example:

```bash
oci bv volume update --volume-id <volume_ID> --vpus-per-gb 20
```

### Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

### Block Volumes

To update a block volume's performance setting, use the following operation:

- **UpdateVolume**

  The volume performance setting is specified in the `vpusPerGB` attribute of `UpdateVolumeDetails`. Allowed values are 0, 10, and 20.

### Boot Volumes

To update a boot volume's performance setting, use the following operation:

- **UpdateBootVolume**

  The volume performance setting is specified in the `vpusPerGB` attribute of `UpdateBootVolumeDetails`. Allowed values are 10 and 20.

### Auto-tune Volume Performance

The Block Volume service has three elastic performance configuration options:

- **Balanced**
- **Higher Performance**
- **Lower Cost**

For more information about these settings, see [Block Volume Elastic Performance](#) on page 581. The auto-tune feature enables you to configure your block volumes and boot volumes to use the optimal performance setting based on whether the volume is attached or detached from an instance.

When you create a volume, the default volume performance setting is **Balanced**. You can change this default performance setting when you create the volume, see [Creating a Volume](#) on page 515. You can also change the default performance setting on an existing volume, see [Changing the Performance of a Volume](#) on page 582. When the performance auto-tune feature is disabled, your volume’s performance will always be the default performance setting. If performance auto-tune is enabled, when your block volume is attached to one or more instances, the volume’s performance will be the default performance setting. When the volume is detached, the Block Volume service will adjust the performance setting to **Lower Cost** for both block volumes and boot volumes. When the volume is reattached, the performance is adjusted back to the default performance setting.

When viewing the **Block Volume Details** or **Boot Volume Details** pages in the Console, the applicable fields are:

- **Current Performance**: This is the volume’s effective performance. If the auto-tune performance feature is disabled for the volume, **Current Performance** will always be what is specified in the **Default Performance**, regardless of whether the volume is attached or detached. If the auto-tune performance feature is enabled for the volume, **Current Performance** will be adjusted to **Lower Cost** when the volume is detached. Note that **Current Performance** won’t show the performance setting as **Lower Cost** until the performance adjustment is complete.
- **Default Performance**: This is the volume’s performance setting that you specify when you create the volume or when you change the performance setting for an existing volume. When the volume is attached, regardless of whether the auto-tune performance feature is enabled or not, this is the volume’s performance.
• **Auto-tune Performance**: This field indicates whether the auto-tune performance feature is enabled for the volume. When it is off, the volume’s effective performance is always the same as what is specified for **Default Performance**. When it is on, the volume performance is adjusted to **Lower Cost** when the volume is detached.

See **Timing Limits and Considerations** for details about when these settings take effect.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators: The policy in **Let volume admins manage block volumes, backups, and volume groups** on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you’re new to policies, see **Getting Started with Policies** on page 2135 and **Common Policies** on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see **Details for the Core Services** on page 2181.

**Timing Limits and Considerations**

The following list identifies some timing considerations you should be aware of when using the performance auto-tune feature.

• When you enable the auto-tune performance feature for a detached volume, the Block Volume service starts the performance adjustment to **Lower Cost** after 14 days.

• When you enable the auto-tune performance feature for an attached volume, the Block Volume service starts the performance adjustment to **Lower Cost** 14 days after you detach the volume.

• If you disable the auto-tune performance feature while a volume is detached, Block Volume service starts the performance adjustment to the **Default Performance** setting right away.

• Attaching a volume with the auto-tune performance feature enabled may take longer than attaching a volume with it off, as the Block Volume service adjusts the performance before the volume attachment completes.

• If you change the **Default Performance** for a detached volume with the auto-tune performance feature enabled, the **Current Performance** for the volume will remain **Lower Cost** until you reattach the volume.

• If you clone a detached volume with the auto-tune performance feature enabled, the Block Volume service starts the performance adjustment to **Lower Cost** after 14 days.

**Using the Console**

The following procedures describe how to enable the auto-tune performance feature in the Console.

**To enable the auto-tune performance feature for a block volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Click the block volume that you want to enable the auto-tune performance feature for.
3. Click **Edit**.
4. In the **Volume Size and Performance** section, click the **AUTO-TUNE PERFORMANCE** slider so that it changes from **Off** to **On**.
5. Click **Save Changes**.

**To enable the auto-tune performance feature for a boot volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. Click the boot volume that you want to enable the auto-tune performance feature for.
3. Click **Edit**.
4. In the **Volume Size and Performance** section, click the **AUTO-TUNE PERFORMANCE** slider so that it changes from **Off** to **On**.
5. Click **Save Changes**.
Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Block Volumes
To enable or disable the auto-tune performance feature for a block volume, use the following operation:

• UpdateVolume

The auto-tune performance setting is specified in the isAutoTuneEnabled attribute of UpdateVolumeDetails.

Boot Volumes
To enable or disable the auto-tune performance feature for a boot volume, use the following operation:

• UpdateBootVolume

The auto-tune performance setting is specified in the isAutoTuneEnabled attribute of UpdateBootVolumeDetails.

Block Volume Metrics
You can monitor the health, capacity, and performance of your block volumes and boot volumes by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace oci_blockstore (the Block Volume service) Resources: Block volumes and boot volumes

See Using Block Volumes Service Metrics to Calculate Block Volume Throughput and IOPS for a walkthrough of a performance testing scenario with FIO that shows how you can use these metrics to determine the performance characteristics of your block volume.

Overview of Metrics for an Instance and Its Storage Devices
If you're not already familiar with the different types of metrics available for an instance and its storage and network devices, see Compute Instance Metrics on page 788.

Available Metrics: oci_blockstore
The Block Volume service metrics help you measure volume operations and throughput related to Compute instances.

The metrics listed in the following table are automatically available for any block volume or boot volume, regardless of whether the attached instance has monitoring enabled. You do not need to enable monitoring on the volumes to get these metrics.

You also can use the Monitoring service to create custom queries.

Each metric includes the following dimensions:

ATTACHMENTID
The OCID of the volume attachment.

RESOURCEID
The OCID of the volume.
### Block Volume

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolumeReadThroughput</td>
<td>Volume Read Throughput</td>
<td>bytes</td>
<td>Read throughput. Expressed as bytes read per interval.</td>
<td>attachmentId, resourceId</td>
</tr>
<tr>
<td>VolumeWriteThroughput</td>
<td>Volume Write Throughput</td>
<td>bytes</td>
<td>Write throughput. Expressed as bytes written per interval.</td>
<td></td>
</tr>
<tr>
<td>VolumeReadOps*</td>
<td>Volume Read Operations</td>
<td>reads</td>
<td>Activity level from I/O reads. Expressed as reads per interval.</td>
<td></td>
</tr>
<tr>
<td>VolumeWriteOps*</td>
<td>Volume Write Operations</td>
<td>writes</td>
<td>Activity level from I/O writes. Expressed as writes per interval.</td>
<td></td>
</tr>
</tbody>
</table>

* The Compute service separately reports network-related metrics as measured on the instance itself and aggregated across all the attached volumes. Those metrics are available in the `oci_computeagent` metric namespace. For more information, see Compute Instance Metrics on page 788.

### Using the Console

**To view default metric charts for a single volume**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance to view its details.
3. Under Resources, click either Attached Block Volumes or Boot Volume to view the volume you're interested in.
4. Click the volume to view its details.
5. Under Resources, click Metrics.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**To view default metric charts for multiple volumes**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that contains the volumes you're interested in.
3. For Metric Namespace, select `oci_blockstore`.

   The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)
Chapter 10

Compliance Documents

This chapter explains how to view and download compliance documents.

Overview of Compliance Documents

The Oracle Cloud Infrastructure Compliance Documents service lets you view and download compliance documents that you could previously access only by submitting a request to the Elevated Support Portal.

Note:
Compliance Documents is not available in Oracle Cloud Infrastructure Government Cloud realms.

Types of Compliance Documents

When viewing compliance documents, you can filter on the following types:

- **Audit**: A general audit report.
- **Bridge Letter (BridgeLetter)**: A bridge letter. Bridge letters provide compliance information for the period of time between the end date of an SOC report and the date of the release of a new SOC report.
- **Certificate**: A document indicating certification by a particular authority, with regard to certification requirements and examination results conforming to said requirements.
- **SOC3**: A Service Organization Controls 3 audit report that provides information relating to a service organization's internal controls for security, availability, confidentiality, and privacy.
- **Other**: A compliance document that doesn't fit into any of the preceding, more specific categories.

If you need to further narrow down what documents are displayed, you can combine the type filter with the environment filter.

Types of Environments

The environments, or business pillars or platforms, to which the documents belong include:

- **OCI**: Oracle Cloud Infrastructure is a set of complementary cloud infrastructure services that let you build and run applications and services in a highly available hosted environment.
- **PAAS**: Oracle Platform as a Service (PaaS) provides various platforms to build and deploy applications within the public, private, or hybrid cloud.

Regions and Availability Domains

You can use the Compliance Documents service in all regions. For a list of supported regions, see Regions and Availability Domains on page 180.
Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. However, you cannot specifically access Compliance Documents by using the API or Command Line Interface (CLI). Compliance Documents does not have public API, SDK, or CLI support at this time.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Viewing and Downloading Compliance Documents

This section describes how to view compliance documents. The Console displays documents available to your tenancy for the currently selected region.

To view a list of all compliance documents

1. Open the navigation menu. Under the Governance and Administration group, go to Governance and click Compliance Documents.
2. The Compliance Documents page displays all documents you have permission to view. From this page, you can do the following:
   - Filter. You can filter documents by environment or by type.
   - Sort. You can sort documents by name, type, or creation date.
   - Download. You can download documents to your local computer.

To download a compliance document

1. Open the navigation menu. Under the Governance and Administration group, go to Governance and click Compliance Documents.
2. The Compliance Documents page displays all documents you have permission to view.
3. Next to the name of the document, click Download.
4. Review the terms of use.
5. When you're ready, select the I have reviewed and accept these terms and conditions check box, and then click Download File.

To sort a list of compliance documents

1. Open the navigation menu. Under the Governance and Administration group, go to Governance and click Compliance Documents.
2. By default, the list displays documents according to the document name, in alphabetical order. To sort the list another way, do one of the following:
   - Click Name. The list sorts alphabetically, according to the summary of the announcement. If you begin by viewing the default sort order, the sort order will change to show documents in reverse alphabetical order by name.
   - Click Type. The list sorts according to the type of the document, in alphabetical order by type.
   - Click Created. The list sorts according to the date and time the document was created.
3. To sort the list again, repeat the previous step.
Chapter 11

Compute

This chapter explains how to launch, access, manage, and terminate compute instances.

Overview of the Compute Service

Oracle Cloud Infrastructure Compute lets you provision and manage compute hosts, known as instances. You can launch instances as needed to meet your compute and application requirements. After you launch an instance, you can access it securely from your computer, restart it, attach and detach volumes, and terminate it when you're done with it. Any changes made to the instance's local drives are lost when you terminate it. Any saved changes to volumes attached to the instance are retained.

Oracle Cloud Infrastructure offers both bare metal and virtual machine instances:

- **Bare Metal**: A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.
- **Virtual Machine**: A virtual machine (VM) is an independent computing environment that runs on top of physical bare metal hardware. The virtualization makes it possible to run multiple VMs that are isolated from each other. VMs are ideal for running applications that do not require the performance and resources (CPU, memory, network bandwidth, storage) of an entire physical machine.

An Oracle Cloud Infrastructure VM compute instance runs on the same hardware as a bare metal instance, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure.

Be sure to review Best Practices for Your Compute Instance on page 594 for important information about working with your Oracle Cloud Infrastructure Compute instance.

Oracle Cloud Infrastructure uses Oracle Ksplice to apply important security and other critical kernel updates to the hypervisor hosts without a reboot. Oracle Cloud Infrastructure can apply these patches transparently without the need to pause any VMs, and all hypervisor hosts support this capability. For more information, see Installing and Running Oracle Ksplice on page 664.

Compute is Always Free eligible. For more information about Always Free resources, including capabilities and limitations, see Oracle Cloud Infrastructure Free Tier on page 140.

Instance Types

When you create a Compute instance, you can select the most appropriate type of instance for your applications based on characteristics such as the number of CPUs, amount of memory, and network resources. Oracle Cloud Infrastructure offers a variety of shapes that are designed to meet a range of compute and application requirements:

- **Standard shapes**: Designed for general purpose workloads and suitable for a wide range of applications and use cases. Standard shapes provide a balance of cores, memory, and network resources. Standard shapes are available with Intel or AMD processors.
- **DenseIO shapes**: Designed for large databases, big data workloads, and applications that require high-performance local storage. DenseIO shapes include locally-attached NVMe-based SSDs.
- **GPU shapes**: Designed for hardware-accelerated workloads. GPU shapes include Intel or AMD CPUs and NVIDIA graphics processors.
• **High performance computing (HPC) shapes:** Designed for high-performance computing workloads that require high frequency processor cores and cluster networking for massively parallel HPC workloads. HPC shapes are available for bare metal instances only.

For more information about the available bare metal and VM shapes, see Compute Shapes on page 655, Bare Metal Instances, Virtual Machines, and Virtual Machines and Bare Metal (GPU).

**Flexible Shapes**

Flexible shapes let you customize the number of OCPUs and the amount of memory allocated to an instance. When you create a VM instance using the flexible shape, you select the number of OCPUs and the amount of memory that you need for the workloads that run on the instance. The network bandwidth and number of VNICS scale proportionately with the number of OCPUs. This flexibility enables you to build VMs that match your workload, allowing you to optimize performance and minimize cost. For more information, see Flexible Shapes on page 655.

Currently, flexible memory is available on VM.Standard.E3.Flex instances that run on AMD Rome processors. For this VM and processor combination, you can select from 1 to 64 OCPUs. The amount of memory allowed is based on the number of OCPUs selected. For each OCPU, you can select up to 64 GB of memory, with a maximum of 1024 GB total. The minimum amount of memory allowed is either 1 GB or a value matching the number of OCPUs, whichever is greater.

**Components for Launching Instances**

The components required to launch an instance are:

- **availability domain**
  The Oracle Cloud Infrastructure data center within your geographical region that hosts cloud resources, including your instances. You can place instances in the same or different availability domains, depending on your performance and redundancy requirements. For more information, see Regions and Availability Domains on page 180.

- **virtual cloud network**
  A virtual version of a traditional network—including subnets, route tables, and gateways—on which your instance runs. At least one cloud network has to be set up before you launch instances. For information about setting up cloud networks, see Networking Overview on page 2748.

- **key pair (for Linux instances)**
  A security mechanism required for Secure Shell (SSH) access to an instance. Before you launch an instance, you’ll need at least one key pair. For more information, see Managing Key Pairs on Linux Instances on page 693.

- **tags**
  You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

- **password (for Windows instances)**
  A security mechanism required to access an instance that uses an Oracle-provided Windows image. The first time you launch an instance using a Windows image, Oracle Cloud Infrastructure will generate an initial, one-time password that you can retrieve using the console or API. This password must be changed after you initially log on.

- **image**
  A template of a virtual hard drive that determines the operating system and other software for an instance. For details about Oracle Cloud Infrastructure platform images, see Oracle-Provided Images on page 629. You can also launch instances from:
Compute

- Trusted third-party images published by Oracle partners from the Partner Image catalog. For more information about partner images, see Overview of Marketplace on page 2650 and Working with Listings on page 2651.
- Pre-built Oracle enterprise images and solutions enabled for Oracle Cloud Infrastructure
- Custom images, including bring your own image scenarios.
- Boot Volumes on page 609.

**shape**

A template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance. You choose the most appropriate shape when you launch an instance. See Compute Shapes on page 655 for a list of available bare metal and VM shapes.

You can optionally attach volumes to an instance. For more information, see Overview of Block Volume on page 500.

**Creating Automation with Events**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

The following Compute resources emit events:

- Autoscaling configurations and autoscaling policies
- Cluster networks
- Console histories
- Images
- Instances and instance attachments
- Instance configurations
- Instance console connections
- Instance pools

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

**Work Requests**

Compute is one of the Oracle Cloud Infrastructure services that is integrated with the Work Requests API. For general information on using work requests in Oracle Cloud Infrastructure, see Work Requests in the user guide, and the Work Requests API.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.
Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Storage for Compute Instances

You can expand the storage that's available for your Compute instances with the following services:

- **Block Volume**: Lets you dynamically provision and manage block volumes that you can attach to one or more Compute instances. See Overview of Block Volume on page 500 for more information. For steps to attach block volumes to Compute instances, see Attaching a Volume on page 517 and Attaching a Volume to Multiple Instances on page 520.
- **File Storage**: A durable, scalable, secure, enterprise-grade network file system that you can connect to from any Compute instance in your virtual cloud network (VCN). See Overview of File Storage on page 1920 for more information.
- **Object Storage**: An internet-scale, high-performance storage platform that lets you store an unlimited amount of unstructured data of any content type. This storage is regional and not tied to any specific Compute instance. See Overview of Object Storage on page 3392 for more information.
- **Archive Storage**: A storage platform that lets you store an unlimited amount of unstructured data of any content type that doesn't require instantaneous data retrieval. This storage is regional and not tied to any specific Compute instance. See Overview of Archive Storage on page 484 for more information.

Limits on Compute Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Additional limits include:

- To attach a volume to an instance, both the instance and volume must be within the same availability domain.
- Many Compute operations are subject to throttling.

A service limit is different from host capacity. A service limit is the quota or allowance set on a resource. Host capacity is the physical infrastructure that resources such as Compute instances run on.

Metadata Key Limits

Custom metadata keys (any key you define that is not ssh_authorized_keys or user_data) have the following limits:

- Max number of metadata keys: 128
- Max size of key name: 255 characters
- Max size of key value: 255 characters

ssh_authorized_keys is a special key that does not have these limits, but its value is validated to conform to a public key in the OpenSSH format.

user_data has a maximum size of 16KB. For Linux instances with cloud-init configured, you can populate the user_data field with a Base64-encoded string of cloud-init user data. For more information on formats that cloud-init accepts, see cloud-init formats.
Best Practices for Your Compute Instance

Oracle Cloud Infrastructure Compute provides bare metal and virtual machine (VM) compute capacity that delivers performance, flexibility, and control without compromise. It's powered by Oracle’s next generation, internet-scale infrastructure, designed to help you develop and run your most demanding applications and workloads in the cloud.

You can provision compute capacity through an easy-to-use web console or the API, SDKs, or CLI. The compute instance, once provisioned, provides you with access to the host. This gives you complete control of your instance.

Though you have full management authority for your instance, we recommend a variety of best practices to ensure system availability and top performance.

IP Addresses Reserved for Use by Oracle

Certain IP addresses are reserved for Oracle Cloud Infrastructure use and may not be used in your address numbering scheme.

169.254.0.0/16

These addresses are used for iSCSI connections to the boot and block volumes, instance metadata, and other services.

Class D and Class E

All addresses from 224.0.0.0 to 239.255.255.255 (Class D) are prohibited for use in a VCN, they are reserved for multicast address assignments in the IP standards. See RFC 3171 for details.

All addresses from 240.0.0.0 to 255.255.255.255 (Class E) are prohibited for use in a VCN, they are reserved for future use in the IP standards. See RFC 1112, Section 4 for details.

Three IP Addresses in Each Subnet

These addresses consist of:

- The first IP address in the CIDR (the network address)
- The last IP address in the CIDR (the broadcast address)
- The first host address in the CIDR (the subnet default gateway address)

For example, in a subnet with CIDR 192.168.0.0/24, these addresses are reserved:

- 192.168.0.0 (the network address)
- 192.168.0.255 (the broadcast address)
- 192.168.0.1 (the subnet default gateway address)

The remaining addresses in the CIDR (192.168.0.2 to 192.168.0.254) are available for use.

Essential Firewall Rules

All Oracle-provided images include rules that allow only "root" on Linux instances or "Administrators" on Windows Server instances to make outgoing connections to the iSCSI network endpoints (169.254.0.2:3260, 169.254.2.0/24:3260) that serve the instance’s boot and block volumes.

- We recommend that you do not reconfigure the firewall on your instance to remove these rules. Removing these rules allows non-root users or non-administrators to access the instance’s boot disk volume.
- We recommend that you do not create custom images without these rules unless you understand the security risks.
• Running Uncomplicated Firewall (UFW) on Ubuntu images might cause issues with these rules. Because of this, we recommend that you do not enable UFW on your instances. See Ubuntu instance fails to reboot after enabling Uncomplicated Firewall (UFW) for more information.

System Resilience
Follow industry-wide hardware failure best practices to ensure the resilience of your solution in the event of a hardware failure. Some best practices include:
• Design your system with redundant compute nodes in different availability domains to support failover capability.
• Create a custom image of your system drive each time you change the image.
• Back up your data drives, or sync to spare drives, regularly.

If you experience a hardware failure and have followed these practices, you can terminate the failed instance, launch your custom image to create a new instance, and then apply the backup data.

Uninterrupted Access to the Instance
Make sure to keep the DHCP client running so you can always access the instance. If you stop the DHCP client manually or disable NetworkManager (which stops the DHCP client on Linux instances), the instance can't renew its DHCP lease and will become inaccessible when the lease expires (typically within 24 hours). Do not disable NetworkManager unless you use another method to ensure renewal of the lease.

Stopping the DHCP client might remove the host route table when the lease expires. Also, loss of network connectivity to your iSCSI connections might result in loss of the boot drive.

User Access
If you created your instance using an Oracle-provided Linux image, you can use SSH to access your instance from a remote host as the opc user. After logging in, you can add users on your instance.

If you do not want to share SSH keys, you can create additional SSH-enabled users.

If you created your instance using an Oracle-provided Windows image, you can access your instance using a Remote Desktop client as the opc user. After logging in, you can add users on your instance.

For more information about user access, see Adding Users on an Instance on page 737. For steps to log in to an instance, see Connecting to an Instance on page 733.

NTP Service
Oracle Cloud Infrastructure offers a fully managed, secure, and highly available NTP service that you can use to set the date and time of your Compute and Database instances from within your virtual cloud network (VCN). We recommend that you configure your instances to use the Oracle Cloud Infrastructure NTP service. For information about how to configure instances to use this service, see Configuring the Oracle Cloud Infrastructure NTP Service for an Instance on page 596.

Fault Domains
A fault domain is a grouping of hardware and infrastructure that is distinct from other fault domains in the same availability domain. Each availability domain has three fault domains. By properly leveraging fault domains you can increase the availability of applications running on Oracle Cloud Infrastructure. See Fault Domains on page 182 for more information.

Your application's architecture will determine whether you should separate or group instances using fault domains.

Scenario 1: Highly Available Application Architecture
In this scenario you have a highly available application, for example you have two web servers and a clustered database. In this scenario you should group one web server and one database node in one fault domain and the other
half of each pair in another fault domain. This ensures that a failure of any one fault domain does not result in an outage for your application.

Scenario 2: Single Web Server and Database Instance Architecture

In this scenario your application architecture is not highly available, for example you have one web server and one database instance. In this scenario both the web server and the database instance must be placed in the same fault domain. This ensures that your application will only be impacted by the failure of that single fault domain.

Customer-Managed Virtual Machine (VM) Maintenance

When an underlying infrastructure component needs to undergo maintenance, you are notified before the impact to your VM instances. During an infrastructure maintenance event, where applicable, Oracle Cloud Infrastructure live migrates Standard VM instances from the physical VM host that needs maintenance to a healthy VM host without disrupting running instances. If a VM cannot be live migrated, there might be a short downtime while the instance is reboot migrated.

You can control how and when your applications experience maintenance downtime by proactively rebooting (or stopping and starting) the instances at any time before the scheduled maintenance event. A maintenance reboot is different from a normal reboot. When you reboot an instance for maintenance, the instance is stopped on the physical VM host that needs maintenance, and then restarted on a healthy VM host.

If you choose not to reboot before the scheduled time, then Oracle Cloud Infrastructure will migrate the instances before proceeding with the planned infrastructure maintenance. Optionally, you can configure the instances to remain stopped after they are reboot migrated. For more information, see Recovering a Virtual Machine (VM) During Planned Maintenance on page 780.

Configuring the Oracle Cloud Infrastructure NTP Service for an Instance

Oracle Cloud Infrastructure offers a fully managed, secure, and highly available NTP service that you can use to set the date and time of your Compute and Database instances from within your virtual cloud network (VCN). The Oracle Cloud Infrastructure NTP service uses redundant Stratum 1 devices in every availability domain. The Stratum 1 devices are synchronized to dedicated Stratum 2 devices that every host synchronizes against. The service is available in every region.

This topic describes how to configure your Compute instances to use this NTP service.

You can also choose to configure your instances to use a public NTP service or use FastConnect to leverage an on-premises NTP service.

Note:

Oracle-provided images for Oracle Autonomous Linux 7.x, Oracle Linux 8.x, Oracle Linux 7.x, CentOS 7.x, and CentOS 8.x released after February 2018 include the Chrony service by default. You do not need to configure the Oracle Cloud Infrastructure NTP service for these instances.

Oracle Linux 6.x

Use the following steps to configure your Oracle Linux 6.x instances to use the Oracle Cloud Infrastructure NTP service.

1. Configure IPtables to allow connections to the Oracle Cloud Infrastructure NTP service, using the following commands:

```
sudo iptables -I BareMetalInstanceServices 8 -d 169.254.169.254/32 -p udp -m udp --dport 123 -m comment --comment "Allow access to OCI local NTP service" -j ACCEPT
```

```
sudo service iptables save
```
2. Install the NTP service with the following command:

   ```
sudo yum install ntp
   ```

3. Set the date of your instance with the following command:

   ```
sudo ntpdate 169.254.169.254
   ```

4. Configure the instance to use the Oracle Cloud Infrastructure NTP service for iburst. To configure, modify the `/etc/ntp.conf` file as follows:
   
a. In the `server` section, comment out the lines specifying the RHEL servers:

   ```
   #server 0.rhel.pool.ntp.org iburst
   #server 1.rhel.pool.ntp.org iburst
   #server 2.rhel.pool.ntp.org iburst
   #server 3.rhel.pool.ntp.org iburst
   ```

   b. Add an entry for the Oracle Cloud Infrastructure NTP server:

   ```
   server 169.254.169.254 iburst
   ```

   The modified `server` section now contains the following:

   ```
   # Please consider joining the pool (http://www.pool.ntp.org/join.html).
   #server 0.rhel.pool.ntp.org iburst
   #server 1.rhel.pool.ntp.org iburst
   #server 2.rhel.pool.ntp.org iburst
   #server 3.rhel.pool.ntp.org iburst
   server 169.254.169.254 iburst
   ```

5. Set the NTP service to launch automatically when the instance boots with the following command:

   ```
sudo chkconfig ntpd on
   ```

6. Start the NTP service with the following command:

   ```
sudo /etc/init.d/ntpd start
   ```

7. Confirm that the NTP service is configured correctly with the following command:

   ```
ntpq -p
   ```

   The output will be similar to the following:

   ```
remote       refid   st  t when poll reach   delay  offset  jitter
==============================================================================
169.254.169.254 192.168.32.3     2 u    2   64    1    0.338    0.278
0.187
```
2. Install the NTP service with the following command:

```
yum -y install ntp
```

3. Change the firewall rules to allow inbound and outbound traffic with the Oracle Cloud Infrastructure NTP server, at 169.254.169.254, on UDP port 123 with the following command:

```
awk -v n=13 -v s=' <passthrough ipv="ipv4">-A OUTPUT -d 169.254.169.254/32 -p udp -m udp --dport 123 -m comment --comment "Allow access to OCI local NTP service" -j ACCEPT </passthrough>' 'NR == n {print s} {print}' /etc/firewalld/direct.xml > tmp && mv tmp /etc/firewalld/direct.xml
```

At the prompt `mv: overwrite '/etc/firewalld/direct.xml'?`, enter `y`.

4. Restart the firewall with the following command:

```
service firewalld restart
```

5. Set the date of your instance with the following command:

```
ntpdate 169.254.169.254
```

6. Configure the instance to use the Oracle Cloud Infrastructure NTP service for iburst. To configure, modify the `/etc/ntp.conf` file as follows:

   a. In the `server` section comment out the lines specifying the RHEL servers:

```
#server 0.rhel.pool.ntp.org iburst
#server 1.rhel.pool.ntp.org iburst
#server 2.rhel.pool.ntp.org iburst
#server 3.rhel.pool.ntp.org iburst
```

   b. Add an entry for the Oracle Cloud Infrastructure NTP service:

```
server 169.254.169.254 iburst
```

The modified `server` section should now contain the following:

```
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.rhel.pool.ntp.org iburst
#server 1.rhel.pool.ntp.org iburst
#server 2.rhel.pool.ntp.org iburst
#server 3.rhel.pool.ntp.org iburst
server 169.254.169.254 iburst
```

7. Start and enable the NTP service with the following commands:

```
systemctl start ntpd
systemctl enable ntpd
```

You also need disable the chrony NTP client to ensure that the NTP service starts automatically after a reboot, using the following commands:

```
systemctl stop chronyd
systemctl disable chronyd
```
8. Confirm that the NTP service is configured correctly with the following command:

```
ntpq -p
```

The output will be similar to the following:

```
remote           refid      st t when poll reach delay  offset  jitter
jitter
==============================================================================
169.254.169.254 192.168.32.3     2 u    2   64    1    0.338    0.278 0.187
```

Windows Server 2012 R2 and later versions

You can configure your Windows Server instances to use the Oracle Cloud Infrastructure NTP service by running the following commands in Windows Powershell as Administrator.

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\Parameters' -Name 'Type' -Value NTP -Type String
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\Config' -Name 'AnnounceFlags' -Value 5 -Type DWord
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer' -Name 'Enabled' -Value 1 -Type DWord
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\Parameters' -Name 'NtpServer' -Value '169.254.169.254,0x9' -Type String
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient' -Name 'SpecialPollInterval' -Value 900 -Type DWord
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\Config' -Name 'MaxPosPhaseCorrection' -Value 1800 -Type DWord
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\W32Time\Config' -Name 'MaxNegPhaseCorrection' -Value 1800 -Type DWord
```

Steps 1 - 7 below walk you though these registry changes, you can use these steps to manually edit the registry instead of using PowerShell. If you use the PowerShell commands, you can skip steps 1 - 7, and proceed with steps 8 and 9 to complete the process of configuring your Windows instance to use the Oracle Cloud Infrastructure NTP service.

1. Change the server type to NTP:
   a. From Registry Editor, navigate to:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type
   ```
   
   b. Click Type.
   
   c. Change the value to NTP and click OK.

2. Configure the Windows Time service to enable the Timeserv_Announce_Yes and Reliable_Timeserv_Announce_Auto flags.
   To configure, set the AnnounceFlags parameter to 5:
   a. From Registry Editor, navigate to:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags
   ```
   
   b. Click AnnounceFlags.
   
   c. Change the value to 5 and click OK.
3. Enable the NTP server:
   a. From Registry Editor, navigate to:
      ```
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\
      \TimeProviders\NtpServer\
      ```
   b. Click **Enabled**.
   c. Change the value to 1 and click **OK**.

4. Set the time sources:
   a. From Registry Editor, navigate to:
      ```
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
      ```
   b. Click **NtpServer**.
   c. Change the value to 169.254.169.254,0x9 and click **OK**.

5. Set the poll interval:
   a. From Registry Editor, navigate to:
      ```
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\
      \TimeProviders\NtpClient\
      ```
   b. Click **SpecialPollInterval**.
   c. Set the value to the interval that you want the time service to synchronize on. The value is in seconds. To set it for 15 minutes, set the value to 900, and click **OK**.

6. Set the phase correction limit settings to restrict the time sample boundaries:
   a. From Registry Editor, navigate to:
      ```
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\
      ```
   b. Click **MaxPosPhaseCorrection**.
   c. Set the value to the maximum time offset in the future for time samples. The value is in seconds. To set it for 30 minutes, set the value to 1800 and click **OK**.
   d. Click **MaxNegPhaseCorrection**.
   e. Set the value to the maximum time offset in the past for time samples. The value is in seconds. To set it for 30 minutes, set the value to 1800 and click **OK**.

7. Restart the time service by running the following command from a command prompt:
   ```
   net stop w32time && net start w32time
   ```

8. Test the connection to the NTP service by running the following command from a command prompt:
   ```
   w32tm /query /peers
   ```
   The output will be similar to the following:
   ```
   #Peer: 1
   Peer: 169.254.169.254,0x9
   State: Active
   Time Remaining: 22.1901786s
   Mode: 3 (Client)
   Stratum: 0 (unspecified)
   PeerPoll Interval: 10 (1024s)
   HostPoll Interval: 10 (1024s)
   ```
   After the time specified in the poll interval has elapsed, **State** will change from **Pending** to **Active**.
Protecting Data on NVMe Devices

Some instance shapes in Oracle Cloud Infrastructure include locally attached NVMe devices. These devices provide extremely low latency, high performance block storage that is ideal for big data, OLTP, and any other workload that can benefit from high-performance block storage.

Note that these devices are not protected in any way; they are individual devices locally installed on your instance. Oracle Cloud Infrastructure does not take images, back up, or use RAID or any other methods to protect the data on NVMe devices. It is your responsibility to protect and manage the durability of the data on these devices.

Oracle Cloud Infrastructure offers high-performance remote block (iSCSI) LUNs that are redundant and can be backed up using an API call. See Overview of Block Volume on page 500 for more information.

See Compute Shapes on page 655 for information about which shapes support local NVMe storage.

Finding the NVMe devices on your instance

You can identify the NVMe devices by using the lsblk command. The response returns a list. NVMe devices begin with "nvme", as shown in the following example for a BM.DenseIO1.36 instance:

```
[root@somehost ~]# lsblk
NAME    MAJ:MIN  RM  SIZE     RO TYPE MOUNTPOINT
sda       8:0    0  46.6G    0 disk
##sda1    8:1    0  512M     0 part /boot/efi
##sda2    8:2    0   8G      0 part [SWAP]
##sda3    8:3    0   38G     0 part /
nvme0n1  259:6    0  2.9T    0 disk
nvme1n1  259:8    0  2.9T    0 disk
nvme2n1  259:0    0  2.9T    0 disk
nvme3n1  259:1    0  2.9T    0 disk
nvme4n1  259:7    0  2.9T    0 disk
nvme5n1  259:4    0  2.9T    0 disk
nvme6n1  259:5    0  2.9T    0 disk
nvme7n1  259:2    0  2.9T    0 disk
nvme8n1  259:3    0  2.9T    0 disk
```

Failure Modes and How to Protect Against Them

There are three primary failure modes you should plan for:

- Protecting Against the Failure of an NVMe Device on page 601
- Protecting Against the Loss of the Instance or Availability Domain on page 609
- Protecting Against Data Corruption or Loss from Application or User Error on page 609

Protecting Against the Failure of an NVMe Device

A protected RAID array is the most recommended way to protect against an NVMe device failure. There are three RAID levels that can be used for the majority of workloads:
- RAID 1: An exact copy (or mirror) of a set of data on two or more disks; a classic RAID 1 mirrored pair contains two disks, as shown:
- RAID 10: Stripes data across multiple mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved, as shown:

Blocks mirrored and striped
• RAID 6: Block-level striping with two parity blocks distributed across all member disks, as shown.

**RAID 6**

For more information about RAID and RAID levels, see [RAID](#).

Because the appropriate RAID level is a function of the number of available drives, the number of individual LUNs needed, the amount of space needed, and the performance requirements, there isn't one correct choice. You must understand your workload and design accordingly.

**Important:**

If you're partitioning or formatting your disk as part of this process and the drive is larger than 2 TB, you should create a GUID Partition Table (GPT).

If you want to create a GPT, use `parted` instead of the `fdisk` command.

For more information, see [About Disk Partitions](#) in the Oracle Linux Administrator's Guide.

---

**Options for Using a BM.DenseIO1.36 Shape**

There are several options for BM.DenseIO1.36 instances with nine NVMe devices.

For all options below, you can optionally increase the default RAID resync speed limit value. Increasing this value to more closely match the fast storage speed on the bare metal instances can decrease the amount of time required to set up RAID.

Use the following command to increase the speed limit value:

```
$ sysctl -w dev.raid.speed_limit_max=10000000
```

**Option 1: Create a single RAID 6 device across all nine devices**

This array is redundant, performs well, will survive the failure of any two devices, and will be exposed as a single LUN with about 23.8TB of usable space.
Use the following commands to create a single RAID 6 device across all nine devices:

$ sudo yum install mdadm -y

$ sudo mdadm --create /dev/md0 --raid-devices=9 --level=6 /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1 /dev/nvme4n1 /dev/nvme5n1 /dev/nvme6n1 /dev/nvme7n1 /dev/nvme8n1

$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf >> /dev/null

Option 2: Create a four device RAID 10 and a five device RAID 6 array

These arrays would be exposed as two different LUNs to your applications. This is a recommended choice when you need to isolate one type of I/O from another, such as log and data files. In this example, your RAID 10 array would have about 6.4TB of usable space and the RAID 6 array would have about 9.6TB of usable space.

Use the following commands to create a four-device RAID 10 and a five-device RAID 6 array:

$ sudo yum install mdadm -y

$ sudo mdadm --create /dev/md0 --raid-devices=4 --level=10 /dev/nvme5n1 /dev/nvme6n1 /dev/nvme7n1 /dev/nvme8n1

$ sudo mdadm --create /dev/md1 --raid-devices=5 --level=6 /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1 /dev/nvme4n1

$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf >> /dev/null

Option 3: Create an eight-device RAID 10 array

If you need the best possible performance and can sacrifice some of your available space, then an eight-device RAID 10 array is an option. Because RAID 10 requires an even number of devices, the ninth device is left out of the array and serves as a hot spare in case another device fails. This creates a single LUN with about 12.8 TB of usable space.

Use the following commands to create an eight-device RAID 10 array:

$ sudo yum install mdadm -y

$ sudo mdadm --create /dev/md0 --raid-devices=8 --level=10 /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1 /dev/nvme4n1 /dev/nvme5n1 /dev/nvme6n1 /dev/nvme7n1

The following command adds /dev/nvme8n as a hot spare for the /dev/md0 array:

$ sudo mdadm /dev/md0 --add /dev/nvme8n1

$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf >> /dev/null

Option 4: Create two four-device RAID 10 arrays

For the best possible performance and I/O isolation across LUNs, create two four-device RAID 10 arrays. Because RAID 10 requires an even number of devices, the ninth device is left out of the arrays and serves as a global hot spare in case another device in either array fails. This creates two LUNS, each with about 6.4 TB of usable space.
Compute

Use the following commands to create two four-device RAID 10 arrays with a global hot spare:

```bash
$ sudo yum install mdadm -y

$ sudo mdadm --create /dev/md0 --raid-devices=4 --level=10 /dev/nvme4n1 /dev/nvme5n1 /dev/nvme6n1 /dev/nvme7n1

$ sudo mdadm --create /dev/md1 --raid-devices=4 --level=10 /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1
```

Creating a global hot spare requires the following two steps:

1. Add the spare to either array (it does not matter which one) by running these commands:

   ```bash
   $ sudo mdadm /dev/md0 --add /dev/nvme8n1
   $ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf >> /dev/null
   ```

2. Edit `/etc/mdadm` to put both arrays in the same spare-group. Add `spare-group=global` to the end of the line that starts with `ARRAY`, as follows:

   ```bash
   $ sudo vi /etc/mdadm.conf
   ```

   ```bash
   ARRAY /dev/md0 metadata=1.2 spares=1 name=mdadm.localdomain:0
   UUID=43f93ce6:4a19d07b:51762f1b:250e2327 spare-group=global

   ARRAY /dev/md1 metadata=1.2 name=mdadm.localdomain:1
   UUID=7521e51a:83999f00:99459a19:0c836693 spare-group=global
   ```

### Monitoring Your Array

It's important for you to be notified if a device in one of your arrays fails. Mdadm has built-in tools that can be utilized for monitoring, and there are two options you can use:

- Set the `MAILADDR` option in `/etc/mdadm.conf` and then run the `mdadm` monitor as a daemon
- Run an external script when `mdadm` detects a failure

#### Set the MAILADDR option in `/etc/mdadm.conf` and run the `mdadm` monitor as a daemon

The simplest method is to set the `MAILADDR` option in `/etc/mdadm.conf`, and then run the `mdadm` monitor as a daemon, as follows:

1. The `DEVICE partitions` line is required for `MAILADDR` to work; if it is missing, you must add it, as follows:

   ```bash
   $ sudo vi /etc/mdadm.conf
   ```

   ```bash
   DEVICE partitions
   ```

   ```bash
   ARRAY /dev/md0 level=raid1 UUID=1b70e34a:2930b5a6:016we78d:eese14532
   ```

   ```bash
   MAILADDR <my.name@example.com>
   ```

2. Run the monitor using the following command:

   ```bash
   $ sudo nohup mdadm --monitor --scan --daemonize &
   ```
3. To verify that the monitor runs at startup, run the following commands:

```bash
$ sudo chmod +x /etc/rc.d/rc.local
$ sudo vi /etc/rc.local
```

Add the following line to the end of `/etc/rc.local`:

```
nohup mdadm --monitor --scan --daemonize &
```

4. To verify that the email and monitor are both working run the following command:

```bash
$ sudo mdadm --monitor --scan --test -1
```

Note that these emails will likely be marked as spam. The `PROGRAM` option, described later in this topic, allows for more sophisticated alerting and messaging.

**Run an external script when a failure is detected**

A more advanced option is to create an external script that would run if the `mdadm` monitor detects a failure. You would integrate this type of script with your existing monitoring solution. The following is an example of this type of script:

```bash
#!/bin/bash
event=$1
device=$2
if [ $event == "Fail" ]
    then
        <"do something">
    else
        if [ $event == "FailSpare" ]
            then
                <"do something else">
        else
            if [ $event == "DegradedArray" ]
                then
                    <"do something else else">
            else
                if [ $event == "TestMessage" ]
                    then
                        <"do something else else else">
                fi
        fi
    fi
$ sudo chmod +x /etc/mdadm.events
```

Next, add the `PROGRAM` option to `/etc/mdadm.conf`, as shown in the following example:
1. The DEVICE partitions line is required for MAILADDR to work; if it is missing, you must add it, as follows:

```
$ sudo vi /etc/mdadm.conf
```

```
DEVICE partitions
```

```
ARRAY /dev/md0 level=raid1 UUID=1b70e34a:2930b5a6:016we78d:eese14532
MAILADDR <my.name@example.com>
```

```
PROGRAM /etc/mdadm.events
```

2. Run the monitor using the following command:

```
$ sudo nohup mdadm --monitor --scan --daemonize &
```

3. To verify that the monitor runs at startup, run the following commands:

```
$ sudo chmod +x /etc/rc.d/rc.local
$ sudo vi /etc/rc.local
```

Add the following line to the end of /etc/rc.local:

```
nohup mdadm --monitor --scan --daemonize &
```

4. To verify that the email and monitor are both working run the following command:

```
$ sudo mdadm --monitor --scan --test -1
```

Note that these emails will likely be marked as spam. The PROGRAM option, described later in this topic, allows for more sophisticated alerting and messaging.

**Simulate the failure of a device**

You can use mdadm to manually cause a failure of a device to see whether your RAID array can survive the failure, as well as test the alerts you have set up.

1. Mark a device in the array as failed by running the following command:

```
$ sudo mdadm /dev/md0 --fail /dev/nvme0n1
```

2. Recover the device or your array might not be protected. Use the following command:

```
$ sudo mdadm /dev/md0 --add /dev/nvme0n1
```

Your array will automatically rebuild in order to use the "new" device. Performance will be decreased during this process.

3. You can monitor the rebuild status by running the following command:

```
$ sudo mdadm --detail /dev/md0
```

**What To Do When an NVMe Device Fails**

Compute resources in the cloud are designed to be temporary and fungible. If an NVMe device fails while the instance is in service, you should start another instance with the same amount of storage or more, and then copy the data onto the new instance, replacing the old instance. There are multiple toolsets for copying large amounts of data, with rsync being the most popular. Since the connectivity between instances is a full 10 Gb/sec, copying data should
be quick. Remember that with a failed device, your array may no longer be protected, so you should copy the data off of the impacted instance as quickly as possible.

**Using the Linux Logical Volume Manager**

The Linux Logical Volume Manager (LVM) provides a rich set of features for managing volumes. If you need these features, we strongly recommend that you use `mdadm` as described in preceding sections of this topic to create the RAID arrays, and then use LVM's `pvcreate`, `vgcreate`, and `lvcreate` commands to create volumes on the `mdadm` LUNs. You should not use LVM directly against your NVMe devices.

**Protecting Against the Loss of the Instance or Availability Domain**

Once your data is protected against the loss of a NVMe device, you need to protect it against the loss of an instance or the loss of the availability domain. This type of protection is typically done by replicating your data to another availability domain or backing up your data to another location. The method you choose depends on your objectives. For details, see the disaster recovery concepts of Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

**Replication**

Replicating your data from one instance in one availability domain to another has the lowest RTO and RPO at a significantly higher cost than backups; for every instance in one availability domain, you must have another instance in a different availability domain.

For Oracle database workloads, you should use the built-in Oracle Data Guard functionality to replicate your databases. Oracle Cloud Infrastructure availability domains are each close enough to each other to support high performance, synchronous replication. Asynchronous replication is also an option.

For general-purpose block replication, DRBD is the recommended option. You can configure DRBD to replicate, synchronously or asynchronously, every write in one availability domain to another availability domain.

**Backups**

Traditional backups are another way to protect data. All commercial backup products are fully supported on Oracle Cloud Infrastructure. If you use backups, the RTO and RPO are significantly higher than using replication because you must recreate the compute resources that failed and then restore the most recent backup. Costs are significantly lower because you don't need to maintain a second instance. Do not store your backups in the same availability domain as their original instance.

**Protecting Against Data Corruption or Loss from Application or User Error**

The two recommended ways of protecting against data corruption or loss from application or user error are regularly taking snapshots or creating backups.

**Snapshots**

The two easiest ways to maintain snapshots are to either use a file system that supports snapshots, such as ZFS, or use LVM to create and manage the snapshots. Because of the way LVM has implemented copy-on-write (COW), performance may significantly decrease when a snapshot is taken using LVM.

**Backups**

All commercial backup products are fully supported on Oracle Cloud Infrastructure. Make sure that your backups are stored in a different availability domain from the original instance.

**Boot Volumes**

When you launch a virtual machine (VM) or bare metal instance based on an Oracle-provided image or custom image, a new boot volume for the instance is created in the same compartment. That boot volume is associated with that instance until you terminate the instance. When you terminate the instance, you can preserve the boot volume and
Compute its data. For more information, see Terminating an Instance on page 783. This feature gives you more control and management options for your compute instance boot volumes, and enables:

- **Instance scaling**: When you terminate your instance, you can keep the associated boot volume and use it to launch a new instance using a different instance type or shape. See Creating an Instance on page 695 for steps to launch an instance based on a boot volume. This allows you to switch easily from a bare metal instance to a VM instance and vice versa, or scale up or down the number of cores for an instance.

- **Troubleshooting and repair**: If you think a boot volume issue is causing a compute instance problem, you can stop the instance and detach the boot volume. Then you can attach it to another instance as a data volume to troubleshoot it. After resolving the issue, you can then reattach it to the original instance or use it to launch a new instance.

Boot volumes are encrypted by default, the same as other block storage volumes. For more information, see Block Volume Encryption on page 504.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-transit encryption for boot and block volumes is only available for virtual machine (VM) instances launched from Oracle-provided images, it is not supported on bare metal instances. It is also not supported in most cases for instances launched from custom images imported for &quot;bring your own image&quot; (BYOI) scenarios. To confirm support for certain Linux-based custom images and for more information contact Oracle support, see Getting Help and Contacting Support on page 125.</td>
</tr>
</tbody>
</table>

You can group boot volumes with block volumes into the same volume group, making it easy to create a group volume backup or a clone of your entire instance, including both the system disk and storage disks at the same time. See Volume Groups on page 506 for more information.

You can move Block Volume resources such as boot volumes and boot volume backups between compartments. For more information, see Move Block Volume Resources Between Compartments on page 564.

For more information about the Block Volume service and boot volumes, see the Block Volume FAQ.

**Custom Boot Volume Sizes**

When you launch an instance, you can choose whether to use the selected image's default boot volume size, or to specify a custom size up to 32 TB. This capability is available for the following image source options:

- Oracle-provided image
- Custom image
- Image OCID

See Creating an Instance on page 695 for more information.

For Linux-based images, the custom boot volume size must be larger than the image's default boot volume size or 50 GB, whichever is higher.

For Windows-based images, the custom boot volume size must be larger than the image's default boot volume size or 256 GB, whichever is higher. The minimum size requirement for Windows images is to ensure that there is enough space available for Windows patches and updates that can require a large amount of space, to improve performance, and to provide adequate space for setting a suitable page file (see this Microsoft known issue for page file settings on Windows Server 2012 R2).

After you launch an instance, you can't change the boot volume size.

If you specify a custom boot volume size, you need to extend the volume to take advantage of the larger size. For steps, see Extending the Partition for a Boot Volume on page 612.
**Boot Volume Performance**

Boot volume performance varies with volume size, see Block Volume Performance on page 567 for more information.

The Block Volume service's elastic performance feature enables you to dynamically change the volume performance for boot volumes. Once an instance has been created, you can change the volume performance of the boot volume to one of the following performance options:

- Balanced
- Higher Performance

For more information about this feature and the performance options, see Block Volume Elastic Performance on page 581 and Changing the Performance of a Volume on page 582

**Required IAM Service Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to list boot volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes, boot volumes, and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Using the Console**

To access the Console, you must use a supported browser.

See the following tasks for managing boot volumes:

- Listing Boot Volumes on page 614
- Attaching a Boot Volume on page 613
- Detaching a Boot Volume on page 623
- Listing Boot Volume Attachments on page 615
- Deleting a Boot Volume on page 624

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage boot volumes:

- BootVolume
- ListBootVolumes
- GetBootVolume
- UpdateBootVolume
- DetachBootVolume
- DeleteVolume
- BootVolumeAttachment
- AttachBootVolume
- GetBootVolumeAttachment
- ListBootVolumeAttachments
Extending the Partition for a Boot Volume

When you create a new virtual machine (VM) instance or bare metal instance based on an Oracle-provided image or custom image, you have the option of specifying a custom boot volume size. You can also expand the size of the boot volume for an existing instance; see Resizing a Volume on page 532 for more information. In order to take advantage of the larger size, you need to extend the partition for the boot volume. For block volumes, see Extending the Partition for a Block Volume on page 536.

Note:

After a boot volume has been resized, the first backup on the resized boot volume will be a full backup. See Boot Volume Backup Types on page 615 for more information about full versus incremental boot volume backups.

Required IAM Policy

Extending a partition on an instance does not require a specific IAM policy. However, you may need permission to run the necessary commands on the instance's guest OS. Contact your system administrator for more information.

Extending the Root Partition on a Linux-Based Image

For instances running Linux-based images, you need to extend the root partition and then grow the file system using the `oci-growfs` operation from OCI Utilities on page 642.

Extending the System Partition on a Windows-Based Image

On Windows-based images, you can extend a partition using the Windows interface or from the command line using the DISKPART utility.

Windows Server 2012 and Later Versions

The steps for extending a system partition on instances running Windows Server 2012, Windows Server 2016, or Windows Server 2019 are the same, and are described in the following procedures.

Extending the system partition using the Windows interface

1. Open the Disk Management system utility on the instance.
2. Right-click the boot volume and select Extend Volume.
3. Follow the instructions in the Extend Volume Wizard:
   a. Select the disk that you want to extend, enter the size, and then click Next.
   b. Confirm that the disk and size settings are correct, and then click Finish.
4. Verify that the boot volume's system disk has been extended in Disk Management.

Extending the system partition using the command line with DISKPART

1. Open a command prompt as administrator on the instance.
2. Run the following command to start the DISKPART utility:

```
diskpart
```

3. At the DISKPART prompt, run the following command to display the instance's volumes:

```
list volume
```

4. Run the following command to select the boot volume:

```
select volume <volume_number>
```

<volume_number> is the number associated with the boot volume that you want to extend the partition for.

5. Run the following command to extend the partition:

```
extend size=<increased_size_in_MB>
```

<increased_size_in_MB> is the size in MB that you want to extend the partition to.

**Caution:**
When using the DISKPART utility, do not overextend the partition beyond the current available space. Overextending the partition could result in data loss.

6. To confirm that the partition was extended, run the following command and verify that the boot volume's partition has been extended:

```
list volume
```

### Attaching a Boot Volume

If a boot volume has been detached from the associated instance, you can reattach it to the instance. If you want to restart an instance with a detached boot volume, you must reattach the boot volume using the steps described in this topic.

If a boot volume has been detached from the associated instance, or if the instance is stopped or terminated, you can attach the boot volume to another instance as a data volume. For steps, see [Attaching a Volume](#) on page 517.

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in [Let users launch compute instances](#) on page 2143 includes the ability to attach and detach existing block volumes. The policy in [Let volume admins manage block volumes, backups, and volume groups](#) on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see [Details for the Core Services](#) on page 2181.

### Security Zones

Security Zones ensure that your cloud resources comply with Oracle security principles. If any operation on a resource in a security zone compartment violates a policy for that security zone, then the operation is denied.

The following security zone policies affect your ability to attach block volumes to Compute instances:

- The boot volume for a Compute instance in a security zone must also be in a security zone.
- A Compute instance that isn't in a security zone can't be attached to a boot volume that is in a security zone.
Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you want to reattach the boot volume to.
4. Click the Actions icon (three dots), and then click Attach Boot Volume. Confirm when prompted.

   You can start the instance when the boot volume’s state is Attached.

Using the API

To attach a volume to an instance, use the following operation:

- AttachBootVolume

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Listing Boot Volumes

You can list all boot volumes in a specific compartment, or detailed information on a single boot volume.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to list volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Boot Volumes.
2. Choose your Compartment.

   A detailed list of volumes in the current compartment is displayed. To see detailed information for a specific volume, click the boot volume name.

   The instance associated with the boot volume is listed in the Attached Instance field. If the value for this field displays the message None in this Compartment, the boot volume has been detached from the associated instance, or the instance has been terminated while the boot volume was preserved.

   To view the volumes in a different compartment, change the compartment in the Compartment drop-down menu.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

List Boot Volumes:

Get a list of boot volumes within a compartment.

- ListBootVolumes

Get a Single Boot Volume:

Get detailed information on a single boot volume:
Listing Boot Volume Attachments

You can use the API to list all the boot volume attachments in a specific compartment. You can also use the API to retrieve detailed information on a single boot volume attachment.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to list volume attachments. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

List Boot Volume Attachments:

Get information on all boot volume attachments in a specific compartment.

- ListBootVolumeAttachments

Get a Single Boot Volume Attachment:

Get detailed information on a single boot volume attachment.

- GetBootVolumeAttachment

Overview of Boot Volume Backups

The backups feature of the Oracle Cloud Infrastructure Block Volume service lets you make a crash-consistent backup, which is a point in time snapshot of a boot volume without application interruption or downtime. You can make a backup of a boot volume while it is attached to a running instance, or you can make a backup of a boot volume while it is detached from the instance. Boot volume backup capabilities are the same as block volume backup capabilities. See Overview of Block Volume Backups on page 540 for more information.

There are two ways you can initiate a boot volume backup, the same as block volume backups. You can either manually start the backup, or assign a policy which defines a set backup schedule. See Manual Backups on page 540 and Policy-Based Backups on page 540 for more information.

Boot Volume Backup Types

The Block Volume service supports the same backups types for boot volumes as for block volumes:

- **Incremental**: This backup type includes only the changes since the last backup.
- **Full**: This backup type includes all changes since the volume was created.

You can restore a boot volume from any of your incremental or full boot volume backups. Both backup types enable you to restore the full boot volume contents to the point-in-time snapshot of the boot volume when the backup was taken. You don't need to keep the initial full backup or subsequent incremental backups in the backup chain and restore them in sequence, you only need to keep the backups taken for the times you care about.
Note:

After a boot volume has been resized, the first backup on the resized boot volume will be a full backup. See Resizing a Volume on page 532 for more information about volume resizing.

Tags

When a boot volume backup is created, the source boot volume’s tags are automatically included in the boot volume backup. This also includes boot volumes with custom backup policies applied to create backups on a schedule. Source boot volume tags are automatically assigned to all backups when they are created. You can also apply additional tags to volume backups as needed.

When you create an instance from the boot volume backup, the instance is created includes the source boot volume’s tags.

Backing Up a Boot Volume

You can create boot volume backups using the Console or the REST APIs/command line interface (CLI). See Backing Up a Boot Volume on page 617 and the BootVolumeBackup API for more information.

Boot Volume Backup Size

Boot volume backup size may be larger than the source boot volume size. Some of the reasons for this could include the following:

- Any part of the boot volume that has been written to is considered initialized, so will always be part of the boot volume backup.
- Many operating systems write or zero out the content, which results in these blocks marked as used. The Block Volume service considers these blocks updated and includes them in the volume backup.
- Boot volume backups also include metadata, which can be up to 1 GB in additional data. For example, in a full backup of a 256 GB Windows boot disk, you may see a backup size of 257 GB, which includes an additional 1 GB of metadata.

Restoring a Boot Volume

Before you can use a boot volume backup, you need to restore it. For steps, see Restoring a Boot Volume on page 618.

Making a boot volume backup while an instance is running creates a crash-consistent backup, meaning the data is in the identical state it was in at the time the backup was made. This is the same state it would be in the case of a loss of power or hard crash. In most cases, you can restore a boot volume backup and use it to create an instance. Alternatively, you can attach it to an instance as a data volume to repair it or recover data, see Attaching a Volume on page 517. To ensure a bootable image, you should create a custom image from your instance. For information about creating custom images, see Managing Custom Images on page 665.

Copying Boot Volume Backups Across Regions

You can copy boot volume backups between regions using the Console, command line interface (CLI), SDKs, or REST APIs. For steps, see Copying a Boot Volume Backup Between Regions on page 619. This capability enhances the following scenarios:

- **Disaster recovery and business continuity:** By copying boot volume backups to another region at regular intervals, it makes it easier for you to restore instances in the destination region if a region-wide disaster occurs in the source region.
- **Migration and expansion:** You can easily migrate and expand your instances to another region.

To copy boot volume backups between regions, you must have permission to read and copy boot volume backups in the source region, and permission to create boot volume backups in the destination region. For more information see Required IAM Policy on page 620.

Once you have copied the boot volume backup to the new region you can then restore from that backup by creating a new volume from the backup using the steps described in Restoring a Boot Volume on page 618.
Differences Between Boot Volume Backups and Clones

Consider the following criteria when you decide whether to create a backup or a clone of a volume.

<table>
<thead>
<tr>
<th></th>
<th>Volume Backup</th>
<th>Volume Clone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Creates a point-in-time backup of data on a volume. You can restore multiple new volumes from the backup later in the future.</td>
<td>Creates a single point-in-time copy of a volume without having to go through the backup and restore process.</td>
</tr>
<tr>
<td><strong>Use case</strong></td>
<td>Retain a backup of the data in a volume, so that you can duplicate an environment later or preserve the data for future use. Meet compliance and regulatory requirements, because the data in a backup remains unchanged over time. Support business continuity requirements. Reduce the risk of outages or data mutation over time.</td>
<td>Rapidly duplicate an existing environment. For example, you can use a clone to test configuration changes without impacting your production environment.</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Slower (minutes or hours)</td>
<td>Faster (seconds)</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Lower cost</td>
<td>Higher cost</td>
</tr>
<tr>
<td><strong>Storage location</strong></td>
<td>Object Storage</td>
<td>Block Volume</td>
</tr>
<tr>
<td><strong>Retention policy</strong></td>
<td>Policy-based backups expire, manual backups do not expire</td>
<td>No expiration</td>
</tr>
<tr>
<td><strong>Volume groups</strong></td>
<td>Supported. You can back up a volume group.</td>
<td>Supported. You can clone a volume group.</td>
</tr>
</tbody>
</table>

Backing Up a Boot Volume

You can create a backup of a boot volume using the Oracle Cloud Infrastructure Block Volume service. Boot volume backups are point-in-time snapshots of a boot volume. For more information about boot volume backups, see Overview of Boot Volume Backups on page 615. This topic describes how to create a manual boot volume backup.

You can also configure a backup policy that creates backups automatically based on a specified schedule and retention policy. This works the same as block volumes. See Policy-Based Backups on page 547 for more information.

For information to help you decide whether to create a backup or a clone of a boot volume, see Differences Between Boot Volume Backups and Clones on page 617.

**Note:**

Boot volume backup size may be larger than the source boot volume size. See Boot Volume Backup Size on page 616 for more information. See also Boot volume backup size larger than expected.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.
When users create a backup from a volume or restore a volume from a backup, the volume and backup don't have to be in the same compartment. However, users must have access to both compartments.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Boot Volumes.
2. Click the boot volume that you want to create a backup for.
3. Click Create Manual Backup.
4. Enter a name for the backup. Avoid entering confidential information.
5. Select the backup type, either incremental or full. See Boot Volume Backup Types on page 615 for information about backup types.
6. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click Create Backup.

The backup is completed when its icon no longer lists it as CREATING in the Boot Volume Backup list.

Using the API

To back up a boot volume, use the following operation:

- CreateBootVolumeBackup

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For more information about backups, see Overview of Block Volume Backups on page 540 and Restoring a Backup to a New Volume on page 557.

Restoring a Boot Volume

You can use a boot volume backup to create an instance or you can attach it to another instance as a data volume. However before you can use a boot volume backup, you need to restore it to a boot volume.

You can restore a boot volume from any of your incremental or full boot volume backups. Both backup types enable you to restore the full boot volume contents to the point-in-time snapshot of the boot volume when the backup was taken. You don't need to keep the initial full backup or subsequent incremental backups in the backup chain and restore them in sequence, you only need to keep the backups taken for the times you care about. See Boot Volume Backup Types on page 615 for information about full and incremental backup types.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Boot Volume Backups.
2. Choose your Compartment.
3. In the list of boot volume backups, click the Actions icon (three dots) for the boot volume backup you want to restore and then click **Create Boot Volume**.

4. Specify a name for the boot volume, select the availability domain to use, and optionally choose a backup policy for scheduled backups. See **Policy-Based Backups** on page 547 for more information about scheduled backups and volume backup policies. Avoid entering confidential information.

5. You can restore a boot volume backup to a larger volume size. To do this, check **Custom Block Volume Size (GB)** and then specify the new size. You can only increase the size of the volume, you cannot decrease the size. If you restore the block volume backup to a larger size volume, you need to extend the volume's partition, see **Extending the Partition for a Boot Volume** on page 612 for more information.

6. Click **Create Boot Volume**.

   The boot volume will be ready to use once its icon no longer lists it as **PROVISIONING** in the details page for the boot volume.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

To restore a boot volume backup, use the **CreateBootVolume** operation and specify **BootVolumeSourceFromBootVolumeBackupDetails** for **CreateBootVolumeDetails**.

**Next Steps**

After you have restored the boot volume backup, you can:

- Use the boot volume to create an instance, for more information, see **Creating an Instance** on page 695.
- Attach the boot volume to an instance as a data volume, for more information, see **Attaching a Volume** on page 517.

Making a boot volume backup while an instance is running creates a crash-consistent backup, meaning the data is in the identical state it was in at the time the backup was made. This is the same state it would be in the case of a loss of power or hard crash. In most cases you can use the restored boot volume to create an instance, however to ensure a bootable image, you should create a custom image from your instance. For information about creating custom images, see **Managing Custom Images** on page 665.

**Copying a Boot Volume Backup Between Regions**

You can copy boot volume backups from one region to another region using the Oracle Cloud Infrastructure Block Volume service. For more information, see **Copying Boot Volume Backups Across Regions** on page 616.

**Note:**

Limitations for Copying Boot Volume Backups Across Regions

When copying boot volume backups across regions in your tenancy, you can only copy one backup at a time from a specific source region.

You can only copy boot volume backups for instances based on **Oracle-Provided Images** on page 629. If you try to copy a boot volume for an instance based on other image types, such as Marketplace images, the request will fail with an error.

You cannot add compatible shapes in the destination region for boot volume backups, the shape compatibility list is from the source region and cannot be changed.

When you create an instance from the Console and specify a boot volume backup that was copied from another region as the image source, you may encounter a message indicating that there was an error loading the source image. You can ignore this error message and click **Create Instance** to finish the instance creation process and launch the instance.
**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

For administrators: The first two statements listed in the *Let volume admins manage block volumes, backups, and volume groups* on page 2146 policy lets the specified group do everything with boot volumes and boot volume backups with the exception of copying boot volume backups across regions. The aggregate resource type *volume-family* does not include the *BOOT_VOLUME_BACKUP_COPY* permission, so to enable copying boot volume backups across regions you need to ensure that you include the third statement in that policy, which is:

```
Allow group VolumeAdmins to use boot-volume-backups in tenancy where request.permission='BOOT_VOLUME_BACKUP_COPY'
```

To restrict access to just creating and managing boot volume backups, including copying boot volume backups between regions, use the policy in *Let boot volume backup admins manage only backups* on page 2147. The individual resource type *boot-volume-backups* includes the *BOOT_VOLUME_BACKUP_COPY* permission, so you do not need to specify it explicitly in this policy.

If you are copying volume backups encrypted using Vault between regions or you want the copied volume backup to use Vault for encryption in the destination region, you need to use a policy that allows the Block Volume service to perform cryptographic operations with keys in the destination region. For a sample policy showing this, see *Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools* on page 2153.

** Restricting Access **

The specific permissions needed to copy volume backups across regions are:

- **Source region**: *BOOT_VOLUME_BACKUP_READ*, *BOOT_VOLUME_BACKUP_COPY*
- **Destination region**: *BOOT_VOLUME_BACKUP_CREATE*

**Sample Policies**

To restrict a group to specific source and destination regions for copying volume backups

In this example, the group is restricted to copying volume backups from the UK South (London) region to the Germany Central (Frankfurt) region.

```
Allow group MyTestGroup to read boot-volume-backups in tenancy where all {request.region='lhr'}
Allow group MyTestGroup to use boot-volume-backups in tenancy where all {request.permission='BOOT_VOLUME_BACKUP_COPY', request.region = 'lhr',}
Allow group MyTestGroup to manage boot-volume-backups in tenancy where all {request.permission='BOOT_VOLUME_BACKUP_CREATE', request.region = 'fra'}
```

To restrict some source regions to specific destination regions while enabling all destination regions for other source regions

In this example, the following is enabled for the group:

- Manage volume backups in all regions.
- Copy volume backups from the US West (Phoenix) and US East (Ashburn) regions to any destination regions.
- Copy volume backups from the Germany Central (Frankfurt) and UK South (London) regions only to the Germany Central (Frankfurt) or UK South (London) regions.

```
Allow group MyTestGroup to read boot-volume-backups in tenancy where all {request.region='lhr'}
Allow group MyTestGroup to manage boot-volume-backups in tenancy where any {request.permission!='BOOT_VOLUME_BACKUP_COPY'}
```
Allow group MyTestGroup to use boot-volume-backups in tenancy where all
{request.permission='BOOT_VOLUME_BACKUP_COPY', any {request.region='lhr',
request.region='fra'}, any{target.region='fra', target.region='lhr'}}
Allow group MyTestGroup to use boot-volume-backups in tenancy where all
{request.permission='BOOT_VOLUME_BACKUP_COPY', any {request.region='phx',
request.region='iad'}}

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Boot Volume Backups.
   A list of the boot volume backups in the compartment you're viewing is displayed. If you don't see the one you're looking for, make sure you're viewing the correct compartment (select from the list on the left side of the page).
2. Click the Actions icon (three dots) for the boot volume backup you want to copy to another region.
3. Click Copy to Another Region.
4. Enter a name for the backup and choose the region to copy the backup to. Avoid entering confidential information.
5. In the Encryption section select whether you want the boot volume backup to use the Oracle-provided encryption key or your own Vault encryption key. If you select the option to use your own key, paste the OCID for encryption key from the destination region.
6. Click Copy Boot Volume Backup.
7. Confirm that the source and destination region details are correct in the confirmation dialog and then click OK.

Using the API
To copy a boot volume backup to another region, use the following operation:

• CopyBootVolumeBackup

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Next Steps
After copying the boot volume backup, switch to the destination region in the Console and verify that the copied backup appears in the list of boot volume backups for that region. You can then restore the backup using the steps in Restoring a Boot Volume on page 618.

For more information about backups, see Overview of Boot Volume Backups on page 615.

Cloning a Boot Volume
You can create a clone from a boot volume using the Oracle Cloud Infrastructure Block Volume service. Cloning enables you to make a copy of an existing boot volume without needing to go through the backup and restore process. For more information about the Block Volume service, see Overview of Block Volume on page 500 and the Block Volume FAQ.

A boot volume clone is a point-in-time direct disk-to-disk deep copy of the source boot volume, so all the data that is in the source boot volume when the clone is created is copied to the boot volume clone. Any subsequent changes to the data on the source boot volume are not copied to the boot volume clone. Since the clone is a copy of the source boot volume it will be the same size as the source boot volume unless you specify a larger volume size when you create the clone.

The clone operation occurs immediately and you can use the cloned boot volume as soon as the state changes to available.

There is a single point-in-time reference for a source boot volume while it is being cloned, so if you clone a boot volume while the associated instance is running, you need to wait for the first clone operation to complete from the source before creating additional clones. You also need to wait for any backup operations to complete as well.
You can only create a clone for a boot volume within the same region, availability domain, and tenant. You can create a clone for a boot volume between compartments as long as you have the required access permissions for the operation.

**Differences Between Boot Volume Backups and Clones**

Consider the following criteria when you decide whether to create a backup or a clone of a volume.

<table>
<thead>
<tr>
<th></th>
<th>Volume Backup</th>
<th>Volume Clone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Creates a point-in-time backup of data on a volume. You can restore multiple new volumes from the backup later in the future.</td>
<td>Creates a single point-in-time copy of a volume without having to go through the backup and restore process.</td>
</tr>
<tr>
<td><strong>Use case</strong></td>
<td>Retain a backup of the data in a volume, so that you can duplicate an environment later or preserve the data for future use. Meet compliance and regulatory requirements, because the data in a backup remains unchanged over time. Support business continuity requirements. Reduce the risk of outages or data mutation over time.</td>
<td>Rapidly duplicate an existing environment. For example, you can use a clone to test configuration changes without impacting your production environment.</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Slower (minutes or hours)</td>
<td>Faster (seconds)</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Lower cost</td>
<td>Higher cost</td>
</tr>
<tr>
<td><strong>Storage location</strong></td>
<td>Object Storage</td>
<td>Block Volume</td>
</tr>
<tr>
<td><strong>Retention policy</strong></td>
<td>Policy-based backups expire, manual backups do not expire</td>
<td>No expiration</td>
</tr>
<tr>
<td><strong>Volume groups</strong></td>
<td>Supported. You can back up a volume group.</td>
<td>Supported. You can clone a volume group.</td>
</tr>
</tbody>
</table>

For more information about boot volume backups, see [Overview of Boot Volume Backups](#) on page 615 and [Backing Up a Boot Volume](#) on page 617.

**Using the Console**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. In the **Boot Volumes** list, click the boot volume that you want to clone.
3. In **Resources**, click **Boot Volume Clones**.
4. Click **Create Clone**.
5. Specify a name for the clone. Avoid entering confidential information.
6. If you want to clone the boot volume to a larger size volume, select **Custom Boot Volume Size (GB)** and then specify the new size. You can only increase the size of the volume, you cannot decrease the size. If you clone the boot volume to a larger size volume, you need to extend the volume's partition. See [Extending the Partition for a Boot Volume](#) on page 612 for more information.
7. Click **Create Clone**.

The boot volume is ready use when its icon lists it as **AVAILABLE** in the **Boot Volumes** list.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To create a clone from a boot volume, use the CreateBootVolume operation and specify BootVolumeSourceFromBootVolumeDetails for CreateBootVolumeDetails.

Next Steps

After you have cloned a boot volume backup, you can:

• Use the boot volume to create an instance. For more information, see Creating an Instance on page 695.
• Attach the boot volume to an instance as a data volume. For more information, see Attaching a Volume on page 517.

Making a boot volume clone while an instance is running creates a crash-consistent clone, meaning the data is in the identical state it was in at the time the clone was made. This is the same state it would be in the case of a loss of power or hard crash. In most cases you can use the cloned boot volume to create an instance, however to ensure a bootable image, you should create a custom image from your instance. For information about creating custom images, see Managing Custom Images on page 665.

Detaching a Boot Volume

If you think a boot volume issue is causing a compute instance problem, you can stop the instance and detach the boot volume using the steps described in this topic. Then you can attach it to another instance as a data volume to troubleshoot it.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to attach and detach existing block volumes. The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups, but not launch instances.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

You can detach a boot volume from an instance only when the instance is stopped. See Stopping and Starting an Instance on page 779 for information about managing an instance's state.

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Choose your Compartment.
3. Click the instance that you want to detach the boot volume from.
5. Click the Actions icon (three dots) for the boot volume, and then click Detach Boot Volume. Confirm when prompted.

You can now attach the boot volume to another instance. For more information, see Attaching a Volume on page 517.

Using the API

To delete an attachment, use the following operation:

• DetachBootVolume

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Deleting a Boot Volume

When you terminate an instance, you choose to delete or preserve the associated boot volume. For more information, see Terminating an Instance on page 783. You can also delete a boot volume if it has been detached from the associated instance. See Detaching a Boot Volume on page 623 for how to detach a boot volume.

Caution:

You cannot undo this operation. Any data on a volume will be permanently deleted once the volume is deleted. You will also not be able to restart the associated instance.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let volume admins manage block volumes, backups, and volume groups on page 2146 lets the specified group do everything with block volumes and backups.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Boot Volumes.
2. Choose your Compartment.
3. In the Boot Volumes list, find the volume you want to delete.
4. Click the Actions icon (three dots) for the boot volume.
5. Click Terminate and confirm the selection when prompted.

Using the API

Use the DeleteBootVolume operation to delete a boot volume.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Boot Volume Metrics

You can monitor the health, capacity, and performance of your Compute instances by using metrics, alarms, and notifications.

The Block Volume service provides a set of metrics that apply to both boot volumes and block volumes. For more information, see Block Volume Metrics on page 585.

Recovering a Corrupted Boot Volume for Linux-Based Instances

If your instance fails to boot successfully or boots with the boot volume set to read-only access, the instance's boot volume may be corrupted. While it is rare, boot volume corruption can occur in the following scenarios:

- When an instance experiences a forced shutdown using the API.
- When an instance experiences a system hang due to an operating system or software error and a graceful reboot or shutdown of the instance times out, and then a forced shutdown occurs.
- When an error or outage occurs in the underlying infrastructure and there were critical disk writes pending in the system.
Compute

**Important:**

In most cases a simple reboot will resolve boot volume corruption issues, so this is the first action you should take when troubleshooting this.

This topic describes how to determine if your Linux-based instance's boot volume is corrupted and what steps to take to troubleshoot and recover the corrupted boot volume. For Windows instances, see Recovering a Corrupted Boot Volume for Windows Instances on page 628.

**Detecting Boot Volume Corruption**

Boot volume corruption can prevent an instance from booting successfully, so you may not be able to connect to the instance using SSH. Instead, you can use the instance console connection feature to connect to the malfunctioning instance. For more information about using this feature, see Troubleshooting Instances Using Instance Console Connections on page 813.

This section describes how to use a serial console connection to detect if boot volume corruption has occurred.

**Tip:**

If you have already confirmed your instance's boot volume is corrupted or if you are using an imported custom image, proceed to the Recovering the Boot Volume on page 626 section, which describes how to use a second instance along with standard file system tools to both detect and repair boot volume corruption.

1. Create a serial console connection for the instance.
2. Connect to the instance through serial console.
   
   At this point, it's normal for the serial console to appear to hang, as the system may have already crashed.
3. Reboot the instance from the Console.
4. Once the reboot process starts, switch back to the terminal window, and you should see system messages from the instance start to appear in the window.
5. Monitor the messages that appear as the system is starting up. Most operating systems will set the boot volume to read-only as soon as disk corruption is detected to prevent writes from further corrupting the volume, so look for messages that indicate the boot volume is in read-only mode. Following are some examples:
   
   • On an instance with iSCSI-attached boot volumes, the `iscsiadm` service will fail to attach a volume because the volume is in read-only mode. This will typically prevent instances from continuing to boot. The serial console may display a message similar to the following:

   ```
   iscsiadm: Maybe you are not root?
   iscsiadm: Could not lock discovery DB: /var/lock/iscsi/lock.write: Read-only file system
   touch: cannot touch '/var/lock/subsys/iscsid': Read-only file system
   touch: cannot touch '/var/lock/subsys/iscsi': Read-only file system
   ```
   
   • On an instance with paravirtualized-attached boot volumes, the system may continue the boot process, but will be in a degraded state because nothing can be written to the boot drive. The serial console may display error messages similar to the following:

   ```
   [FAILED] Failed to start Create Volatile Files and Directories. See 'systemctl status systemd-tmpfiles-setup.service' for details.
   ...
   [ 27.160070] cloud-init[819]: os.chmod(path, real_mode)
   [ 27.166027] cloud-init[819]: OSError: [Errno 30] Read-only file system: '/var/lib/cloud/data'
   ```
   
   The error messages and system behavior described here are the most commonly seen for boot volume corruption, however depending on the operating system, you may see different error messages and system behavior. If you don't see the ones described here, consult the documentation for your operating system for additional troubleshooting information.
Recovering the Boot Volume

To troubleshoot and recover the corrupted boot volume, you need to detach the boot volume from the instance and then attach the boot volume to a second instance as a data volume.

Detaching the Boot Volume

If you have detected that your instance's boot volume is corrupted, you need to detach the boot volume from the instance before you can begin troubleshooting and recovery steps.

1. Stop the instance.
2. Detach the boot volume from the instance.

Attaching the Boot Volume as a Data Volume to a Second Instance

For the second instance, we recommend that you use an instance running an operating system that most closely matches the operating system for the boot volume's instance. You should only attach boot volumes for Linux-based instances to other Linux-based instances. The second instance must be in the same availability domain and region as the boot volume's instance. If no existing instance is available, create a new Linux instance using the steps described in Creating an Instance on page 695. Once you have the second instance, make sure you can log into the instance and that it is functional before proceeding with the recovery steps. For steps to access the instance, see Connecting to a Linux Instance on page 734. After you have confirmed that the instance is functional, perform the following steps.

1. Run the `lsblk` command and make note of the drives that are currently on the instance, for example:

```
lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0 46.6G  0 disk
##sda2   8:2    0    8G  0 part [SWAP]
##sda3   8:3    0 38.4G  0 part /
##sda1   8:1    0  200M  0 part /boot/efi
```

2. Attach the boot volume to the second instance as a data volume. For more information, see Attaching a Volume on page 517.

   To attach the boot volume as a data volume
   a. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
   b. Click the instance that you want to attach a volume to.
   c. Under Resources, click Attached Block Volumes.
   d. Click Attach Block Volume.
   e. Select the volume attachment type. If Paravirtualized attachments are available for this instance, we recommend that you select this attachment type for this procedure.

      If you select iSCSI as the volume attachment type, you need to connect to the volume, see Connecting to a Volume on page 524 for more information.
   f. In the Block Volume Compartment drop-down list, select the compartment.
   g. Choose the Select Volume option and then select the volume from the Boot Volume section of the Block Volume drop-down list.
   h. Select Read/Write as the access type.
   i. Click Attach.

      When the volume's icon no longer lists it as Attaching, proceed with the next steps.

3. Run the `lsblk` command again to confirm that the boot volume now shows up as a volume attached to the instance. In this sample output for the `lsblk`, the boot volume attached as a data volume shows up as sdb:

```
lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sdb     8:16   0 46.6G  0 disk
```
4. Run the `fsck` command on the volume’s root partition. The root partition is usually the largest partition on the volume.

The following sample for the `fsck` command shows the output when there are no errors or corruption present on the partitions for an Oracle 7.6 instance:

```
sudo fsck -V /dev/sdb1
fsck from util-linux 2.23.2
[/sbin/fsck.vfat (1) -- /boot/efi] fsck.vfat /dev/sdb1
fsck.fat 3.0.20 (12 Jun 2013)
/dev/sdb1: 17 files, 2466/51145 clusters

sudo fsck -V /dev/sdb2
fsck from util-linux 2.23.2

sudo fsck -V /dev/sdb3
fsck from util-linux 2.23.2
[/sbin/fsck.xfs (1) -- /] fsck.xfs /dev/sdb3
If you wish to check the consistency of an XFS filesystem or repair a damaged filesystem, see xfs_repair(8).
```

If errors are present on a partition, you will usually be prompted to repair the errors. Following is an example of an interactive repair session of a corrupt ext4 boot volume for an Ubuntu instance:

```
sudo fsck -V /dev/sdb1
fsck from util-linux 2.31.1
[/sbin/fsck.ext4 (1) -- /] fsck.ext4 /dev/sdb1
e2fsck 1.44.1 (24-Mar-2018)
One or more block group descriptor checksums are invalid. Fix<y> yes
Group descriptor 92 checksum is 0xe9a1, should be 0x1f53. FIXED.
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
Block bitmap differences: Group 92 block bitmap does not match checksum. FIXED.
cloudimg-rootfs: ***** FILE SYSTEM WAS MODIFIED *****
cloudimg-rootfs: 75336/5999616 files (0.1% non-contiguous),
798678/12181243 blocks
```

**Note:**

XFS file systems will usually auto-repair their contents when the system boots up, fixing any corruption during the boot process. You can use the `xfs_repair` command to force a repair for scenarios where boot volume corruption is preventing the auto-repair functionality from working, as shown in the following example:

```
sudo xfs_repair /dev/sdb3
Phase 1 - find and verify superblock...
Phase 2 - using internal log
```
Recovering a Corrupted Boot Volume for Windows Instances

If your instance fails to boot successfully or boots with the boot volume set to read-only access, the instance's boot volume may be corrupted. While it is rare, boot volume corruption can occur in the following scenarios:

• When an instance experiences a forced shutdown using the API.
• When an instance experiences a system hang due to an operating system or software error and a graceful reboot or shutdown of the instance times out, and then a forced shutdown occurs.
• When an error or outage occurs in the underlying infrastructure and there were critical disk writes pending in the system.

Important:

In most cases a simple reboot will resolve boot volume corruption issues, so this is the first action you should take when troubleshooting this.

This topic describes how to determine if your Windows instance's boot volume is corrupted and what steps to take to troubleshoot and recover the corrupted boot volume. For Linux-based instances, see Recovering a Corrupted Boot Volume for Linux-Based Instances on page 624.

Detecting Boot Volume Corruption

When Windows operating systems detect boot volume corruption, the instance is usually able to recover from it by automatically repairing the file system. You can use a VNC console connection to verify that the instance isn't experiencing a system hang while repairing the file system, or to detect if there are other issues. VNC console connections enable you to see what's displayed through the VGA port, for more information about the VNC console, see Troubleshooting Instances Using Instance Console Connections on page 813.

Important:

VNC console connections only work for virtual machine (VM) instances launched on October 13, 2017 or later, and bare metal instances launched on February 21, 2019 or later. If your instance does not support VNC console connections, proceed to Recovering the Boot Volume on page 629.

1. Create a VNC console connection for the instance.
2. Connect to the instance through VNC console.

Check what is displayed in the VNC console to see if the instance is stuck in the boot process or if it is in the recovery partition.

Tip:

For Windows Server 2012 and later versions, if the instance has booted into the recovery partition it may be possible to directly perform the steps to recover the boot volume in the recovery partition.

Detaching the Boot Volume

If you have detected that your instance's boot volume is corrupted, you need to detach the boot volume from the instance before you can begin troubleshooting and recovery steps.

1. Stop the instance.
2. Detach the boot volume from the instance.
Computing

Recovering the Boot Volume

To troubleshoot and recover the corrupted boot volume, you need to attach the boot volume to a second instance as a data volume. For the second instance we recommend that you use an instance running an operating system that most closely matches the operating system for the boot volume's instance, and you should only attach boot volumes for Windows instances to other Windows instances. The second instance must be in the same availability domain and region as the boot volume's instance. If no existing instance is available create a new Windows instance using the steps described in Creating an Instance on page 695.

Once you have the second instance, make sure you can log in to the instance and that it is functional before proceeding with the recovery steps. After you have confirmed that the instance is functional perform the following steps.

1. Attach the boot volume to the second instance as a data volume. For more information, see Attaching a Volume on page 517.

   To attach the boot volume as a data volume
   a. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
   b. Click the instance that you want to attach a volume to.
   c. Under Resources, click Attached Block Volumes.
   d. Click Attach Block Volume.
   e. Select iSCSI for the volume attachment type.
   f. In the Block Volume Compartment drop-down list, select the compartment.
   g. Choose the Select Volume option and then select the volume from the Boot Volume section of the Block Volume drop-down list.
   h. Select Read/Write as the access type.
   i. Click Attach.

When the volume's icon no longer lists it as Attaching, proceed with the next steps.

2. Connect to the second instance, see Connecting to a Windows Instance on page 735 for more information.

3. Connect to the volume, see Connecting to a Volume on a Windows Instance on page 526 for more information.

   Since you are attaching a boot volume as a data volume you must also run the Connect-IscsiTarget and set IsMultiEnabled to true. For example:

   ```powershell
   Set-Service -Name msiscsi -StartupType Automatic
   Start-Service msiscsi
   New-IscsiTargetPortal -TargetPortalAddress 169.254.2.4
   Connect-IscsiTarget -NodeAddress iqn.2015-02.oracle.boot:uefi -TargetPortalAddress 169.254.2.4 -IsPersistent $True -IsMultipathEnabled $True
   ```

4. Open Computer Management and navigate to Storage, and then Disk Management.

5. Select the new disk and mark it Online.

6. Click This PC and then right-click on the new disk and select Properties.

7. Navigate to Tools, Error Checking, and then Check.

8. Select Scan Drive and fix issues as they come up.

9. Mark the new disk Offline.

10. Open iscsi initiator with administrator privileges.

11. In Favorite Targets, remove the iscsi target of the attached volume.

Oracle-Provided Images

An image is a template of a virtual hard drive. The image determines the operating system and other software for an instance. The following table lists the platform images that are available in Oracle Cloud Infrastructure. For specific
image and kernel version details, along with changes between versions, see the Oracle-Provided Image Release Notes.

<table>
<thead>
<tr>
<th>Image</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Autonomous Linux 7 Unbreakable Enterprise Kernel Release 6</td>
<td>Autonomous-Oracle-Linux-7.&lt;date&gt;-&lt;number&gt;</td>
<td>Oracle Autonomous Linux provides autonomous capabilities such as automated patching with zero downtime, and known exploit detection, to help keep the operating system highly secure and reliable. Oracle Autonomous Linux is based on Oracle Linux. GPU shapes are supported with this image.</td>
</tr>
<tr>
<td>Oracle Linux 8 Unbreakable Enterprise Kernel Release 6</td>
<td>Oracle-Linux-8.&lt;date&gt;-&lt;number&gt;</td>
<td>The Unbreakable Enterprise Kernel (UEK) is Oracle's optimized operating system kernel for demanding Oracle workloads. GPU shapes are supported with this image.</td>
</tr>
<tr>
<td>Oracle Linux 7 Unbreakable Enterprise Kernel Release 6</td>
<td>Oracle-Linux-7.&lt;date&gt;-&lt;number&gt;</td>
<td>The Unbreakable Enterprise Kernel (UEK) is Oracle's optimized operating system kernel for demanding Oracle workloads. GPU shapes are supported with this image.</td>
</tr>
<tr>
<td>Oracle Linux 6 Unbreakable Enterprise Kernel Release 4</td>
<td>Oracle-Linux-6.&lt;date&gt;-&lt;number&gt;</td>
<td>The Unbreakable Enterprise Kernel (UEK) is Oracle's optimized operating system kernel for demanding Oracle workloads.</td>
</tr>
<tr>
<td>CentOS 8</td>
<td>CentOS-8.&lt;date&gt;-&lt;number&gt;</td>
<td>CentOS is a free, open-source Linux distribution that is suitable for use in enterprise cloud environments. For more information, see <a href="https://www.centos.org/">https://www.centos.org/</a>. GPU shapes are supported with this image.</td>
</tr>
<tr>
<td>CentOS 7</td>
<td>CentOS-7.&lt;date&gt;-&lt;number&gt;</td>
<td>CentOS is a free, open-source Linux distribution that is suitable for use in enterprise cloud environments. For more information, see <a href="https://www.centos.org/">https://www.centos.org/</a>.</td>
</tr>
<tr>
<td>Image</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Ubuntu 20.04 LTS | Canonical-Ubuntu-20.04-<date>-<number> | Ubuntu is a free, open-source Linux distribution that is suitable for use in the cloud. For more information, see [https://www.ubuntu.com](https://www.ubuntu.com).  
Minimal Ubuntu is designed for automated use at scale. It uses a smaller boot volume, boots faster, and has a smaller surface for security patches than standard Ubuntu images. For more information, see [https://wiki.ubuntu.com/Minimal](https://wiki.ubuntu.com/Minimal). |
| Ubuntu 18.04 LTS | Canonical-Ubuntu-18.04-<date>-<number> | Ubuntu is a free, open-source Linux distribution that is suitable for use in the cloud. For more information, see [https://www.ubuntu.com](https://www.ubuntu.com).  
Minimal Ubuntu is designed for automated use at scale. It uses a smaller boot volume, boots faster, and has a smaller surface for security patches than standard Ubuntu images. For more information, see [https://wiki.ubuntu.com/Minimal](https://wiki.ubuntu.com/Minimal).  
GPU shapes are supported with this image. You must install the appropriate GPU drivers from NVIDIA. |
| Ubuntu 16.04 LTS | Canonical-Ubuntu-16.04-<date>-<number> | Ubuntu is a free, open-source Linux distribution that is suitable for use in the cloud. For more information, see [https://www.ubuntu.com](https://www.ubuntu.com).  
Minimal Ubuntu is designed for automated use at scale. It uses a smaller boot volume, boots faster, and has a smaller surface for security patches than standard Ubuntu images. For more information, see [https://wiki.ubuntu.com/Minimal](https://wiki.ubuntu.com/Minimal).  
GPU shapes are supported with this image. For Minimal Ubuntu, you must install the appropriate GPU drivers from NVIDIA. |
You also can create custom images of your boot disk OS and software configuration for launching new instances.

**Essential Firewall Rules**

All Oracle-provided images include rules that allow only "root" on Linux instances or "Administrators" on Windows Server instances to make outgoing connections to the iSCSI network endpoints (169.254.0.2:3260, 169.254.2.0/24:3260) that serve the instance’s boot and block volumes.

- We recommend that you do not reconfigure the firewall on your instance to remove these rules. Removing these rules allows non-root users or non-administrators to access the instance’s boot disk volume.
- We recommend that you do not create custom images without these rules unless you understand the security risks.
- Running Uncomplicated Firewall (UFW) on Ubuntu images might cause issues with these rules. Because of this, we recommend that you do not enable UFW on your instances. See Ubuntu instance fails to reboot after enabling Uncomplicated Firewall (UFW) for more information.

**User Data**

Oracle-provided images give you the ability to run custom scripts or supply custom metadata when the instance launches. To do this, you specify a custom user data script in the **Initialization Script** field when you create the instance. For more information about startup scripts, see cloud-init for Linux-based images and cloudbase-init for Windows-based images.

**OS Updates for Linux Images**

Oracle Linux and CentOS images are preconfigured to let you install and update packages from the repositories on the Oracle public yum server. The repository configuration file is in the /etc/yum.repos.d directory on your instance. You can install, update, and remove packages by using the yum utility.
On Oracle Autonomous Linux images, Oracle Ksplice is installed and configured by default to run automatic updates.

**Note:**

OS Security Updates for Oracle Linux and CentOS images

After you launch an instance using Oracle Linux or CentOS images, you are responsible for applying the required OS security updates published through the Oracle public yum server. For more information, see Installing and Using the Yum Security Plugin.

The Ubuntu image is preconfigured with suitable repositories to allow you to install, update, and remove packages.

**Note:**

OS Security Updates for the Ubuntu image

After you launch an instance using the Ubuntu image, you are responsible for applying the required OS security updates using the `sudo apt-get upgrade` command.

**Linux Kernel Updates**

Oracle Linux images on Oracle Cloud Infrastructure include Oracle Linux Premier Support at no extra cost. This gives you all the services included with Premier Support, including Oracle Ksplice. Ksplice enables you to apply important security and other critical kernel updates without a reboot. For more information, see About Oracle Ksplice and Ksplice Overview.

Ksplice is available for Linux instances launched on or after February 15, 2017. For instances launched before August 25, 2017, you must install Ksplice before running it. See Installing and Running Oracle Ksplice on page 664 for more information.

**Note:**

Ksplice Support

Oracle Ksplice is not supported for CentOS and Ubuntu images, or on Linux images launched before February 15, 2017.

**Configuring Automatic Package Updating on Instance Launch**

You can configure your instance to automatically update to the latest package versions when the instance first launches using a cloud-init startup script. To do this, add the following code to the startup script:

```
package_upgrade: true
```

The upgrade process starts when the instance launches and runs in the background until it completes. To verify that it completed successfully, check the cloud-init logs in `/var/log`.

See User Data on page 632 and Cloud config examples - Run apt or yum upgrade for more information.

**Linux Image Details**

See Lifetime Support Policy: Coverage for Oracle Linux and Oracle VM for details about the Oracle Linux support policy.

**Users**

For instances created using Oracle Linux and CentOS images, the username `opc` is created automatically. The `opc` user has `sudo` privileges and is configured for remote access over the SSH v2 protocol using RSA keys. The SSH public keys that you specify while creating instances are added to the `/home/opc/.ssh/authorized_keys` file.
For instances created using the Ubuntu image, the username \texttt{ubuntu} is created automatically. The \texttt{ubuntu} user has \texttt{sudo} privileges and is configured for remote access over the SSH v2 protocol using RSA keys. The SSH public keys that you specify while creating instances are added to the \texttt{/home/ubuntu/.ssh/authorized_keys} file.

Note that \texttt{root} login is disabled.

\textbf{Remote Access}

Access to the instance is permitted only over the SSH v2 protocol. All other remote access services are disabled.

\textbf{Firewall Rules}

Instances created using Oracle-provided images have a default set of firewall rules that allow only SSH access. Instance owners can modify those rules as needed, but must not restrict link local traffic to address 169.254.0.2 in accordance with the warning in Essential Firewall Rules on page 632.

Be aware that the Networking service uses network security groups and security lists to control packet-level traffic in and out of the instance. When troubleshooting access to an instance, make sure all of the following items are set correctly: the network security groups that the instance is in, the security lists associated with the instance's subnet, and the instance's firewall rules.

\textbf{Disk Partitions}

Starting with Oracle Linux 8.x, the main disk partition is managed using Logical Volume Management (LVM). This gives you increased flexibility to create and resize partitions to suit your workloads. In addition, there is no dedicated swap partition. Swap is now handled by a file on the file system, giving you more detailed control over swap.

\textbf{Cloud-init Compatibility}

Instances created using Oracle-provided images are compatible with cloud-init. When launching an instance with the Core Services API, you can pass cloud-init directives with the metadata parameter. For more information, see LaunchInstance.

\textbf{Oracle Autonomous Linux}

\begin{center}
\begin{tabular}{|l|}
\hline
\textbf{Important:} \\
Beginning with the December 2020 Oracle Autonomous Linux platform image, the image is based on Unbreakable Enterprise Kernel (UEK) 6 and is configured to use the standard Oracle Linux yum repositories. The Autonomous Linux repository (\texttt{al7}) is deprecated and all customers with existing Oracle Autonomous Linux instances are migrated to the new repositories automatically. \\
\hline
\end{tabular}
\end{center}

The following repositories are enabled by default beginning with the December 2020 Oracle Autonomous Linux platform image:

- \texttt{ol7\textunderscore UEKR6}
- \texttt{ol7\textunderscore addons}
- \texttt{ol7\textunderscore ksplice}
- \texttt{ol7\textunderscore latest}
- \texttt{ol7\textunderscore oci\textunderscore included}
- \texttt{ol7\textunderscore optional\textunderscore latest}
- \texttt{ol7\textunderscore software\textunderscore collections}
- \texttt{ol7\textunderscore x86\textunderscore 64\textunderscore userspace\textunderscore ksplice}

The image includes the release packages for the \texttt{ol7\_developer} and \texttt{ol7\_developer\_EPEL} repositories, but these repositories are disabled by default.
For existing Oracle Autonomous Linux instances, after yum migration, the `ol7_developer` and `ol7_developer_EPEL` repositories are not available. If you need packages from these repositories, you can install the appropriate release package to obtain the correct repository configuration before enabling the repository by using the following commands:

```
sudo yum install oraclelinux-developer-release-el7
sudo yum install oracle-epel-release-el7
```

**Note:**

Packages found in either the `ol7_developer` and `ol7_developer_EPEL` repositories are considered unsupported and are only entitled to basic installation support. Content from these repositories is not recommended for production environments and is intended for developer purposes only.

To verify that your Oracle Autonomous Linux instance has been migrated to the new repositories, use the following command:

```
yum repolist
```

For example:

```
# yum repolist
Loaded plugins: langpacks, ulninfo
repo id                                           repo name
status                                                                                          
ol7_UEKR6/x86_64                                  Latest Unbreakable Enterprise Kernel Release 6 for Oracle Linux 7Server (x86_64) 197
ol7_addons/x86_64                                 Oracle Linux 7Server Add ons (x86_64) 473
ol7_ksplice                                       Ksplice for Oracle Linux 7Server (x86_64) 9,655
ol7_latest/x86_64                                 Oracle Linux 7Server Latest (x86_64) 21,367
ol7_oci_included/x86_64                           Oracle Software for OCI users on Oracle Linux 7Server (x86_64) 680
ol7_optional_latest/x86_64                        Oracle Linux 7Server Optional Latest (x86_64) 15,491
ol7_software_collections/x86_64                   Software Collection Library release 3.0 packages for Oracle Linux 7 (x86_64) 15,375
ol7_x86_64_userspace_ksplice                       Ksplice aware userspace packages for Oracle Linux 7Server (x86_64) 447
repolist: 63,685
```

**Note:**

For existing Oracle Autonomous Linux instances, after yum migration, the UEK6 repository is enabled and the next daily update installs the latest UEK6. After reboot, the instance boots into UEK6.
For more information about installing and configuring Oracle Autonomous Linux, see Getting Started: Deploying and Configuring Oracle Autonomous Linux on Oracle Cloud Infrastructure and Oracle Autonomous Linux for Oracle Cloud Infrastructure.

Oracle Instant Client 18.3 basic package cannot be updated to Version 19.5 because of changes in packaging. To update Oracle Instant Client on Oracle Autonomous Linux images that were launched before March 18, 2020, you must first manually remove the Oracle Instant Client 18.3, and then install 19.5. Use the following commands:

```
sudo yum remove oracle-instantclient18.3-basic
sudo yum install oracle-instantclient19.5-basic
```

On Oracle Autonomous Linux images that were launched after March 18, 2020, Oracle Instant Client is not installed by default. To install Oracle Instant Client 19.5, you must manually install the package. Use the following command:

```
sudo yum install oracle-instantclient19.5-basic
```

On Oracle Autonomous Linux images that were launched after December 9, 2020, the Oracle Instant Client repository (ol7_oracleinstant_client) is not available by default. To add the repository, you must first install the oracle-release-el7 release package and then enable the ol7_oracle_instantclient repository. You can then install the appropriate Oracle Instant Client version package. Use the following commands:

```
sudo yum install oracle-release-el7
sudo yum-config-manager --enable ol7_oracle_instantclient
```

Oracle Autonomous Linux instances cannot be managed by the OS Management service.

For more information about using Oracle Autonomous Linux, see Known Issues.

**OCI Utilities**

Instances created using Oracle Linux include a preinstalled set of utilities that are designed to make it easier to work with Oracle Linux images. These utilities consist of a service component and related command line tools.

For more information, see the OCI Utilities on page 642 reference.

**Windows OS Updates for Windows Images**

Windows images include the Windows Update utility, which you can run to get the latest Windows updates from Microsoft. You have to configure the instance’s network security group or the security list used by the instance’s subnet to allow instances to access Windows update servers.

**Windows Image Details**

**Windows Editions**

Depending on whether you create a bare metal instance or a virtual machine (VM) instance, different editions of Windows Server are available as Oracle-provided images. Windows Server Standard edition is available only for VMs. Windows Server Datacenter edition is available only for bare metal instances.

**Users**

For instances created using Oracle-provided Windows images, the username opc is created automatically. When you launch an instance using the Windows image, Oracle Cloud Infrastructure will generate an initial, one-time password that you can retrieve using the console or API. This password must be changed after you initially log on.

**Remote Access**

Access to the instance is permitted only through a Remote Desktop connection.
Firewall Rules

Instances created using the Windows image have a default set of firewall rules that allow Remote Desktop protocol or RDP access on port 3389. Instance owners can modify these rules as needed, but must not restrict link local traffic to 169.254.169.253 for the instance to activate with Microsoft Key Management Service (KMS). This is how the instance stays active and licensed.

Be aware that the Networking service uses network security groups and security lists to control packet-level traffic in and out of the instance. When troubleshooting access to an instance, make sure all of the following items are set correctly: the network security groups that the instance is in, the security lists associated with the instance's subnet, and the instance's firewall rules.

User Data on Windows Images

On Windows images custom user data scripts are executed using cloudbase-init, which is the equivalent of cloud-init on Linux-based images. All Oracle-provided Windows images on Oracle Cloud Infrastructure include cloudbase-init installed by default. When an instance launches, cloudbase-init runs PowerShell, batch scripts, or additional user data content. See cloudbase-init Userdata for information about supported content types.

You can use user data scripts to perform various tasks, such as:

- Enable GPU support using a custom script to install the applicable GPU driver.
- Add or update local user accounts.
- Join the instance to a domain controller.
- Install certificates into the certificate store.
- Copy any required application workload files from the Object Storage service directly to the instance.

Caution:

Do not include anything in the script that could trigger a reboot, because this could impact the instance launch, causing it to fail. Any actions requiring a reboot should only be performed after the instance state is **RUNNING**.

Windows Remote Management

**Windows Remote Management** (WinRM) is enabled by default on Oracle-provided Windows images. WinRM provides you with the capability to remotely manage the operating system.

To use WinRM you need to add a stateful ingress security rule for TCP traffic on destination port 5986. You can implement this security rule in either a network security group that the instance belongs to, or a security list that is used by the instance's subnet.

Caution:

The following procedure allows WinRM connections from 0.0.0.0/0, which means any IP address, including public IP addresses. To allow access only from instances within the VCN, change the source CIDR value to the VCN's CIDR block. For more information, see Security Recommendations on page 3696.

To enable WinRM access

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN that you're interested in.
3. To add the rule to a network security group that the instance belongs to:
   a. Under **Resources**, click **Network Security Groups**. Then click the network security group that you're interested in.
   b. Click **Add Rules**.
   c. Enter the following values for the rule:
      - **Stateless**: Leave the check box cleared.
      - **Source Type**: CIDR
      - **Source CIDR**: 0.0.0.0/0
      - **IP Protocol**: TCP
      - **Source Port Range**: All
      - **Destination Port Range**: 5986
      - **Description**: An optional description of the rule.
   d. When done, click **Add**.

4. Or, to add the rule to a security list that is used by the instance's subnet:
   a. Under **Resources**, click **Security Lists**. Then click the security list you're interested in.
   b. Click **Add Ingress Rules**.
   c. Enter the following values for the rule:
      - **Stateless**: Leave the check box cleared.
      - **Source Type**: CIDR
      - **Source CIDR**: 0.0.0.0/0
      - **IP Protocol**: TCP
      - **Source Port Range**: All
      - **Destination Port Range**: 5986
      - **Description**: An optional description of the rule.
   d. When done, click **Add Ingress Rules**.

To use WinRM on an instance

1. Get the instance's public IP address.
2. Open Windows PowerShell on the Windows client that you're using to connect to the instance.
3. Run the following command:

   ```powershell
   # Get the public IP from your OCI running windows instance
   $ComputerName = Public IP Address

   # Store your username and password credentials (default username is opc)
   $c = Get-Credential

   # Options
   $opt = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck

   # Create new PSSession (Pre-requisite: ensure network security group or security list has Ingress Rule for port 5986)
   $PSSession = New-PSSession -ComputerName $ComputerName -UseSSL -SessionOption $opt -Authentication Basic -Credential $c

   # Connect to Instance PSSession
   Enter-PSSession $PSSession

   # To close connection use: Exit-PSSession
   ```

You can now remotely manage the Windows instance from your local PowerShell client.
Operating System Lifecycle and Support Policy

When an operating system reaches the end of its support lifecycle, the OS vendor (such as Microsoft) no longer provides security updates for the OS. You should upgrade to the latest version to remain secure.

Here's what you should expect when an OS version reaches the end of its support lifecycle:

• Oracle Cloud Infrastructure no longer provides new images for the OS version. Images that were previously published are deprecated, and are no longer updated.
• Although you can continue to run instances that use deprecated images, Oracle Cloud Infrastructure does not provide any support for operating systems that have reached the end of the support lifecycle.
• If you have an instance that runs an OS version that will be deprecated, and you want to launch new instances with this OS version after the end of support, you can create a custom image of the instance and then use the custom image to launch new instances in the future. For custom Linux images, you must purchase extended support from the OS vendor. For custom Windows images, see Can I purchase Microsoft Extended Security Updates for end-of-support Windows OSs? on page 809. Oracle Cloud Infrastructure does not provide any support for custom images that use end-of-support operating systems.

Be aware of these end-of-support dates:

• CentOS 6: Support ended on November 30, 2020.
• Ubuntu 14.04: Support ended on April 19, 2019.

Using NVIDIA GPU Cloud with Oracle Cloud Infrastructure

NVIDIA GPU Cloud (NGC) is a GPU-accelerated cloud platform optimized for deep learning and scientific computing. This topic provides an overview of how to use NGC with Oracle Cloud Infrastructure.

NVIDIA makes available on Oracle Cloud Infrastructure a customized Compute image that is optimized for the NVIDIA Tesla Volta and Pascal GPUs. Running NGC containers on this instance provides optimum performance for deep learning jobs.

Prerequisites

• An Oracle Cloud Infrastructure tenancy with a GPU quota. For more information about quotas, see Compute Quotas on page 247.
• A cloud network to launch the instance in. For information about setting up cloud networks, see Using the Console on page 2824 in VCNs and Subnets on page 2821.
• A key pair, to use for connecting to the instance via SSH. For information about generating a key pair, see Managing Key Pairs on Linux Instances on page 693.
• Security group and policy configured for the File Storage service. For more information, see Managing Groups on page 2419, Getting Started with Policies on page 2135, and Details for the File Storage Service on page 2273.
• An NGC API key for authenticating with the NGC service.

To generate your NGC API key

1. Sign in to the NGC website.
2. On the NGC Registry page, click Get API Key.
3. Click Generate API Key and then click Confirm to generate the key. If you have an existing API key it will become invalid once you generate a new key.

Launching an Instance Based on the NGC Image

Using the Console

1. Open the Console. For steps, see Signing In to the Console on page 41.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Select a Compartment that you have permission to work in.
4. Click **Create Instance**.
5. Enter a name for the instance. Avoid entering confidential information.
6. In the **Placement and hardware** section, make the following selections:
   a. Select the **Availability Domain** that you want to create the instance in.
   b. In the **Shape** section, click **Change Shape**. Then, do the following:
      1. For **Instance type**, select **Virtual Machine** or **Bare Metal Machine**.
      2. Select a GPU shape for the instance. For more information about GPU shapes, see virtual machine GPU shapes and bare metal GPU shapes.

     | Important: |
     |------------|
     | In order to access the GPU shapes, your tenancy must have a GPU quota. If your tenancy does not have a GPU quota, the GPU shapes will not be in the shape list. See Prerequisites on page 639 for more information. |

   3. Click **Select Shape**.
   c. To select the NGC image, do the following:
      1. Under **Image**, click **Change Image**.

     | Important: |
     |------------|
     | In order to access the NVIDIA GPU Cloud images, your tenancy must have a GPU quota and you must select a GPU shape. |

      2. In the **Image source** list, select **Oracle Images**.
      3. Select the check box next to **NVIDIA GPU Cloud Machine Image**.
      4. Review and accept the terms of use, and then click **Select Image**.

   7. In the **Networking** section, leave **Select existing virtual cloud network** selected, and then select the virtual cloud network (VCN) compartment, VCN, subnet compartment, and subnet.

   8. In the **Add SSH keys** section, upload the public key portion of the key pair that you want to use for SSH access to the instance. Browse to the key file that you want to upload, or drag and drop the file into the box.

   9. Click **Create**.

You should now see the NGC instance with the state of **Provisioning**. After the state changes to **Running**, you can connect to the instance. For general information about launching Compute instances, see Creating an Instance on page 695.

See the following topics for steps to access and work with the instance:

- Connecting to an Instance on page 733
- Stopping and Starting an Instance on page 779
- Terminating an Instance on page 783

When you connect to the instance using SSH, you are prompted for the NGC API key. If you supply the API key at the prompt, the instance automatically logs you in to the NGC container registry so that you can run containers from the registry. You can choose not to supply the API key at the prompt and still log in to the instance. You can then log in later to the NGC container registry. See Logging in to the NGC Container Registry for more information.

**Using the CLI**

Oracle Cloud Infrastructure provides a **Command Line Interface (CLI)** on page 4192 you can use to complete tasks. For more information, see Quickstart on page 4195 and Configuring the CLI on page 4202.

Use the **launch** command to create an instance, specifying image for **sourceType** and the image OCID `ocid1.image.oc1..aaaaaaaaknl6phck7e3iuii4r4axpwhenw5qtnnsk3tqppajdjb5nhoma3q` in **InstanceSourceDetails** for **LaunchInstanceDetails**.
Using the File Storage Service for Persistent Data Storage

You can use the File Storage service for data storage when working with NGC. For more information, see Overview of File Storage on page 1920. See the following tasks for creating and working with the File Storage service:

- Creating File Systems on page 1948
- Using the Console on page 1956
- Using the API on page 1979
- Managing File Systems on page 1970
- Using the Command Line Interface (CLI) on page 1976

Using the Block Volume Service for Persistent Data Storage

You can use the Block Volume service for data storage when working with NGC. For more information, see Overview of Block Volume on page 500. See the following tasks for creating and working with the Block Volume service:

- Creating a Volume on page 515
- Attaching a Volume on page 517
- Connecting to a Volume on page 524

You can also use the CLI to manage block volumes, see the volume commands.

Examples of Running Containers

You first need to log into the NGC container registry. You can skip this section if you provided your API key when logging into the instance via SSH. If you did not provide your API key when connecting to your instance, then you must perform this step.

To log into the NGC container registry

1. Run the following Docker command:

   
   ```
   docker login nvcr.io
   ```

2. When prompted for a username, enter $oauthtoken.
3. When prompted for a password enter your NGC API key.

At this point you can run Docker commands and access the NGC container registry from the instance.

Example: MNIST Training Run Using PyTorch Container

This sample demonstrates running the MNIST example under PyTorch. This example downloads the MNIST dataset from the web.

1. Pull and run the PyTorch container with the following Docker commands:

   ```
   docker pull nvcr.io/nvidia/pytorch:17.10
   docker run --gpus all --rm -it nvcr.io/nvidia/pytorch:17.10
   ```

2. Run the MNIST example with the following commands:

   ```
   cd /opt/pytorch/examples/mnist
   python main.py
   ```

Example: MNIST Training Run Using TensorFlow Container

This sample demonstrates running the MNIST example under TensorFlow. This example downloads the MNIST dataset from the web.

1. Pull and run the TensorFlow container with the following Docker commands:

   ```
   docker pull nvcr.io/nvidia/tensorflow:17.10
   docker run --gpus all --rm -it nvcr.io/nvidia/tensorflow:17.10
   ```
2. Run the MNIST_with_summaries example with the following commands:

```
   cd /opt/tensorflow/tensorflow/examples/tutorials/mnist
   python mnist_with_summaries.py
```

**OCI Utilities**

Instances created using Oracle-Provided Images on page 629 based on Oracle Linux include a pre-installed set of utilities that are designed to make it easier to work with Oracle Linux images. These utilities consist of a service component and related command line tools that can help with managing block volumes (attach, remove, and automatic discovery), secondary VNIC configuration, discovering the public IP address of an instance, and retrieving instance metadata.

The following table summarizes the components that are included in the OCI utilities.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ocid</td>
<td>The service component of oci-utils, which runs as a daemon started via systemd. This service scans for changes in the iSCSI and VNIC device configurations and caches the OCI metadata and public IP address of the instance.</td>
</tr>
<tr>
<td>oci-growfs</td>
<td>Expands the root filesystem of the instance to its configured size.</td>
</tr>
<tr>
<td>oci-iscsi-config</td>
<td>Lists or configures iSCSI devices attached to a compute instance. If no command line options are specified, lists devices that need attention.</td>
</tr>
<tr>
<td>oci-metadata</td>
<td>Displays metadata for the compute instance. If no command line options are specified, lists all available metadata. Metadata includes the instance OCID, display name, compartment, shape, region, availability domain, creation date, state, image, and any custom metadata that you provide, such as an SSH public key.</td>
</tr>
<tr>
<td>oci-network-config</td>
<td>Lists or configures virtual network interface cards (VNICs) attached to the Compute instance. When a secondary VNIC is provisioned in the cloud, it must be explicitly configured on the instance using this script or similar commands.</td>
</tr>
<tr>
<td>oci-network-inspector</td>
<td>Displays a detailed report for a given compartment or network.</td>
</tr>
<tr>
<td>oci-notify</td>
<td>Sends a message to a Oracle Cloud Infrastructure Notifications service topic.</td>
</tr>
<tr>
<td>oci-public-ip</td>
<td>Displays the public IP address of the current system in either human-readable or JSON format.</td>
</tr>
</tbody>
</table>

**Installing the OCI Utilities**

The OCI utilities (oci-utils) are automatically included with instances launched with Oracle Linux 7 and later images. They are not currently available on other distributions.

Much of the OCI utilities functionality requires that you have the Oracle Cloud Infrastructure SDK for Python and the Oracle Cloud Infrastructure CLI installed and configured.
To install the Oracle Cloud Infrastructure SDK and CLI using `yum`, install the required packages corresponding to the image used by the instance.

**Oracle Linux 7**

```bash
sudo yum install python36-oci-sdk python36-oci-cli
```

**Oracle Linux 8**

```bash
sudo yum install python3-oci-sdk python3-oci-cli
```

For configuration information, see the Oracle Cloud Infrastructure SDK for Python documentation and the documentation for configuring the Oracle Cloud Infrastructure CLI.

**Updating the OCI Utilities**

To update to the latest version of `oci-utils`:

```bash
sudo yum update oci-utils
```

**Using the OCI Utilities**

To use the OCI utilities, you first need to start the `ocid` service:

```bash
sudo systemctl start ocid.service
```

Example output:

```
Redirecting to /bin/systemctl start ocid.service
```

**The ocid Daemon**

**Description**

The `ocid` daemon is the service component of the `oci-utils`. It monitors for changes in the VNIC and iSCSI configuration of the instance and attempts to automatically attach or detach devices as they appear or disappear - for example, when they are created or deleted using the Oracle Cloud Infrastructure Console, CLI, or the API.

**Configuration**

The `ocid` daemon requires root privileges. You can configure root privileges for `ocid` using one of the following methods:

- Run the `oci setup config` configuration command as root to create SDK configuration files for the host. For more information, see SDK and CLI Configuration File on page 4184.
- Use instance principals by adding the instance to a dynamic group that was granted access to Oracle Cloud Infrastructure services. For more information, see Managing Dynamic Groups on page 2422.
- Configure `oci-utils` to allow root to use a non-privileged user's Oracle Cloud Infrastructure configuration files. For more information, see the configuration file located in the `/etc/oci-utils.conf.d` directory of the instance.

**Usage**

To start the `ocid` daemon using `systemd`:

```bash
service ocid start
```
To set `ocid` to start automatically during system boot:

```
sudo systemctl enable ocid.service
```

### oci-growfs

**Description**

Expands the root filesystem of the instance to its configured size. This command must be run as root.

**Usage**

`oci-growfs [-y] [-n] [-h]`

**Options**

- `-y`  
  Answer 'yes' to all prompts.

- `-n`  
  Answer 'no' to all prompts.

- `-h` | `--help`  
  Display a summary of the command line options.

**Example**

```
# sudo /usr/libexec/oci-growfs
CHANGE: disk=/dev/sda partition=3: start=17188864 old:  
  size=80486399, end=97675263 new:  size=192526302, end=209715166
Confirm? [y/n]: y
CHANGED: disk=/dev/sda partition=3: start=17188864 old:  
  size=80486399, end=97675263 new:  size=192526302, end=209715166
meta-data=/dev/sda3 isize=256 agcount=4, agsize=2515200
  bsize=4096 blocks=10060800, imaxpct=25
  sunit=0 swidth=0 blocks change from 10060800 to 24065787
```

### oci-iscsi-config

**Description**

Lists and configures iSCSI devices attached to a Compute instance running in Oracle Cloud Infrastructure. When run without any command line options, `oci-iscsi-config` lists devices that need attention.

**Usage**

```
ocsi-iscsi-config [-i|--interactive] [-s|--show] [-a | --attach IQN ]
 [-d IQN | --detach IQN ] [--username username] [--password password]
[---help] oci-iscsi-config [-s|--show] [-c | --create-volume size]
```
Compute

[--volume-name name] [--destroy-volume OCID]

**Options**

-i | --interactive
Run in interactive mode. This option displays devices that need attention and offers to attach and configure them. Requires root privileges.

-s | --show
List all devices. If ocid is not running, then root privileges are required.

-a | --attach target
Attempt to attach the device with the given IQN (a unique ID assigned to a device) or Oracle Cloud Identifier (OCID). When using an IQN, the volume must already be attached (assigned) to the instance in the Console. The Oracle Cloud Infrastructure SDK for Python is required for selecting volumes using their OCID. This option can be used multiple times to attach multiple devices at the same time. Requires root privileges.

-d | --detach device
Detach the device with the given IQN (a unique ID assigned to a device). If the volume (or any partition of the volume) is mounted, this option attempts to unmount it first. This option can be used multiple times to detach multiple devices at the same time. Requires root privileges.

-c | --create-volume size
Create a volume of SIZE gigabytes and attach it to the current instance. This option requires the Oracle Cloud Infrastructure SDK for Python to be installed and configured.

--destroy-volume OCID
Destroy the block storage volume with the given OCID. Be sure that the volume is not attached to any instances before performing this operation.

**Caution:**

This action is irreversible.

--volume-name name
Set the display name for the volume. This option is used with the --create-volume option. Avoid entering confidential information.

--username name
Use the specified username as the CHAP username when authentication is needed for attaching a device. This option is not needed when the Oracle Cloud Infrastructure SDK for Python is available.

--password password
Use the supplied password as the CHAP password when authentication is needed for attaching a device. This option is not needed when the Oracle Cloud Infrastructure SDK for Python is available.

--help
Display a summary of the command line options.
Examples

Displaying iSCSI configuration

The oci-iscsi-config utility works with the ocid daemon to monitor device creation and deletion through the command line, Console, or SDK and automatically discover those changes. You can use the --show option to display a list of all devices attached to an instance:

```bash
# oci-iscsi-config -s
For full functionality of this utility the ocid service must be running
The administrator can start it using this command:
sudo systemctl start ocid.service
ocid already running.
Currently attached iSCSI devices:

Target iqn.2015-02.oracle.boot:uefi
Persistent portal: 169.254.0.2:3260
Current portal: 169.254.0.2:3260
State: running
Attached device: sda
Size: 46.6G
Partitions: Device Size Filesystem Mountpoint
sda1 544M vfat /boot/efi
sda2 8G swap [SWAP]
sda3 38G xfs /
```

The following example shows the output of the --show option after adding a 50-GB block volume using the Console:

```bash
# oci-iscsi-config --show
Currently attached iSCSI devices:

Target iqn.2015-12.com.oracleiaas:abcdefghijklmnopqrstuvwxyz1234567890
Persistent portal: 169.254.2.2:3260
Current portal: 169.254.2.2:3260
State: running
Attached device: sdb
Size: 50G
File system type: Unknown
Mountpoint: Not mounted

Target iqn.2015-02.oracle.boot:uefi
Persistent portal: 169.254.0.2:3260
Current portal: 169.254.0.2:3260
State: running
Attached device: sda
Size: 46.6G
Partitions: Device Size Filesystem Mountpoint
sda1 544M vfat /boot/efi
sda2 8G swap [SWAP]
sda3 38G xfs /
```

Creating a volume

The following example shows how to create a volume:

```bash
# oci-iscsi-config --create-volume 50
For full functionality of this utility the ocid service must be running
```
The administrator can start it using this command:
`sudo systemctl start ocid.service`

Creating a new 50 GB volume
`Volume abcdefghijklmnopqrstuvwxyz1234567890123456789012345678901234 created`

Deleting a volume

The following example shows how to destroy a volume:

```
# oci-iscsi-config --destroy-volume ocid1.volume.oc1.phx.exampleuniqueID
```

oci-metadata

**Description**
Displays metadata for an Oracle Cloud Infrastructure Compute instance.

For more information about instance metadata, see [Getting Instance Metadata](#) on page 757.

**Usage**
```
oci-metadata [-h] [-j] [-g key] [--help]
```

**Options**

-h | --human-readable
Display human readable output (default).

-j | --json
Display output in JSON.

-g | --get key
Retrieve data only for the specified key.

--help
Display a summary of the command line options.

**Examples**

Getting all metadata for the instance

Running `oci-metadata` with no options returns all metadata for the instance:

```
# oci-metadata
Instance details:
  Display Name: my-example-instance
  Region: phx - us-phoenix-1 (Phoenix, AZ, USA)
  Canonical Region Name: us-phoenix-1
  Availability Domain: cumS:PHX-AD-1
  Fault domain: FAULT-DOMAIN-3
  OCID: ocid1.instance.oc1.phx.exampleuniqueID
  Compartment OCID: ocid1.compartment.oc1..exampleuniqueID
  Instance shape: VM.Standard2.1
  Image ID: ocid1.image.oc1.phx.exampleuniqueID
  Created at: 1569529065596
  state: Running
```
agentConfig:
  managementDisabled: False
  monitoringDisabled: False
Instance Metadata:
  ssh_authorized_keys: example-key
Networking details:
  VNIC OCID: ocid1.vnic.oc1.phx.exampleuniqueID
  VLAN Tag: 2392
  Private IP address: 10.0.0.16
  MAC address: 02:00:17:03:D8:FE
  Subnet CIDR block: 10.0.0.0/24
  Virtual router IP address: 10.0.0.1

Getting only specific metadata
The following example shows how to retrieve metadata for a specified key by using the --get parameter:

# oci-metadata --get state
Instance details:
Instance state: Running

oci-network-config

Description
Configures network interfaces for an Oracle Cloud Infrastructure Compute instance.

Usage
  [--del-private-ip ip_address] [--private-ip ip_address] [--subnet subnet] [--vnic-name name]
  [-r] [-X | --exclude item] [-I | --include item] [--quiet]

Options

-s | --show
Show information on all provisioning and interface configuration. If no options are specified, the oci-network-config utility defaults to this option.

--create-vnic
Create a new virtual network interface card (VNIC) and attach it to this instance.

--detach-vnic OCID
Detach and delete the VNIC with the given Oracle Cloud Identifier (OCID) or primary IP address. Cannot be the primary VNIC for the instance.

--add-private-ip OCID
Add a secondary private IP to an existing VNIC.
--del-private-ip ip_address
Delete the secondary private IP address with the given IP address.

--private-ip ip_address
Assign the given private IP address to the VNIC. Used with the --create-vnic and --add-private-ip options.

--subnet subnet
Connect the new VNIC to the specified subnet. Used with the --create-vnic option.

--vnic-name name
Display name for the new VNIC. Used with the --create-vnic option. Avoid entering confidential information.

--assign-public-ip
Assign a public IP address to the new VNIC. Used with the --create-vnic option.

--vnic OCID
Assign the private IP address to the given VNIC. Used with the --add-private-ip option.

-a | --auto | -c | --configure
Add IP configuration for VNICs that are not configured and delete IP configuration for VNICs that are no longer provisioned.

-d | --deconfigure
Deconfigure all VNICs (except the primary). If used with the -e option, only the secondary IP addresses are deconfigured.

-e ip_address VNIC_OCID
Secondary private IP address to configure or deconfigure. Used with --configure and --deconfigure options.

-n | -ns format
When configuring, place interfaces in namespace identified by the given format. Format can include $nic and $vltag variables.

-r | --sshd
Start sshd in namespace (if -n is present).

-X | --exclude item
Persistently exclude the given item from automatic configuration or deconfiguration. Use the --include option to include the item again.

-I | --include item
Include an item that was previously excluded using the --exclude option in automatic configuration/deconfiguration.
-q | --quiet
Do not display information messages.

-h | --help
Display a summary of the command line options.

Examples

Displaying current network configuration
Running the `oci-network-config` command with no options returns the network configuration of the current instance:

```
VNIC configuration for instance my-test-instance-20180622-1222

VNIC 1 (primary): my-test-instance-20180622-1222
Hostname: my-test-instance-20180622-1222
OCID: ocid1.vnic.oc1.phx.uniqueID
MAC address: 00:00:00:00:00:01
Public IP address: 203.0.113.2
Subnet: Public Subnet cumS:PHX-AD-1 (10.0.0.0/24)
```

Operating System level network configuration

```
 | IFACE | ADDR | SPREFIX | SBITS | VIRTRT | NS | IND |
---|---|---|---|---|---|---|---
- | 10.0.0.3 | 10.0.0.0 | 24 | 10.0.0.1 | - | - |
0 | ens3 | - | - | UP | 00:00:00:00:00:01 |
```

Creating a VNIC
This example creates a VNIC named MY_NEW_VNIC and attaches it to the instance:

```
# sudo oci-network-config --create-vnic --vnic-name MY_NEW_VNIC
Info: creating VNIC: 10.0.0.4
```

Running `oci-network-config` with the `-s` option shows information for the new VNIC:

```
# sudo oci-network-config -s
VNIC configuration for instance scottb-instance-20180622-1222

VNIC 1 (primary): scottb-instance-20180622-1222
Hostname: scottb-instance-20180622-1222
OCID: ocid1.vnic.oc1.phx.uniqueID
MAC address: 00:00:00:00:00:01
Public IP address: 203.0.113.254
Subnet: Public Subnet cumS:PHX-AD-1 (10.0.0.0/24)

VNIC 2: MY_NEW_VNIC
Hostname: scottb-instance-20180622-1222-mynewvnic
OCID: ocid1.vnic.oc1.phx.uniqueID
MAC address: None
Public IP address: None
Subnet: Public Subnet cumS:PHX-AD-1 (10.0.0.0/24)
```
Detaching a VNIC

To detach a VNIC from the instance, use the `--detach-VNIC` option. The given VNIC cannot be the primary VNIC for the instance:

```
sudo oci-network-config --detach-vnic 00:00:00:00:02
```

oci-network-inspector

**Description**

Displays a detailed report for a given compartment or network.

**Usage**

```
oci-network-inspector [-C OCID] [-N OCID] [--help]
```

**Options**

```
-C  |  --compartment OCID
```

Show report for the specified compartment.

```
-N  |  --vcn OCID
```

Show report for the specified virtual cloud network.

```
-h  |  --help
```

Display a summary of the command line options.

**Examples**

**Displaying a detailed report for a specified compartment**

Running the `oci-network-inspector` command and specifying an OCID with the `-C` parameter returns a detailed network report for that compartment:

```
$ oci-network-inspector -C ocid1.compartment.oc1..example_OCID

Compartment: scottb_sandbox (ocid1.compartment.oc1..example_OCID)

vcn: scottb_vcn

Security List: Default Security List for scottb_vcn

<table>
<thead>
<tr>
<th>Ingress</th>
<th>Source</th>
<th>Destination</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0.0.0.0/0:-</td>
<td>---:22</td>
<td></td>
</tr>
<tr>
<td>icmp</td>
<td>0.0.0.0/0:-</td>
<td>code-4:type-3</td>
<td></td>
</tr>
<tr>
<td>icmp</td>
<td>10.0.0.0/16:-</td>
<td>code-None:type-3</td>
<td></td>
</tr>
<tr>
<td>tcp</td>
<td>0.0.0.0/0:80</td>
<td>---:80</td>
<td></td>
</tr>
<tr>
<td>tcp</td>
<td>0.0.0.0/0:43</td>
<td>---:43</td>
<td></td>
</tr>
<tr>
<td>tcp</td>
<td>0.0.0.0/0:-</td>
<td>---:</td>
<td></td>
</tr>
<tr>
<td>Egress</td>
<td>all</td>
<td>0.0.0.0/0:-</td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Subnet: Public Subnet cumS:PHX-AD-3 Availability domain: cumS:PHX-AD-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cidr_block: 10.0.2.0/24</td>
</tr>
<tr>
<td>Domain name: sub99999999999.scottbvcn.oraclevcn.com</td>
</tr>
<tr>
<td>Security List: Default Security List for scottb_vcn</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: icmp</td>
</tr>
<tr>
<td>code-4:type-3</td>
</tr>
<tr>
<td>Ingress: icmp</td>
</tr>
<tr>
<td>None:type-3</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Egress: all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cidr_block: 10.0.1.0/24</td>
</tr>
<tr>
<td>Domain name: sub99999999998.scottbvcn.oraclevcn.com</td>
</tr>
<tr>
<td>Security List: Default Security List for scottb_vcn</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: icmp</td>
</tr>
<tr>
<td>code-4:type-3</td>
</tr>
<tr>
<td>Ingress: icmp</td>
</tr>
<tr>
<td>None:type-3</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Egress: all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subnet: Public Subnet cumS:PHX-AD-1 Availability domain: cumS:PHX-AD-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cidr_block: 10.0.0.0/24</td>
</tr>
<tr>
<td>Domain name: sub99999999997.scottbvcn.oraclevcn.com</td>
</tr>
<tr>
<td>Security List: Default Security List for scottb_vcn</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: icmp</td>
</tr>
<tr>
<td>code-4:type-3</td>
</tr>
<tr>
<td>Ingress: icmp</td>
</tr>
<tr>
<td>None:type-3</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Ingress: tcp</td>
</tr>
<tr>
<td>Egress: all</td>
</tr>
</tbody>
</table>

Private IP: 10.0.0.2(primary) Host: instance-20180608-1230
Vnic:
oci1.vnic.oc1.phx.abcxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(AVAILABLE-ATTACHED)
Vnic PublicIP: 203.0.113.2
Instance: instance-20180608-1230(STOPPED)
Private IP: 10.0.0.3( primary) Host: scottb-instance-20180622-1222
Vnic:
oci1.vnic.oc1.phx.abcxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
(AVAILABLE-ATTACHED)
Vnic PublicIP: 203.0.113.3
Instance: scottb-instance-20180622-1222(RUNNING)

**oci-notify**

**Description**

Sends a message to a Oracle Cloud Infrastructure Notifications service topic. This command must be run as root.
A message is composed of a message header (subject) and file. The Notifications service configuration for the topic
determines where and how the messages are delivered. Topics are configured for the Notification service using the
Oracle Cloud Infrastructure Console, API, or CLI.

For more information about the Notifications service, including how to create topics, see Notifications Overview.

Usage

oci-notify [-c topic_OCID] [-t subject -f file] [-h]

Options

-c topic_OCID
Write the topic to the /etc/oci-utils/oci.conf file. The path to the configuration file can be overridden by
using OCI_CONFIG_DIR environment variable.

For topic_OCID, specify the Oracle Cloud Identifier (OCID) associated with the Notifications service topic.

-t subject -f file
Publish the contents of specified file with the specified subject to the topic, which is sent to each subscription for the
topic.

For subject, enter an appropriate subject to be used as the message header (for example, 'log messages' if you
are sending log files). The subject must be enclosed in either single or double quotation marks. Message headers are
truncated to 128 characters.

Note:
When the message is published, the oci-notify utility prepends the
instance name to the subject of the message, for example, <instance
name>:log messages.

For file, enter the full or relative directory path, HTTP, or FTP URL of the message file to be sent. Large files are split
into 64-KB chunks.

Note:
The oci-notify utility writes log and error messages to the /var/log/
oci-notify.log file.

-h | help
Display a summary of the command line options.

Examples

Configuring a Topic on an Instance

The following example shows how to write the OCID of a configured Notifications service topic to the oci.conf file. Once configured, you can publish messages to the configured topic.

```
sudo oci-notify -c ocid1.onstopic.oc1..example_OCID
```

Publishing a Message to a Topic

The following example shows how to send the contents of the /var/log/messages file with the subject
'logging messages' to the configured topic:

```
sudo oci-notify -t 'logging messages' -f /var/log/messages
```
The following example shows how to send the contents of the /proc/meminfo file with the subject 'memory information' to the configured topic:

```
sudo oci-notify -t 'memory information' -f /proc/meminfo
```

The following example shows how to send the contents of the /tmp/uptrack-show file with the subject 'installed Ksplice updates' to the configured topic:

```
sudo oci-notify -t 'installed Ksplice updates' -f /tmp/uptrack-show
```

oci-public-ip

Description
Displays the public IP address of the current system in either human-readable or JSON format.

The oci-public-ip utility uses the Oracle Cloud Infrastructure SDK to discover the IP address. If the IP address cannot be obtained through this method, the oci-public-ip utility then tries the Session Traversal Utilities for NAT (STUN) protocol as a last resort to discover the IP address. For more information on STUN, see the STUN Wikipedia article.

Usage

Options

- **h | --human-readable**
  Display human readable output (default).

- **j | --json**
  Display output in JSON.

- **g | get**
  Print the IP address only.

- **a | all**
  Display all public IP addresses.

- **s | --sourceip source_IP**
  Specify the source IP address to use.

- **S | --stun-server STUN_server**
  Specify the STUN server to use.

- **L | --list-servers**
  Print a list of known STUN servers and exit.

  --instance-id OCID
  Display the public IP address of the given instance instead of the current one. Requires the Oracle Cloud Infrastructure SDK for Python to be installed and configured.
**--help**
Display a summary of the command line options.

**Examples**

**Displaying current IP address**
Running the `oci-public-ip` command with no options returns the IP address of the current instance:

```bash
# oci-public-ip
Public IP address: 203.0.113.2
```

**Displaying the IP address of another instance**
You can pass in the OCID of a running instance with the `--instance-id` option to return the IP address for that instance:

```bash
# oci-public-ip --instance-id ocid1.instance.oc1.phx.example_OCID
Public IP address: 203.0.113.2
```

**Listing STUN servers**
Use the `--list-servers` option to return a list of STUN servers:

```bash
# oci-public-ip --list-servers
stun.stunprotocol.org
stun.counterpath.net
stun.voxgratia.org
stun.callwithus.com
stun.ekiga.net
stun.ideasip.com
stun.voipbuster.com
stun.voiparound.com
stun.voipstunt.com
```

**Compute Shapes**
A shape is a template that determines the number of CPUs, amount of memory, and other resources that are allocated to an instance.

This topic provides basic information about the shapes that are available for bare metal instances, virtual machines (VMs), and dedicated virtual machine hosts.

**Flexible Shapes**
A flexible shape is a shape that lets you customize the number of OCPUs and the amount of memory when launching or resizing your VM. When you create a VM instance using the flexible shape, you select the number of OCPUs and the amount of memory that you need for the workloads that run on the instance. The network bandwidth and number of VNICs scale proportionately with the number of OCPUs. This flexibility lets you build VMs that match your workload, enabling you to optimize performance and minimize cost.

Currently, flexible memory is available on VM.Standard.E3.Flex instances that run on AMD Rome processors. For this VM and processor combination, you can select from 1 to 64 OCPUs. The amount of memory allowed is based on the number of OCPUs selected. For each OCPU, you can select up to 64 GB of memory, with a maximum of 1024 GB total. The minimum amount of memory allowed is either 1 GB or a value matching the number of OCPUs, whichever is greater. For example, if you select 25 OCPUs, the minimum amount of memory allowed is 25 GB.
These resources are billed at a per-second granularity with a one-minute minimum. Optimize your costs by choosing the shape that matches your workload and by changing the shape when your workload changes. For example, you can configure the VM to maximize compute processing power by choosing a low core-to-memory ratio. Or, for applications like in-memory databases or big data processing engines, configure an instance with a high core-to-memory ratio. Modify the OCPUs and memory as your workload changes, scaling up to increase performance or scaling down to reduce costs.

The VM.Standard.E3.Flex shape, a VM standard shape, is a flexible shape.

**Note:**
When a new region becomes available, it might take a few weeks before host capacity for flexible shapes also becomes available.

**Supported Images**
The following Oracle-provided platform images are compatible with flexible shapes. Use an image that was published in March 2020 (for Linux images) or April 2020 (for Windows images) or later.

**Images**
- Oracle Autonomous Linux 7.x
- Oracle Linux 8.x
- Oracle Linux 7.x
- Oracle Linux 6.x (VMs only)
- CentOS 8.x
- CentOS 7.x
- Ubuntu 18.04
- Ubuntu 16.04
- Windows Server 2019 (VMs only)
- Windows Server 2016 (VMs only)
- Windows Server 2012 (VMs only)

Custom images are also supported, depending on the image. You must add flexible shape compatibility to the custom image, and then test the image on the flexible shape to ensure that it actually works on the shape.

**Bare Metal Shapes**
The following shapes are available for bare metal instances:

- **Standard Shapes** on page 656
- **Dense I/O Shapes** on page 657
- **GPU Shapes** on page 657
- **HPC Shapes** on page 658

Network bandwidth is based on expected bandwidth for traffic within a VCN. To determine which physical NICs are active for a shape, refer to the network bandwidth specifications in the following tables. If the network bandwidth is listed as "2 x `<bandwidth>` Gbps," it means that both NIC 0 and NIC 1 are active.

**Standard Shapes**
Designed for general purpose workloads and suitable for a wide range of applications and use cases. Standard shapes provide a balance of cores, memory, and network resources. Standard shapes are available with Intel or AMD processors.

These are the bare metal standard series:
- **BM.Standard2**: X7-based standard compute. Processor: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.
Dense I/O Shapes

Designed for large databases, big data workloads, and applications that require high-performance local storage. Dense I/O shapes include locally-attached NVMe-based SSDs.

This is the bare metal dense I/O series:

- **BM.DenseIO2**: X7-based dense I/O compute. Processor: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.DenseIO2.52</td>
<td>52</td>
<td>768</td>
<td>Block storage only</td>
<td>2 x 25 Gbps</td>
<td>52 total (26 per physical NIC)</td>
<td>27 total (1 on the first physical NIC, 26 on the second)</td>
</tr>
</tbody>
</table>

GPU Shapes

Designed for hardware-accelerated workloads. GPU shapes include Intel or AMD CPUs and NVIDIA graphics processors.

These are the bare metal GPU series:

- **BM.GPU3**: X7-based GPU compute.
  - GPU: NVIDIA Tesla V100 16 GB
  - CPU: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.

- **BM.GPU4**: E2-based GPU compute.
  - GPU: NVIDIA A100 40 GB
  - CPU: AMD EPYC 7542. Base frequency 2.9 GHz, max boost frequency 3.4 GHz.
<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.GPU3.8</td>
<td>52</td>
<td>128</td>
<td>768 Block storage only</td>
<td>2 x 25 Gbps</td>
<td>52</td>
<td>27 (1 on the first physical NIC, 26 on the second)</td>
</tr>
<tr>
<td>(GPU: 8xV100)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BM.GPU4.8</td>
<td>64</td>
<td>320</td>
<td>2048 27.2 TB NVMe SSD (4 drives)</td>
<td>1 x 50 Gbps 8 x 200 Gbps RDMA</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>(GPU: 8xA100)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**HPC Shapes**

Designed for high-performance computing workloads that require high frequency processor cores and cluster networking for massively parallel HPC workloads.

This is the bare metal HPC series:

- **BM.HPC2**: X7-based high frequency compute. Processor: Intel Xeon Gold 6154. Base frequency 3.0 GHz, max turbo frequency 3.7 GHz.

**VM Shapes**

The following shapes are available for VMs:

- **Standard Shapes** on page 658
- **Dense I/O Shapes** on page 659
- **GPU Shapes** on page 660

Network bandwidth is based on expected bandwidth for traffic within a VCN.

**Standard Shapes**

Designed for general purpose workloads and suitable for a wide range of applications and use cases. Standard shapes provide a balance of cores, memory, and network resources. Standard shapes are available with Intel or AMD processors.

These are the VM standard series:

- **VM.Standard2**: X7-based standard compute. Processor: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.
- **VM.Standard.E3**: E3-based standard compute, with a flexible number of OCPUs. Processor: AMD EPYC 7742. Base frequency 2.25 GHz, max boost frequency 3.4 GHz.
### Compute Shapes

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard2.1</td>
<td>15</td>
<td>15</td>
<td>Block storage only</td>
<td>1 Gbps</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VM.Standard2.2</td>
<td>30</td>
<td>30</td>
<td>Block storage only</td>
<td>2 Gbps</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VM.Standard2.4</td>
<td>60</td>
<td>60</td>
<td>Block storage only</td>
<td>4.1 Gbps</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>VM.Standard2.8</td>
<td>120</td>
<td>120</td>
<td>Block storage only</td>
<td>8.2 Gbps</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>VM.Standard4.16</td>
<td>240</td>
<td>240</td>
<td>Block storage only</td>
<td>16.4 Gbps</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>VM.Standard4.24</td>
<td>320</td>
<td>320</td>
<td>Block storage only</td>
<td>24.6 Gbps</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>VM.Standard.E2.1.Micro</td>
<td>1 OCPU minimum, 64 OCPU maximum</td>
<td>1 GB minimum, 1024 GB maximum</td>
<td>Block storage only</td>
<td>480 Mbps</td>
<td>1</td>
<td>-</td>
</tr>
</tbody>
</table>

1: Instances are billed for the full amount of memory that you provision. Usable memory is reduced by up to 256 MB per instance. This difference is due to memory reserved to support the VM on the hypervisor.

### Dense I/O Shapes

Dense I/O Shapes are designed for large databases, big data workloads, and applications that require high-performance local storage. Dense I/O shapes include locally-attached NVMe-based SSDs.

This is the VM dense I/O series:

- **VM.DenseIO2**: X7-based dense I/O compute. Processor: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.DenseIO2.8</td>
<td>120</td>
<td>120</td>
<td>Block storage only</td>
<td>6.4 TB NVMe SSD</td>
<td>8.2 Gbps</td>
<td>8</td>
</tr>
<tr>
<td>VM.DenseIO2.16</td>
<td>240</td>
<td>240</td>
<td>Block storage only</td>
<td>12.8 TB NVMe SSD</td>
<td>16.4 Gbps</td>
<td>16</td>
</tr>
</tbody>
</table>
### GPU Shapes

Designed for hardware-accelerated workloads. GPU shapes include Intel or AMD CPUs and NVIDIA graphics processors.

This is the VM GPU series:
- **VM.GPU3**: X7-based GPU compute.
  - GPU: NVIDIA Tesla V100 16 GB
  - CPU: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.DenseEI2i24</td>
<td>24</td>
<td>320</td>
<td>25.6 TB NVMe SSD</td>
<td>24.6 Gbps</td>
<td>24</td>
<td>24</td>
</tr>
</tbody>
</table>

- **DVH.Standard2.52**: X7-based VM host
  - Billed OCPU: 52
  - Usable OCPU: 48
  - Supported Shapes for Hosted VMs: VM.Standard2
**Upgrading from a Previous Generation Shape**

To upgrade from a previous generation shape to a current generation shape, you can do the following things:

- For supported VM instances, **change the shape of the instance**.
- For bare metal instances and VM instances that don't support changing the shape, **terminate the instance but DO NOT delete the boot volume**. Then, **use the boot volume to create a new instance**.

**Previous Generation Bare Metal Shapes**

These are the previous generation bare metal shape series.

**BM.Standard1**

*Newer shape recommendation:* BM.Standard2 or BM.Standard.E3 series

*End of orderability date:* December 31, 2020

X5-based standard compute. Processor: Intel Xeon E5-2699 v3. Base frequency 2.3 GHz, max turbo frequency 3.6 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.Standard1.36</td>
<td>36</td>
<td>256</td>
<td>Block storage only</td>
<td>1 x 10 Gbps</td>
<td>36</td>
<td>1</td>
</tr>
</tbody>
</table>

**BM.Standard.B1**

*Newer shape recommendation:* BM.Standard2 or BM.Standard.E3 series

*End of orderability date:* December 31, 2020

X6-based standard compute. Processor: Intel Xeon E5-2699 v4. Base frequency 2.2 GHz, max turbo frequency 3.6 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.Standard.B1.44</td>
<td>44</td>
<td>512</td>
<td>Block storage only</td>
<td>1 x 25 Gbps</td>
<td>44</td>
<td>None</td>
</tr>
</tbody>
</table>

**BM.Standard.E2**

*Newer shape recommendation:* BM.Standard2 or BM.Standard.E3 series

*End of orderability date:* February 8, 2021

E2-based standard compute. Processor: AMD EPYC 7551. Base frequency 2.0 GHz, max boost frequency 3.0 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.Standard.E2.64</td>
<td>64</td>
<td>512</td>
<td>Block storage only</td>
<td>2 x 25 Gbps</td>
<td>75</td>
<td>76 (1 on the first physical NIC, 75 on the second)</td>
</tr>
</tbody>
</table>

**BM.DenseIO1**

*Newer shape recommendation:* BM.DenseIO2
End of orderability date: December 31, 2020

X5-based dense I/O compute. Processor: Intel Xeon E5-2699 v3. Base frequency 2.3 GHz, max turbo frequency 3.6 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.DenseIO1.36</td>
<td>36</td>
<td>512</td>
<td>28.8 TB NVMe SSD (9 drives)</td>
<td>1 x 10 Gbps</td>
<td>36</td>
<td>1</td>
</tr>
</tbody>
</table>

BM.GPU2

Newer shape recommendation: BM.GPU3 or BM.GPU4 series

End of orderability date: December 31, 2020

X7-based GPU compute.
- GPU: NVIDIA Tesla P100 16 GB
- CPU: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.GPU2.2</td>
<td>28</td>
<td>GPU Memory: 32 CPU Memory: 192</td>
<td>Block storage only</td>
<td>2 x 25 Gbps</td>
<td>28</td>
<td>15 (1 on the first physical NIC, 14 on the second)</td>
</tr>
<tr>
<td>(GPU: 2xP100)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Previous Generation VM Shapes

These are the previous generation VM shape series.

VM.Standard1

Newer shape recommendation: VM.Standard2 or VM.Standard.E3 series

End of orderability date: December 31, 2020

X5-based standard compute. Processor: Intel Xeon E5-2699 v3. Base frequency 2.3 GHz, max turbo frequency 3.6 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICs Total: Linux</th>
<th>Max VNICs Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard1.1</td>
<td>7</td>
<td>Block storage only</td>
<td></td>
<td>600 Mbps</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>VM.Standard1.2</td>
<td>14</td>
<td>Block storage only</td>
<td></td>
<td>1.2 Gbps</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>VM.Standard1.4</td>
<td>28</td>
<td>Block storage only</td>
<td></td>
<td>1.2 Gbps</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>VM.Standard1.8</td>
<td>56</td>
<td>Block storage only</td>
<td></td>
<td>2.4 Gbps</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>VM.Standard1.16</td>
<td>112</td>
<td>Block storage only</td>
<td></td>
<td>4.8 Gbps</td>
<td>16</td>
<td>1</td>
</tr>
</tbody>
</table>

VM.Standard.B1
Newer shape recommendation: VM.Standard2 or VM.Standard.E3 series

End of orderability date: December 31, 2020

X6-based standard compute. Processor: Intel Xeon E5-2699 v4. Base frequency 2.2 GHz, max turbo frequency 3.6 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard.B1.1</td>
<td>12</td>
<td>Block storage only</td>
<td>600 Mbps</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.B1.2</td>
<td>24</td>
<td>Block storage only</td>
<td>1.2 Gbps</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.B1.4</td>
<td>48</td>
<td>Block storage only</td>
<td>2.4 Gbps</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.B1.8</td>
<td>96</td>
<td>Block storage only</td>
<td>4.8 Gbps</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.B1.16</td>
<td>192</td>
<td>Block storage only</td>
<td>9.6 Gbps</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

VM.Standard.E2

Newer shape recommendation: VM.Standard2 or VM.Standard.E3 series

End of orderability date: February 8, 2021

E2-based standard compute. Processor: AMD EPYC 7551. Base frequency 2.0 GHz, max boost frequency 3.0 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard.E2.1</td>
<td>8</td>
<td>Block storage only</td>
<td>700 Mbps</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.E2.2</td>
<td>16</td>
<td>Block storage only</td>
<td>1.4 Gbps</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.E2.4</td>
<td>32</td>
<td>Block storage only</td>
<td>2.8 Gbps</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>VM.Standard.E2.8</td>
<td>64</td>
<td>Block storage only</td>
<td>5.6 Gbps</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

VM.DenseIO1

Newer shape recommendation: VM.DenseIO2 series

End of orderability date: December 31, 2020

X5-based dense I/O compute. Processor: Intel Xeon E5-2699 v3. Base frequency 2.3 GHz, max turbo frequency 3.6 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.DenseIO1.4</td>
<td>60</td>
<td>3.2 TB NVMe SSD</td>
<td>1.2 Gbps</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>VM.DenseIO1.8</td>
<td>120</td>
<td>6.4 TB NVMe SSD</td>
<td>2.4 Gbps</td>
<td>8</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>VM.DenseIO1.16</td>
<td>240</td>
<td>12.8 TB NVMe SSD</td>
<td>4.8 Gbps</td>
<td>16</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

VM.GPU2

Newer shape recommendation: VM.GPU3 series
**End of orderability date:** December 31, 2020

X7-based GPU compute.

- GPU: NVIDIA Tesla P100 16 GB
- CPU: Intel Xeon Platinum 8167M. Base frequency 2.0 GHz, max turbo frequency 2.4 GHz.

<table>
<thead>
<tr>
<th>Shape</th>
<th>OCPU</th>
<th>Memory (GB)</th>
<th>Local Disk (TB)</th>
<th>Max Network Bandwidth</th>
<th>Max VNICS Total: Linux</th>
<th>Max VNICS Total: Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>VML.GPU2.1xP100</td>
<td>12</td>
<td>GPU Memory: 16, CPU Memory: 72</td>
<td>Block storage only</td>
<td>8 Gbps</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

## Installing and Running Oracle Ksplice

Oracle Ksplice lets you apply important security updates and other critical kernel updates without a reboot. For more information, see [About Oracle Ksplice](#) and [Ksplice Overview](#).

This topic describes how to install and configure Ksplice. Ksplice is available for Oracle Linux instances that were launched on or after February 15, 2017. Ksplice is installed on instances that were launched on or after August 25, 2017, so you just need to run it on these instances to install the available Ksplice patches. For instances that were launched before August 25, 2017, you must install Ksplice before running it.

On Oracle Autonomous Linux images, Ksplice is installed and configured by default to run automatic updates.

### Installing Ksplice on instances launched before August 25, 2017

To install Ksplice, you must connect to your Linux instance by using a Secure Shell (SSH). See [Connecting to an Instance](#) for more information.

1. Use the following SSH command to access the instance.

   ```bash
   ssh -l opc@<public-ip-address>
   ```

   `<public-ip-address>` is your instance IP address that you retrieved from the Console, see [Getting the Instance Public IP Address](#) on page 67.

2. Run the following SSH commands to sudo to the root:

   ```bash
   sudo bash
   ```

3. Download the Ksplice installation script with the following SSH command:

   ```bash
   ```

4. Once the script is downloaded, use the following SSH command to install Ksplice:

   ```bash
   sh install-uptrack-oc
   ```

## Running Ksplice

To run Ksplice, you must connect to your Linux instance using a Secure Shell (SSH) connection. See [Connecting to an Instance](#) on page 733 for more information.
1. Use the following SSH command to access the instance.

```bash
ssh -l opc <public-ip-address>
```

`<public-ip-address>` is the instance IP address that you retrieved from the Console, see Getting the Instance Public IP Address on page 67.

2. Run the following SSH commands to sudo to the root:

```bash
sudo bash cd
```

3. To install available Ksplice patches, run the following SSH command:

```bash
uptrack-upgrade
```

**Automatic Updates**

To configure automatic updates, set the value of `autoinstall` to `yes` in `/etc/uptrack/uptrack.conf`.

**Note:**

OS Security Updates for Oracle Linux images

Oracle Linux images are updated regularly with the necessary patches, but after you launch an instance using these images, you are responsible for applying the required OS security updates published through the Oracle public Yum server. For more information, see Installing and Using the Yum Security Plugin.

**Managing Custom Images**

Oracle Cloud Infrastructure uses images to launch instances. You specify an image to use when you launch an instance.

You can create a custom image of a bare metal instance's boot disk and use it to launch other instances. Instances you launch from your image include the customizations, configuration, and software installed when you created the image.

For details on Windows images, see Creating Windows Custom Images on page 668.

Custom images do not include the data from any attached block volumes. For information about backing up volumes, see Backing Up a Volume on page 546.

**Tip:**

Follow industry-wide hardware failure best practices to ensure the resilience of your solution in the event of a hardware failure. Some best practices include:

- Design your system with redundant compute nodes in different availability domains to support failover capability.
- Create a custom image of your system drive each time you change the image.
- Back up your data drives, or sync to spare drives, regularly.

If you experience a hardware failure and have followed these practices, you can terminate the failed instance, launch your custom image to create a new instance, and then apply the backup data.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let image admins manage custom images on page 2144 includes the ability to create, delete, and manage custom images.

The policy in Let users launch compute instances on page 2143 includes the ability to create an instance using any custom image. The policy in Let users launch compute instances from a specific custom image on page 2144 restricts the ability to create an instance from a custom image on an image-by-image basis.

Tip:

When users create a custom image from an instance or launch an instance from a custom image, the instance and image don't have to be in the same compartment. However, users must have access to both compartments.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Limitations and Considerations

- Certain IP addresses are reserved for Oracle Cloud Infrastructure use and may not be used in your address numbering scheme. See IP Addresses Reserved for Use by Oracle on page 2754 for more information.
- Before you create a custom image of an instance, you must disconnect all iSCSI attachments and remove all iscsid node configurations from the instance. For steps, see Disconnecting From a Volume on page 562.
- When you create an image of a running instance, the instance shuts down and remains unavailable for several minutes. The instance restarts when the process completes.
- You cannot create additional custom images of an instance while the instance is engaged in the image creation process. When you start to create a custom image, the system implements a 20-minute timeout, during which you cannot create another image of the same instance. You can, however, create images of different instances at the same time.
- Custom images are available to all users authorized for the compartment in which the image was created.
- Custom images inherit the compatible shapes that are set by default from the base image.
- The maximum size for importing a custom image is 400 GB.
- The maximum size for custom exported images is 400 GB.
- You cannot create an image of an Oracle Database instance.
- If you use a custom image and update the OS kernel on your instance, you must also upload the update to the network drive. See OS Kernel Updates on page 691 for more information.

For information about how to deploy any version of any operating system that is supported by the Oracle Cloud Infrastructure hardware, see Bring Your Own Image (BYOI) on page 675.

X5 and X7 Compatibility for Custom Images

Oracle X5, X6, and X7 servers have different host hardware. As a result, using an X5 or X6 image on an X7 bare metal or virtual machine (VM) instance may not work without additional modifications. Oracle Cloud Infrastructure recommends for X7 hosts that you use the Oracle-provided images for X7. See Oracle-Provided Image Release Notes for more information about which images support X7. These images have been explicitly created and tested with X7 hardware.

If you attempt to use an existing X5 image on X7 hardware, note the following:

- No Windows versions are cross-compatible.
- Oracle Autonomous Linux 7 and Oracle Linux 8 are cross-compatible.
• Oracle Linux 6, Oracle Linux 7, Ubuntu 16.04, CentOS 7, and CentOS 8 are cross-compatible. However, you must update the kernel to the most recent version to install the latest device drivers. To do this, run the following commands from a terminal session:

  • Oracle Linux
    ```
yum update
    ```
  • CentOS 7, CentOS 8
    ```
yum update
    ```
  • Ubuntu 16.04
    ```
    apt-get update
    apt-get dist-upgrade
    ```

If you attempt to use an X6 image on non-X6 hardware, note the following:

• Oracle Linux 6, all CentOS versions, and all Windows versions are not cross-compatible.
• Oracle Autonomous Linux 7 and Oracle Linux 8 are cross-compatible.
• Oracle Linux 7, Ubuntu 18.04, and Ubuntu 16.04 are cross-compatible. Use the Oracle-provided images for X6.

The primary device drivers that are different between X5, X6, and X7 hosts are:

• Network device drivers
• NVMe drive device drivers
• GPU device drivers

Additional updates might be required depending on how you have customized the image.

**Using the Console**

**To create a custom image**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you want to use as the basis for the custom image.
3. Click **More Actions**, and then click **Create Custom Image**.
4. In the **Create in Compartment** list, select the compartment to create the custom image in.
5. Enter a **Name** for the image. You can change the name later, if needed. You cannot use the name of an Oracle-provided image for a custom image. Avoid entering confidential information.
6. **Show Tagging Options**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click **Create Custom Image**.

To track the progress of the operation, you can monitor the associated work request. For more information, see **Using the Console to View Work Requests** on page 260.

**Note:**

If you see a message indicating that you are at the limit for custom images, you must delete at least one image before you can create another. Or, you can request a service limit increase.

**To launch an instance from a custom image**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Custom Images**.
2. Click the custom image that you're interested in.
3. Click **Create Instance**.
4. Provide additional launch options as described in **Creating an Instance** on page 695.
To edit the name or compatible shapes for a custom image

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
2. Click the custom image that you're interested in.
3. Click Edit Details.
4. Edit the name, or add and remove compatible shapes for the custom image. Avoid entering confidential information.
5. To configure the minimum and maximum number of OCPUs that users can select when they use this image on a flexible shape, click the down arrow in the row for the shape, and then enter the minimum and maximum OCPU counts.
6. Click Save Changes.

**Note:**
After you add shape compatibility to an image, test the image on the shape to ensure that the image actually works on the shape. Some images (especially Windows) might never be cross-compatible with other shapes because of driver or hardware differences.

To manage tags for a custom image

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
2. Click the custom image that you're interested in.
3. Click the Tags tab to view or edit the existing tags. Or click More Actions, and then click Add tags to add new ones.

For more information, see Resource Tags on page 211.

To delete a custom image

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
2. Click the custom image that you're interested in.
3. Click More Actions, and then click Delete. Confirm when prompted.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage custom images:

- CreateImage
- GetImage
- ListImages
- UpdateImage
- DeleteImage
- AddImageShapeCompatibilityEntry
- ListImageShapeCompatibilityEntries
- GetImageShapeCompatibilityEntry
- RemoveImageShapeCompatibilityEntry

Creating Windows Custom Images

You can create a Windows custom image of a bare metal or virtual machine (VM) instance's boot disk and use it to launch other instances. Instances you launch from your image include the customizations, configuration, and software installed when you created the image. For information about custom images, see Managing Custom Images on page 665. For information about the licensing requirements for Windows images, see Microsoft Licensing on Oracle Cloud Infrastructure on page 803.
Windows supports two kinds of images: generalized and specialized. Generalized images are images that have been cleaned of instance-specific information. Specialized images are point-in-time snapshots of the boot disk of a running instance, and are useful for creating backups of an instance. Oracle Cloud Infrastructure supports bare metal and VM instances launched from both generalized and specialized custom Windows images.

**Generalized images**

A generalized image has a generalized OS disk, cleaned of computer-specific information. The images are generalized using Sysprep. Generalized images can be useful in scenarios such as quickly scaling an environment. Generalized images can be configured to preserve the existing opc user's account, including the password, at the time the image is created, or configured to recreate the opc user account, including generating a new, random password that you retrieve using the API. For background information, see [Sysprep (Generalize) a Windows installation](#).

**Specialized images**

A specialized image has an OS disk that is already fully installed, and is essentially a copy of the original bare metal or VM instance. Specialized images are intended to be used for backups so that you can recover from a failure. Specialized images are useful when you are testing a task and may need to roll back to known good configuration. Specialized images are not recommended for cloning multiple identical bare metal instances or VMs in the same network because of issues with multiple computers having the same computer name and ID. When creating a specialized image, you must remember the opc user's password; a new password is not generated when the instance launches, and it cannot be retrieved from the console or API.

**Creating a Generalized Image**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a generalized image from an instance will render the instance non-functional, so you should first create a custom image from the instance, and then launch a new instance from the custom image. Steps 1 - 2 describe how to do this. This is the instance that you'll generalize. Alternatively, you can make a backup image of the instance that you can use to launch a replacement instance if needed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you upgrade to PowerShell 5.0/WMF 5.0, you may encounter an issue where Sysprep fails which will prevent the image generalization process from completing. If this occurs, you may not be able to log into instances launched from the custom image. See <a href="#">Unable to log in to instance launched from new generalized Windows custom image</a> for more information and how to work around the issue.</td>
</tr>
</tbody>
</table>

1. Create the new image using [To create a custom image](#).
2. Launch an instance from the new image using [To launch an instance from a custom image](#).
3. Connect to the instance using a Remote Desktop client.
4. Go to [Windows Generalized Image Support Files](#) on page 831 and download to the instance the file matching the instance shape.
5. Right-click the file, and then click Run as administrator.
6. Extract the files to C:\Windows\Panther. The following files are extracted into the Panther folder for all Windows Server versions:
   - Generalize.cmd
   - Specialize.cmd
   - unattend.xml
   - Post-Generalize.ps1
7. Optional: If you want to preserve the opc user account, edit C:\Program Files\bmcs \imageType.json and change the imageType setting to custom. A new password is not created and the password is not retrievable from the console or API.

If you want to configure the generalized image to recreate the opc user account when a new instance is launched from the image, leave the imageType setting defaulted to general. The new account's password can be retrieved through the API using GetInstanceDefaultCredentials.

8. Right-click Generalize.cmd, and then click Run as administrator. Keep in mind the following outcomes of running this command:

   • Your connection to the Remote Desktop client might immediately be turned off and you will be logged out of the instance. If this does not occur, you should log out of the instance yourself.
   • Because sysprep generalize turns off Remote Desktop, you won't be able to log in to the instance again.
   • Creating a generalized image essentially destroys the instance's functionality.

   You should wait for a few minutes before proceeding to the following step to ensure the generalization process has completed.

9. Create the new image using To create a custom image.

10. After you create an image from an instance that has been generalized, we recommend that you terminate the instance. Although it may appear to be running, it won't be fully operable.

Creating a Specialized Image

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When creating a specialized image, you must remember the opc user's password. It cannot be retrieved from the Console or API.</td>
</tr>
</tbody>
</table>

You create a specialized image the same way you create other custom images. For steps, see Managing Custom Images on page 665.

Image Import/Export

Oracle Cloud Infrastructure Compute lets you share custom images across tenancies and regions using image import/export.

Linux-Based Operating Systems

The following operating systems support image import/export:

   • Oracle Linux 6.x
   • Oracle Linux 7.x
   • Oracle Linux 8.x
   • CentOS 7
   • CentOS 8
   • Ubuntu 16.04 and later

For more information about Oracle-provided platform images, see Oracle-Provided Images on page 629.

Windows-Based Operating Systems

The following Windows versions support image import/export:

   • Windows Server 2012 Standard, Datacenter
   • Windows Server 2012 R2 Standard, Datacenter
   • Windows Server 2016 Standard, Datacenter
   • Windows Server 2019 Standard, Datacenter
Note:
When exporting Windows-based images, you are responsible for complying with the Microsoft Product Terms and all product use conditions, as well as verifying your compliance with Microsoft.

For information about the licensing requirements for Windows images, see Microsoft Licensing on Oracle Cloud Infrastructure on page 803.

**Verify Your Windows Operating System**

When importing custom Windows images, ensure that the version you select matches the Windows image that you imported. Failure to provide the correct version and SKU information could be a violation of your Microsoft Licensing Agreement.

**Windows System Time Issue on Custom Windows Instances**

If you change the time zone from the default setting on Windows VM instances, when the instance reboots or syncs with the hardware clock, the system time will revert back to the time for the default time zone. However, the time zone setting will stay set to the new time zone, so the system clock will be incorrect. You can fix this by setting the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation registry key to 1.

Oracle-provided Windows images already have the RealTimeIsUniversal registry key set by default, but you must set this for any custom Windows images that you import.

To fix this issue for custom Windows images:

1. Open the Windows Registry Editor and navigate to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation registry key.
2. Create a new DWORD key named RealTimeIsUniversal and set the value to 1.
3. Reboot the instance.
4. Reset the time and time zone manually.

**Bring Your Own Image Scenarios**

You can also use image import/export to share custom images from Bring Your Own Image (BYOI) on page 675 scenarios across tenancies and regions, so you don't need to recreate the image manually in each region. You must go through the steps required to manually create the image in one of the regions, but after this is done, you can export the image, making it available for import in additional tenancies and regions. Export the image in the .oci format, which is a file format that contains a QCOW2 image file and Oracle Cloud Infrastructure-specific metadata.

**Best practices for replicating an image across regions**

You can replicate an image from one region to another region using the Console or API. At a high level:

1. Export the image to an Object Storage bucket in the same region as the image. For steps, see Exporting an Image on page 672.
2. Copy the image to an Object Storage bucket in the destination region. For steps, see Copying Objects on page 3487.
3. Obtain the URL path to the image object. For steps, see To view object details on page 3423.
4. In the destination region, import the image. Use the URL path as the Object Storage URL. For steps, see Importing an Image on page 673.

**Best practices for sharing an image across tenancies**

You can replicate an image from one tenancy to another tenancy using the Console or API. At a high level:

1. Export the image to an Object Storage bucket in the same region as the image. For steps, see Exporting an Image on page 672.
2. Create a pre-authenticated request with read-only access for the image in the destination region. For steps, see Working with Pre-Authenticated Requests on page 3483.
3. In the destination tenancy, import the image. Use the pre-authenticated request URL as the Object Storage URL. For steps, see Importing an Image on page 673.

Object Storage Service URLs
When you import or export custom images using the Console, you might need to specify the Object Storage URL pointing to the location that you want to import the image from or export the image to. Object Storage URLs are structured as follows:

https://<host_name>/n/<namespace_name>/b/<bucket_name>/o/<object_name>

For example:

https://objectstorage.us-phoenix-1.oraclecloud.com/n/MyNamespace/b/MyBucket/o/MyCustomImage.qcow2

Pre-Authenticated Requests
When using import/export across tenancies, you need to use an Object Storage pre-authenticated request. See Working with Pre-Authenticated Requests on page 3483 for steps to create a pre-authenticated request. When you go through these steps, after you click Create Pre-Authenticated Request, the Pre-Authenticated Request Details dialog box opens. You must make a copy of the pre-authenticated request URL displayed here, because this is the only time this URL is displayed. This is the Object Storage URL that you specify for import/export.

Note:

Pre-authenticated requests for a bucket

With image export, if you create the pre-authenticated request for a bucket, you need to append the object name to the generated URL. For example:

/o/MyCustomImage.qcow2

Exporting an Image
You can use the Console or API to export images, and the exported images are stored in the Oracle Cloud Infrastructure Object Storage service. To perform an image export, you need write access to the Object Storage bucket for the image. For more information, see Overview of Object Storage on page 3392 and Let users write objects to Object Storage buckets on page 2149.

To export an image using the Console
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
2. Click the custom image that you're interested in.
3. Click Export.
4. Specify the Object Storage location to export the image to:
   - **Export to an Object Storage bucket**: Select a bucket. Then, enter a name for the exported image. Avoid entering confidential information.
   - **Export to an Object Storage URL**: Enter the Object Storage URL.

5. In the **Image format** list, select the format that you want to export the image to. The following formats are available:
   - Oracle Cloud Infrastructure file with a QCOW2 image and OCI metadata (.oci). Use this format to export a custom image that you want to import into other tenancies or regions.
   - QEMU Copy On Write (.qcow2)
   - Virtual Disk Image (.vdi) for Oracle VM VirtualBox
   - Virtual Hard Disk (.vhd) for Hyper-V
   - Virtual Machine Disk (.vmdk)

6. Click **Export Image**.

After you click **Export Image**, the image state changes to **Exporting**. You can still launch instances while the image is exporting, but you can't delete the image until the export has finished. To track the progress of the operation, you can monitor the associated work request. For more information, see **Using the Console to View Work Requests** on page 260.

When the export is complete, the image state changes to **Available**. If the image state changes to **Available**, but you don't see the exported image in the Object Storage location you specified, this means that the export failed, and you will need to go through the steps again to export the image.

**Importing an Image**

You can use the Console or API to import exported images from Object Storage. To import an image, you need read access to the Object Storage object containing the image. For more information, see **Let users download objects from Object Storage buckets** on page 2149.

**To import an image using the Console**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Custom Images**.
2. Click **Import Image**.
3. In the **Create in Compartment** list, select the compartment that you want to import the image to.
4. Enter a **Name** for the image. Avoid entering confidential information.
5. Select the **Operating System**:
   - For Linux images, select **Linux**.
   - For Windows images, select **Windows**. Select the **Operating System Version**, and then certify that the selected operating system complies with Microsoft licensing agreements.
6. Specify the **Object Storage location** to import the image from:
   - **Import from an Object Storage bucket**: Select the **Bucket** that contains the image. In the **Object Name** list, select the image file.
   - **Import from an Object Storage URL**: Enter the **Object Storage URL** of the image. When importing across tenancies, you must specify a pre-authenticated request URL.
7. In the **Image Type** section, select the format of the image.
8. **Select the Launch Mode:**

- For custom images where the image type is `.oci`, the launch mode is disabled. Oracle Cloud Infrastructure selects the appropriate launch mode based on the launch mode for the source image.
- For custom images exported from Oracle Cloud Infrastructure where the image type is QCOW2, select **Native Mode**.
- To import other custom images, select **Paravirtualized Mode** or **Emulated Mode**. For more information, see *Bring Your Own Image (BYOI)* on page 675.

9. **Show Tagging Options:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see *Resource Tags* on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

10. **Click Import Image.**

After you click **Import Image**, you'll see the imported image in the **Custom Images** list for the compartment, with a state of **Importing**. To track the progress of the operation, you can monitor the associated work request. For more information, see *Using the Console to View Work Requests* on page 260.

When the import completes successfully, the state changes to **Available**. If the state does not change, or no entry appears in the **Custom Images** list, the import failed. If the import failed, ensure you have read access to the Object Storage object, and that the object contains a supported image.

**Editing Image Details**

You can edit the details of custom images, such as the image name and compatible shapes for the image. For more information, see *To edit the name or compatible shapes for a custom image* on page 668 in *Managing Custom Images* on page 665.

**Managing Tags for an Image**

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see *Resource Tags* on page 211.

**To manage tags for an image**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Custom Images**.
2. Click the image that you're interested in.
3. Click the **Tags** tab to view or edit the existing tags. Or click **More Actions**, and then click **Add tags** to add new ones.

**Using the API**

For information about using the API and signing requests, see *REST APIs* on page 4368 and *Security Credentials* on page 179. For information about SDKs, see *Software Development Kits and Command Line Interface* on page 4225.

Use the following API operations for custom image import/export:

- **ExportImage**: Exports a custom image to Object Storage.
- **CreateImage**: To import an exported image, specify **ImageSourceDetails** in the request body.
- **AddImageShapeCompatibilityEntry**: Adds a shape to the compatible shapes list for the image.
- **ListImageShapeCompatibilityEntries**
- **GetImageShapeCompatibilityEntry**
- **RemoveImageShape CompatibilityEntry**: Removes a shape from the compatible shapes list for the image.

**X5 and X7 Compatibility for Image Import/Export**

Oracle X5, X6, and X7 servers have different host hardware. As a result, using an X5 or X6 image on an X7 bare metal or virtual machine (VM) instance may not work without additional modifications. Oracle Cloud Infrastructure
recommends for X7 hosts that you use the Oracle-provided images for X7. See Oracle-Provided Image Release Notes for more information about which images support X7. These images have been explicitly created and tested with X7 hardware.

If you attempt to use an existing X5 image on X7 hardware, note the following:

- No Windows versions are cross-compatible.
- Oracle Autonomous Linux 7 and Oracle Linux 8 are cross-compatible.
- Oracle Linux 6, Oracle Linux 7, Ubuntu 16.04, CentOS 7, and CentOS 8 are cross-compatible. However, you must update the kernel to the most recent version to install the latest device drivers. To do this, run the following commands from a terminal session:
  - **Oracle Linux**
    ```
    yum update
    ```
  - **CentOS 7, CentOS 8**
    ```
    yum update
    ```
  - **Ubuntu 16.04**
    ```
    apt-get update
    apt-get dist-upgrade
    ```

If you attempt to use an X6 image on non-X6 hardware, note the following:

- Oracle Linux 6, all CentOS versions, and all Windows versions are not cross-compatible.
- Oracle Autonomous Linux 7 and Oracle Linux 8 are cross-compatible.
- Oracle Linux 7, Ubuntu 18.04, and Ubuntu 16.04 are cross-compatible. Use the Oracle-provided images for X6.

The primary device drivers that are different between X5, X6, and X7 hosts are:

- Network device drivers
- NVMe drive device drivers
- GPU device drivers

Additional updates might be required depending on how you have customized the image.

**Bring Your Own Image (BYOI)**

The Bring Your Own Image (BYOI) feature enables you to bring your own versions of operating systems to the cloud as long as the underlying hardware supports it. The services do not depend on the OS you run.

The BYOI feature does the following things:

- Enables virtual machine cloud migration projects.
- Supports both old and new operating systems.
- Encourages experimentation.
- Increases infrastructure flexibility.

**Note:**

Licensing Requirements

You must comply with all licensing requirements when you upload and start instances based on OS images that you supply.
Bringing Your Own Image

A critical part of any lift-and-shift cloud migration project is the migration of on-premises virtual machines (VMs) to the cloud. You can import your on-premises virtualized root volumes to Oracle Cloud Infrastructure using the custom image import feature, and then launch Compute instances using those images.

You can import Windows and Linux-based custom images and use them to launch VMs on Oracle Cloud Infrastructure. Bringing your own image to a bare metal instance is not supported.

- **Windows images**

  These Windows versions support custom image import:
  - Windows Server 2008 R2 Standard, Enterprise, Datacenter
  - Windows Server 2012 Standard, Datacenter
  - Windows Server 2012 R2 Standard, Datacenter
  - Windows Server 2016 Standard, Datacenter
  - Windows Server 2019 Standard, Datacenter

  For steps to import a Windows image, see Importing Custom Windows Images on page 677.

  Bring your own license (BYOL) for Windows Server is not permitted when launching a VM instance on a shared host. For more information about BYOL and the licensing requirements for Windows images, see Licensing Options for Microsoft Windows on page 809 and Microsoft Licensing on Oracle Cloud Infrastructure on page 803.

- **Linux images**

  These Linux distributions support custom image import:

<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Supported Versions</th>
<th>Preferred Launch Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>7 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>4.0, 4.8, 5.11, 6.9</td>
<td>Emulated</td>
</tr>
<tr>
<td>Debian</td>
<td>8 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>5.0.10, 6.0, 7</td>
<td>Emulated</td>
</tr>
<tr>
<td>Flatcar Container Linux</td>
<td>2345.3.0 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>8, 9, 10, 11, 12 or later</td>
<td>Emulated</td>
</tr>
<tr>
<td>openSUSE Leap</td>
<td>15.1</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td>Oracle Linux</td>
<td>7.x, 8.x</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>5.11, 6.x</td>
<td>Emulated</td>
</tr>
<tr>
<td>RHEL</td>
<td>7 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>4.5, 5.5, 5.6, 5.9, 5.11, 6.5, 6.9</td>
<td>Emulated</td>
</tr>
<tr>
<td>SUSE</td>
<td>12.2 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>11, 12.1</td>
<td>Emulated</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>13.04 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>12.04</td>
<td>Emulated</td>
</tr>
</tbody>
</table>

  You might also have success importing other distributions of Linux.

  For steps to import a Linux-based image, see Importing Custom Linux Images on page 682.
Bringing Your Own Hypervisor Guest OS

You can bring your own hypervisor guest OS using Kernel-based Virtual Machine (KVM) or Hyper-V.

**Note:**

Bring your own hypervisor deployment of ESXi on bare metal Compute instances is not supported. ESXi is supported only by provisioning an Oracle Cloud VMware Solution software-defined data center (SDDC). See Oracle Cloud VMware Solution on page 4026 for more information.

Bringing Your Own KVM

You can bring your own operating system images or older operating systems, such as Ubuntu 6.x, RHEL 3.x, and CentOS 5.4, using KVM on bare metal instances.

To bring your own KVM, first create a bare metal instance using the KVM image from Marketplace. Then, copy your on-premises guest OS to KVM on the bare metal instance.

For more information, see the following resources:

- Getting Started: Oracle Linux KVM Image for Oracle Cloud Infrastructure
- Installing and Configuring KVM on Bare Metal Instances with Multi-VNIC

Bringing Your Own Hyper-V

You can bring your own operating system images or older operating systems, such as Windows Server 2003 and Windows Server 2008, using Hyper-V on bare metal instances.

To bring your own Hyper-V, first create a bare metal instance using the Oracle-provided Windows Server Datacenter platform image. Oracle Cloud Infrastructure will issue a license for Windows Server when the instance is launched. Then, copy your on-premises guest OS to Hyper-V on the bare metal instance. No additional license is required because Windows Server Datacenter includes unlimited virtual machines.

Be aware of the following considerations:

- Oracle Cloud Infrastructure will issue a license when you launch an instance using a custom image. If you want to bring your own license (BYOL) for Windows Server, you must activate Windows Server with your own license. For steps, see Activating Licenses on a Dedicated Host on page 811.
- Importing your own ISO image is not supported.

For a list of supported Hyper-V guests, see the following resources:

- Supported Windows guest operating systems for Hyper-V on Windows Server
- Supported Linux and FreeBSD virtual machines for Hyper-V on Windows

For more information about deploying Hyper-V, see Deploying Hyper-V on Oracle Cloud Infrastructure.

Importing Custom Windows Images

The Compute service enables you to import Windows images that were created outside of Oracle Cloud Infrastructure. For example, you can import images running on your on-premises physical or virtual machines (VMs), or VMs running in Oracle Cloud Infrastructure Classic. You can then launch your imported images on Compute virtual machines.

For information about the licensing requirements for Windows images, see Microsoft Licensing on Oracle Cloud Infrastructure on page 803.

**Supported Operating Systems**

These Windows versions support custom image import:

- Windows Server 2008 R2 Standard, Enterprise, Datacenter
- Windows Server 2012 Standard, Datacenter
• Windows Server 2012 R2 Standard, Datacenter
• Windows Server 2016 Standard, Datacenter
• Windows Server 2019 Standard, Datacenter

Note:
• Oracle Cloud Infrastructure has tested the operating systems listed previously and will support customers in ensuring that instances launched from these images and built according to the guidelines in this topic are accessible using RDP.
• For OS editions not listed previously, Oracle Cloud Infrastructure will provide commercially reasonable support to customers in an effort to get instances that are launched from these images accessible via RDP.
• Support from Oracle Cloud Infrastructure in launching an instance from a custom OS does not ensure that the operating system vendor also supports the instance.
• Oracle Cloud Infrastructure licenses and charges the Windows licensing fee for all instances launched using an imported Windows OS image. This applies whether or not those instances are registered with Oracle Cloud Infrastructure’s Microsoft Key Management service.
• The Oracle Cloud Agent (used for monitoring) is not supported on Windows Server 2008 R2.

Windows Source Image Requirements

Custom images must meet the following requirements:
• The maximum image size is 400 GB.
• The image must be set up for BIOS boot.
• Only one disk is supported, and it must be the boot drive with a valid master boot record (MBR) and boot loader. You can migrate additional data volumes after you import the image’s boot volume.
• The minimum boot volume size is 256 GB. For more information, see Custom Boot Volume Sizes on page 610.
• The boot process must not require additional data volumes to be present for a successful boot.
• The disk image cannot be encrypted.
• The disk image must be a VMDK or QCOW2 file.
  • Create the image file by cloning the source volume, not by creating a snapshot.
  • VMDK files must be either the "single growable" (monolithicSparse) type or the "stream optimized" (streamOptimized) type, both of which consist of a single VMDK file. All other VMDK formats, such as those that use multiple files, split volumes, or contain snapshots, are not supported.
• The network interface must use DHCP to discover the network settings. When you import a custom image, existing network interfaces are not recreated. Any existing network interfaces are replaced with a single NIC after the import process is complete. You can attach additional VNICs after you launch the imported instance.
• The network configuration must not hardcode the MAC address for the network interface.

Preparing Windows VMs for Import

Before you can import a custom Windows image, you must prepare the image to ensure that instances launched from the image can boot correctly and that network connections will work.

You can perform the tasks described in this section on the running source system. If you have concerns about modifying the live source system, you can export the image as-is, import it into Oracle Cloud Infrastructure, and then launch an instance based on the custom image. You can then connect to the instance using the VNC console and perform the preparation steps.
Important:

The system drive where Windows is installed will be imported to Oracle Cloud Infrastructure. All partitions on the drive will follow through the imported image. Any other drives will not be imported and you must recreate them on the instance after import. You will then need to manually move the data on the non-system drives.

To prepare a Windows VM for import:

1. Follow your organization’s security guidelines to ensure that the Windows system is secured. This can include, but is not limited to the following tasks:
   - Install the latest security updates for the operating system and installed applications.
   - Enable the firewall, and configure it so that you only enable the rules which are needed.
   - Disable unnecessary privileged accounts.
   - Use strong passwords for all accounts.
2. Configure Remote Desktop Protocol (RDP) access to the image:
   a. Enable Remote Desktop connections to the image.
   b. Modify the Windows Firewall inbound port rule to allow RDP access for both Private and Public network location types. When you import the image, the Windows Network Location Awareness service will identify the network connection as a Public network type.
3. Determine whether the current Windows license type is a volume license by running the following command in PowerShell:
   ```powershell
   Get-CimInstance -ClassName SoftwareLicensingProduct | where {$_._PartialProductKey} | select ProductKeyChannel
   ```
   If the license is not a volume license, after you import the image, you will update the license type.
4. If you plan to launch the imported image on more than one VM instance, create a generalized image of the boot disk. A generalized image is cleaned of computer-specific information, such as unique identifiers. When you create instances from a generalized image, the unique identifiers are regenerated. This prevents two instances that are created from the same image from colliding on the same identifiers.
5. Create a backup of the root volume.
6. If the VM has remotely attached storage, such as NFS or block volumes, configure any services that rely on this storage to start manually. Remotely attached storage is not available the first time that an imported instance boots on Oracle Cloud Infrastructure.
7. Ensure that all network interfaces use DHCP, and that the MAC address and IP addresses are not hardcoded. See your system documentation for steps to perform network configuration for your system.
8. Download the Oracle Windows VirtIO drivers:
   a. Sign in to the Oracle Software Delivery Cloud site.
   b. In the All Categories list, select Release.
   c. Type Oracle Linux 7.7 in the search box and click Search.
   d. Add REL: Oracle Linux 7.7.x to your cart, and then click Continue.
   e. In the Platforms/Languages list, select x86 64 bit. Click Continue.
   f. Accept the license agreement and then click Continue.
   g. Select the check box next to Oracle VirtIO Drivers Version for Microsoft Windows 1.1.5. Clear the other check boxes.
   h. Click Download and then follow the prompts.
9. Install the Oracle VirtIO drivers for Windows:
   a. Follow the prompts in the installation wizard. On the Installation Type page, select Custom, as shown in the following screenshot.
   ![Drivers Installer](image)
   b. Reboot the VM.
10. Stop the VM.
11. Clone the stopped VM as a VMDK or QCOW2 file, and then export the image from your virtualization environment. See the tools documentation for your virtualization environment for steps.

**Importing a Windows-Based VM**

After you prepare a Windows image for import, follow these steps to import the image:

1. **Upload the image file to an Object Storage bucket.** You can upload the file using the Console or using the command line interface (CLI). If you use the CLI, use the following command:
   ```bash
   oci os object put -bn <destination_bucket_name> --file <path_to_the_VMDK_or_QCOW2_file>
   ```
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
3. Click Import Image.
4. In the Create in Compartment list, select the compartment that you want to import the image to.
5. Enter a Name for the image. Avoid entering confidential information.
6. For the Operating System, select Windows.
7. In the Operating System Version list, select the version of Windows.
8. Confirm that you chose the operating system version that complies with your Microsoft licensing agreement, and then select the compliance check box.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to provide the correct version and SKU information could be a violation of your Microsoft Licensing Agreement.</td>
</tr>
</tbody>
</table>

9. Select the Import from an Object Storage bucket option.
10. Select the Bucket that you uploaded the image to.
11. In the Object Name list, select the image file that you uploaded.
12. For the Image Type, select the file type of the image, either VMDK or QCOW2.
13. In the Launch Mode area, select Paravirtualized Mode.
14. Show Tagging Options: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
15. Click Import Image.

The imported image appears in the Custom Images list for the compartment, with a state of Importing. When the import completes successfully, the state changes to Available.

If the state doesn't change, or no entry appears in the Custom Images list, the import failed. Ensure that you have read access to the Object Storage object, and that the object contains a supported image.


**Post-Import Tasks for Windows Images**

After you import a custom Windows-based image, do the following:

1. If you want to use the image on AMD or X6-based shapes, add the shapes to the image's list of compatible shapes.
2. Create an instance based on the custom image. For the image source, select Custom Images, and then select the image that you imported.
3. Enable Remote Desktop Protocol (RDP) access to the Compute instance.
4. Connect to the instance using RDP.
5. If the instance requires any remotely attached storage, such as block volumes or file storage, create and attach it.
6. Create and attach any required secondary VNICs.
7. Test that all applications are working as expected.
8. Reset any services that were set to start manually.
9. Register the instance with the Oracle-provided Key Management Service (KMS) server:

   a. On the instance, open PowerShell as Administrator.

   b. To set the KMS endpoint, run the following command:

```
slmgr /skms 169.254.169.253:1688
```

   c. If the Windows license type that you noted while preparing the image isn't a volume license, you must update the license type. Run the following command:

```
slmgr /ipk <setup key>
```

   <setup key> is the KMS client setup key that corresponds to the version of Windows that you imported:

<table>
<thead>
<tr>
<th>Windows Version</th>
<th>KMS Client Setup Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2 Standard</td>
<td>YC6KT-GKW9T-YTKYR-T4X34-R7VHC</td>
</tr>
<tr>
<td>Windows Server 2008 R2 Enterprise</td>
<td>489J6-VHDMP-X63PK-3K798-CPX3Y</td>
</tr>
<tr>
<td>Windows Server 2008 R2 Datacenter</td>
<td>74YFP-3QFB3-KQT8W-PMXWJ-7M648</td>
</tr>
<tr>
<td>Windows Server 2012 Standard</td>
<td>XC9B7-NBPP2-83J2H-RHMBY-92BT4</td>
</tr>
<tr>
<td>Windows Server 2012 Datacenter</td>
<td>48HP8-DN98B-MYWDG-T2DCC-8W83P</td>
</tr>
<tr>
<td>Windows Server 2012 R2 Standard</td>
<td>D2N9P-3P6X9-2R39C-7RTCD-MDVIJX</td>
</tr>
<tr>
<td>Windows Server 2012 R2 Datacenter</td>
<td>W3GGN-FT8W3-Y4M27-J84CP-Q3VJ9</td>
</tr>
<tr>
<td>Windows Server 2016 Standard</td>
<td>WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY</td>
</tr>
<tr>
<td>Windows Server 2016 Datacenter</td>
<td>CB7KF-BWN84-R7R2Y-793K2-8XDDG</td>
</tr>
<tr>
<td>Windows Server 2019 Standard</td>
<td>N69G4-B89J2-4G8F4-WWYCC-J464C</td>
</tr>
<tr>
<td>Windows Server 2019 Datacenter</td>
<td>WMDGN-G9PQG-XVVXX-R3X43-63DFG</td>
</tr>
</tbody>
</table>

   d. To activate Windows, run the following command:

```
slmgr /ato
```

   e. To verify the license status, run the following command:

```
Get-CimInstance -ClassName SoftwareLicensingProduct | where ($_.PartialProductKey) | select Description, LicenseStatus
```

If the LicenseStatus is 1, the instance is properly licensed. It might take up to 48 hours for the license status to update.

**Importing Custom Linux Images**

The Compute service lets you import Linux-based images that were created outside of Oracle Cloud Infrastructure. For example, you can import images running on your on-premises physical or virtual machines (VMs), or VMs running in Oracle Cloud Infrastructure Classic. You can then launch your imported images on Compute virtual machines.

**Supported Operating Systems**

You can launch imported Linux VMs in either paravirtualized mode or emulated mode. On AMD shapes, imported images are supported in paravirtualized mode only.

Paravirtualized mode offers better performance than emulated mode. We recommend that you use paravirtualized mode if your OS supports it. Linux-based operating systems running the kernel version 3.4 or later support paravirtualized drivers. You can verify your system's kernel version using the `uname` command.
To verify the kernel version using the `uname` command

Run the following command:

```
uname -a
```

The output should look similar to this sample:

```
Linux ip_bash 4.14.35-1818.2.1.el7uek.x86_64 #2 SMP Mon Aug 27 21:16:31 PDT 2018 x86_64 x86_64 x86_64 GNU/Linux
```

The kernel version is the number at the first part of the output string. In the sample output shown previously, the version is 4.14.35.

Linux Distributions that Support Custom Image Import

These Linux distributions support custom image import:

<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Supported Versions</th>
<th>Preferred Launch Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>7 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>4.0, 4.8, 5.11, 6.9</td>
<td>Emulated</td>
</tr>
<tr>
<td>Debian</td>
<td>8 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>5.0.10, 6.0, 7</td>
<td>Emulated</td>
</tr>
<tr>
<td>Flatcar Container Linux</td>
<td>2345.3.0 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>8, 9, 10, 11, 12 or later</td>
<td>Emulated</td>
</tr>
<tr>
<td>openSUSE Leap</td>
<td>15.1</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td>Oracle Linux</td>
<td>7.x, 8.x</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>5.11, 6.x</td>
<td>Emulated</td>
</tr>
<tr>
<td>RHEL</td>
<td>7 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>4.5, 5.5, 5.6, 5.9, 5.11, 6.5, 6.9</td>
<td>Emulated</td>
</tr>
<tr>
<td>SUSE</td>
<td>12.2 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>11, 12.1</td>
<td>Emulated</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>13.04 or later</td>
<td>Paravirtualized</td>
</tr>
<tr>
<td></td>
<td>12.04</td>
<td>Emulated</td>
</tr>
</tbody>
</table>

Note:

- Oracle Cloud Infrastructure has tested the operating systems listed in the previous table and will support customers in ensuring that instances launched from these images and built according to the guidelines in this topic are accessible using SSH.
- For any OS version other than those covered by an official support service from Oracle (for example, Oracle Linux with Premier Support), Oracle Cloud Infrastructure will provide commercially reasonable support limited to getting an instance launched and accessible via SSH.
- Support from Oracle Cloud Infrastructure in launching an instance from a custom OS does not ensure that the operating system vendor also
Compute

supports the instance. Customers running Oracle Linux on Oracle Cloud Infrastructure automatically have access to Oracle Linux Premier Support.

Tip:
If your image supports paravirtualized drivers, you can convert your existing emulated mode instances into paravirtualized instances. Create a custom image of your instance, export it to Object Storage, and then reimport it using paravirtualized mode.

Linux Source Image Requirements

Custom images must meet the following requirements:

- The maximum image size is 400 GB.
- The image must be set up for BIOS boot.
- Only one disk is supported, and it must be the boot drive with a valid master boot record (MBR) and boot loader. You can migrate additional data volumes after you import the image's boot volume.
- The boot process must not require additional data volumes to be present for a successful boot.
- The boot loader should use LVM or a UUID to locate the boot volume.
- The disk image cannot be encrypted.
- The disk image must be a VMDK or QCOW2 file.
  - Create the image file by cloning the source volume, not by creating a snapshot.
  - VMDK files must be either the "single growable" (monolithicSparse) type or the "stream optimized" (streamOptimized) type, both of which consist of a single VMDK file. All other VMDK formats, such as those that use multiple files, split volumes, or contain snapshots, are not supported.
- The network interface must use DHCP to discover the network settings. When you import a custom image, existing network interfaces are not recreated. Any existing network interfaces are replaced with a single NIC after the import process is complete. You can attach additional VNICs after you launch the imported instance.
- The network configuration must not hardcode the MAC address for the network interface.

We recommend that you enable certificate-based SSH, however this is optional. If you want your image to automatically use SSH keys supplied from the User Data field when you launch an instance, you can install cloud-init when preparing the image. See Creating an Instance on page 695 for more information about providing user data.

Preparing Linux VMs for Import

Before you import a custom Linux image, you must prepare the image to ensure that instances launched from the image can boot correctly and that network connections will work. Do the following:

1. Optionally, configure your Linux image to support serial console connections. A console connection can help you remotely troubleshoot malfunctioning instances, such as an imported image that does not complete a successful boot.
2. Create a backup of the root volume.
3. If the VM has remotely attached storage, such as NFS or block volumes, configure any services that rely on this storage to start manually. Remotely attached storage is not available the first time that an imported instance boots on Oracle Cloud Infrastructure.
4. Ensure that all network interfaces use DHCP, and that the MAC address and IP addresses are not hardcoded. See your system documentation for steps to perform network configuration for your system.
5. Stop the VM.
6. Clone the stopped VM as a VMDK or QCOW2 file, and then export the image from your virtualization environment. See the tools documentation for your virtualization environment for steps.

Importing a Linux-Based VM

After you prepare a Linux image for import, follow these steps to import the image:
1. **Upload the image file to an Object Storage bucket.** You can upload the file using the Console or using the command line interface (CLI). If you use the CLI, use the following command:

```
oci os object put -bn <destination_bucket_name> --file <path_to_the_VMDK_or_QCOW2_file>
```

2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Custom Images**.

3. Click **Import Image**.

4. In the **Create in Compartment** list, select the compartment that you want to import the image to.

5. Enter a **Name** for the image. Avoid entering confidential information.

6. For the **Operating System**, select **Linux**.

7. Select the **Import from an Object Storage bucket** option.

8. Select the **Bucket** that you uploaded the image to.

9. In the **Object Name** list, select the image file that you uploaded.

10. For the **Image Type**, select the file type of the image, either **VMDK** or **QCOW2**.

11. Depending on your image's version of Linux, in the **Launch Mode** area, select **Paravirtualized Mode** or **Emulated Mode**. If your image supports paravirtualized drivers, we recommend that you select paravirtualized mode.

12. **Show Tagging Options:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

13. Click **Import Image**.

The imported image appears in the **Custom Images** list for the compartment, with a state of **Importing**. When the import completes successfully, the state changes to **Available**.

If the state doesn’t change, or no entry appears in the **Custom Images** list, the import failed. Ensure that you have read access to the Object Storage object, and that the object contains a supported image.


### Post-Import Tasks for Linux Images

After you import a custom Linux-based image, do the following:

1. If you want to use the image on AMD or X6-based **shapes**, add the shapes to the image's list of compatible shapes.
2. **Create an instance based on the custom image.** For the image source, select **Custom Images**, and then select the image that you imported.
3. **Connect to the instance using SSH.**
4. If the instance requires any remotely attached storage, such as **block volumes** or **file storage**, create and attach it. If you are using **iSCSI** on page 501 attachments, see **Recommended iSCSI Initiator Parameters for Linux-based Images** on page 506.
5. **Create and attach any required secondary VNICS.**
6. Test that all applications are working as expected.
7. Reset any services that were set to start manually.
8. If you enabled serial console access to the image, test it by creating a serial console connection to the instance.

See the **current issues and workarounds** for known issues with imported custom images.

### Enabling Serial Console Access for Imported Linux Images

You can configure your custom Linux image to support connections using the serial console feature in the Compute service.

For more information about serial console connections, and steps to troubleshoot if your image has network connectivity issues after it is launched, see **Troubleshooting Instances Using Instance Console Connections** on page 813.
The serial console connection in Oracle Cloud Infrastructure uses the first serial port, ttyS0, on the VM. The boot loader and the operating system should be configured to use ttyS0 as a console terminal for both input and output.

**Configuring the Boot Loader**

The steps to configure the boot loader to use ttyS0 as a console terminal for both input and output depend on the GRUB version. Run the following command on the operating system to determine the GRUB version:

```
grub install --version
```

If the version number returned is 2.x, use the steps for GRUB 2. For earlier versions, use the steps for GRUB.

**To configure GRUB2**

1. Run the following command to modify the GRUB configuration file:

   ```
sudo vi /etc/default/grub
```

2. Confirm that the configuration file contains the following:

   ```
GRUB_SERIAL_COMMAND="serial --unit=0 --speed=115200"
GRUB_TERMINAL="serial console"
```

3. Append the following to the end of the `GRUB_CMDLINE_LINUX` line:

   ```
console=tty1 console=ttyS0,115200
```

   If `GRUB_CMDLINE_LINUX` does not exist, create this line, using `GRUB_CMDLINE_OUTPUT` as a template.

4. Regenerate the GRUB2 configuration using the following command:

   ```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

   If you have a beta version of GRUB 2, use this command instead:

   ```
sudo grub-mkconfig -o /boot/grub/grub.cfg
```

**To configure GRUB**

1. Run the following command to modify the GRUB configuration file:

   ```
sudo vi /boot/grub/grub.conf
```

2. Add following after the line containing `timeout`:

   ```
serial --unit=0 --speed=115200
terminal --timeout=5 serial console
```

3. Append the following to each `kernel` line:

   ```
console=tty1 console=ttyS0,115200
```

**Configuring the Operating System**

The operating system may already be configured to usettyS0 as a console terminal for both input and output. To verify, run the following command:

```
sudo vi /etc/securetty
```

Check the file for `ttyS0`. If you don't see it, append `ttyS0` to the end of the file.
Validating Serial Console Access

After completing the steps to enable serial console access to the image, you should validate that serial console access is working by testing the image with serial console in your virtualization environment. Consult the documentation for your virtualization environment for steps to do this. Verify that the boot output displays in the serial console output and that there is interactive input after the image has booted.

Troubleshooting the Serial Console

If no output is displayed on the serial console, verify in the configuration for your virtualization environment that the serial console device is attached to the first serial port.

If the serial console displays output, but there is no interactive input available, check that there is a terminal process listening on the ttyS0 port. To do this, run the following command:

```
ps aux | grep ttyS0
```

This command should output a terminal process that is listening on the ttyS0 port. For example, if your system is using getty, you will see the following output:

```
/sbin/getty ttyS0
```

If you don't see this output, it is likely that a login process is not configured for the serial console connection. To resolve this, enable the init settings, so that a terminal process is listening on the ttyS0 at startup.

For example, if your system is using getty, add the following command to the init settings to run on system startup:

```
getty -L 9600 ttyS0 vt102
```

The steps to do this will vary depending on the operating system, so consult the documentation for the image's operating system.

Configuring Image Capabilities for Custom Images

Image capabilities are the configuration options available when launching an instance from an image. Some image capability examples are the firmware used to boot the instance, the volume attachment types supported, and so on. The full set of image capabilities provided by Oracle Cloud Infrastructure Compute are defined in the global image capability schema. You can also create your own custom image capability schemas based on the global image capability schema to specify and configure image capabilities for your custom images. Using these schemas, you can customize the image configuration and options available when users launch instances from your custom images.

You can configure image capability schemas using the REST APIs, SDKs, or the CLI.

**Caution:**

Using this feature allows you to customize image capabilities from the default capabilities that Oracle recommends and should be used for advanced custom image scenarios only. Ensure that you understand the optimal configuration options for your custom image.

Global Image Capability Schema

The following JSON is what's returned when you use the GetComputeGlobalImageCapabilitySchemaVersion API operation or the `global-image-capability-schema-version` CLI command. It represents the full set of image capabilities available for images. The default values specified for each element are the recommended values for each option. You can create a schema to customize these options, however they must be a subset, you cannot specify values that are not included in the global capabilities schema.
"Compute.Firmware": {
  "descriptorType": "enumstring",
  "values": [
    "BIOS",
    "UEFI_64"
  ],
  "defaultValue": "UEFI_64"
},
"Compute.LaunchMode": {
  "descriptorType": "enumstring",
  "values": [
    "NATIVE",
    "EMULATED",
    "PARAVIRTUALIZED",
    "CUSTOM"
  ],
  "defaultValue": "PARAVIRTUALIZED"
},
"Network.AttachmentType": {
  "descriptorType": "enumstring",
  "values": [
    "E1000",
    "VFIO",
    "PARAVIRTUALIZED"
  ],
  "defaultValue": "PARAVIRTUALIZED"
},
"Storage.BootVolumeType": {
  "descriptorType": "enumstring",
  "values": [
    "ISCSI",
    "SCSI",
    "IDE",
    "PARAVIRTUALIZED"
  ],
  "defaultValue": "PARAVIRTUALIZED"
},
"Storage.LocalDataVolumeType": {
  "descriptorType": "enumstring",
  "values": [
    "ISCSI",
    "SCSI",
    "IDE",
    "PARAVIRTUALIZED"
  ],
  "defaultValue": "PARAVIRTUALIZED"
},
"Storage.RemoteDataVolumeType": {
  "descriptorType": "enumstring",
  "values": [
    "ISCSI",
    "SCSI",
    "IDE",
    "PARAVIRTUALIZED"
  ],
  "defaultValue": "PARAVIRTUALIZED"
},
"Storage.ConsistentVolumeNaming": {
  "descriptorType": "boolean",
  "defaultValue": "true"
},
"Storage.ParaVirtualization.EncryptionInTransit": {
  "descriptorType": "boolean",
  "defaultValue": "true"
Compute

},
"Storage.ParaVirtualization.AttachmentVersion": {
  "descriptorType": "enuminteger",
  "values": [
    1,
    2
  ],
  "defaultValue": 2
}

Schema Elements

The following list describes all the available elements in the global image capabilities schema.

- **Compute.Firmware**: The firmware used to boot the virtual machine instance. The default value is UEFI_64.
- **Compute.LaunchMode**: The configuration mode for launching instances. The default value is PARAVIRTUALIZED.
- **Network.AttachmentType**: The emulation type for the primary VNIC, which is automatically created and attached when the instance is launched. The default value is PARAVIRTUALIZED.
- **Storage.BootVolumeType**: Specifies the driver options for the image's boot volume. The default value is PARAVIRTUALIZED.
- **Storage.LocalDataVolumeType**: Specifies the driver options for the image to access local storage volumes. The default value is PARAVIRTUALIZED.
- **Storage.RemoteDataVolumeType**: Specifies the driver options for the image to access remote storage volumes. The default value is PARAVIRTUALIZED.
- **Storage.ConsistentVolumeNaming**: Specifies whether consistent device paths for iSCSI and paravirtualized attached block volumes are enabled for the image. If enabled, the image must support consistent device names. The default value is true.
- **Storage.ParaVirtualization.EncryptionInTransit**: Specifies whether in-transit encryption is enabled for the image's boot volume attachment. Applies only to paravirtualized boot volume attachments. The default value is true.
- **Storage.ParaVirtualization.AttachmentVersion**: Specifies the paravirtualization version for boot volume and block volume attachments. Applies only to paravirtualized volume attachments. The default value is 2.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

For administrators, the following policy provides full access to the image capability schema framework:

```
Allow group IAM_group_name to manage compute-image-capability-schema in tenancy
```

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
2. Click the custom image that you're interested in.
3. Click Edit Image Capabilities.
4. Edit the image capabilities you want to configure. See Schema Elements on page 689 for details about the image capabilities you can configure.
5. Click **Save Changes**.

### Using the CLI

For information about using the CLI, see [Command Line Interface (CLI)](page 4192). To work with image capability schemas using the CLI, open a command prompt and run any of the following commands.

To list out the global image capability schema:

```
oci compute global-image-capability-schema list
```

To list out the global image capability schema versions:

```
oci compute global-image-capability-schema-version list --global-image-capability-schema-id <GLOBAL_IMAGE_CAPABILITY_SCHEMA_ID>
```

To retrieve the global image capability schema version:

```
oci compute global-image-capability-schema-version get --global-image-capability-schema-id <GLOBAL_IMAGE_CAPABILITY_SCHEMA_ID> --global-image-capability-schema-version-name <VERSION_NAME>
```

To list the image capability schemas in the specified compartment:

```
oci compute image-capability-schema list --compartment-id <COMPARTMENT_ID>
```

To retrieve the image capability schema for the specified ID:

```
oci compute image-capability-schema get --image-capability-schema-id <IMAGE_CAPABILITY_SCHEMA_ID>
```

To update the specified image capability schema:

```
oci -d compute image-capability-schema update --image-capability-schema-id <IMAGE_CAPABILITY_SCHEMA_ID> --schema-data file://<SCHEMA_DATA_FILE>.json
```

To create an image capability schema:

```
```

When you create the schema, you specify the image OCID for the custom image you want to apply the image capability schema to.

To delete the specified image capability schema:

```
oci -d compute image-capability-schema delete --image-capability-schema-id <IMAGE_CAPABILITY_SCHEMA_ID>
```

### Using the API

For information about using the API and signing requests, see [REST APIs](page 4368) and [Security Credentials](page 179). For information about SDKs, see [Software Development Kits and Command Line Interface](page 4225).

Use the following API operations for working with image capability schemas:

- ListComputeGlobalImageCapabilitySchemas
- ListComputeGlobalImageCapabilitySchemaVersions
- GetComputeGlobalImageCapabilitySchema
OS Kernel Updates

**Note:**

This topic applies only to Linux instances that were launched before February 15, 2017. Linux instances launched on or after February 15, 2017 boot directly from the image and do not require further action for kernel updates.

Oracle Cloud Infrastructure boots each instance from a network drive. This configuration requires additional actions when you update the OS kernel.

Oracle Cloud Infrastructure uses Unified Extensible Firmware Interface (UEFI) firmware and a Preboot eXecution Environment (PXE) interface on the host server to load iPXE from a Trivial File Transfer Protocol (TFTP) server. The iPXE implementation runs a script to boot Oracle Linux. During the boot process, the system downloads the kernel, the initrd file, and the kernel boot parameters from the network. The instance does not use the host's GRUB boot loader.

Normally, the `yum update kernel-uek` command edits the GRUB configuration file, either `grub.cfg` or `grub.conf`, to configure the next boot. Since bare metal instances do not use the GRUB boot loader, changes to the GRUB configuration file are not implemented. When you update the kernel on your instance, you also must upload the update to the network to ensure a successful boot process. The following approaches address this need:

- Instances launched from an Oracle-provided image include an Oracle yum plug-in that seamlessly handles the upload when you run the `yum update kernel-uek` command.
- If you use a custom image based on an Oracle-provided image, the included yum plug-in will continue to work, barring extraordinary changes.
- If you install your own package manager, you must either write your own plug-in or upload the kernel, initrd, and kernel boot parameters manually.

**Oracle Yum Plug-in**

On instances launched with an Oracle-provided image, you can find the Oracle yum plug-in at:

```
/usr/share/yum-plugins/kernel-update-handler.py
```

The plug-in configuration is at:

```
/etc/yum/pluginconf.d
```

The plug-in looks for two variables in the `/etc/sysconfig/kernel` file, `UPDATEDEFAULT` and `DEFAULTKERNEL`. It picks up the updates only when the first variable is set to "yes" and the `DEFAULTKERNEL` value matches the kernel being updated. For example:

```
# UPDATEDEFAULT specifies if new-kernel-pkg should make
# new kernels the default
UPDATEDEFAULT=yes

# DEFAULTKERNEL specifies the default kernel package type
DEFAULTKERNEL=kernel-uek
```

Oracle-provided images incorporate the Unbreakable Enterprise Kernel (UEK). If you want to switch to a non-UEK kernel, you must update the `DEFAULTKERNEL` value to "kernel" before you run `yum update kernel`. 
Manual Updates

Tip:
Oracle recommends using the Oracle yum plug-in to update the kernel.

If you manually upload the updates, there are four relevant URLs:

- http://169.254.0.3/kernel
- http://169.254.0.3/initrd
- http://169.254.0.3/cmdline
- http://169.254.0.3/activate

The first three URLs are for uploading files (HTTP request type PUT). The fourth URL is for activating the uploaded files (HTTP request type POST). The system discards the uploaded files if they are not activated before the host restarts.

The kernel and initrd are simple file uploads. The cmdline upload must contain the kernel boot parameters found in the `grub.cfg` or `grub.conf` file, depending on the Linux version. The following example is an entry from the `/boot/efi/EFI/redhat/grub.cfg` file in Red Hat Linux 7. The highlighted text represents the parameters to upload.

```
kernel /boot/vmlinuz-4.1.12-37.5.1.el6uek.x86_64
ro root=UUID=8079e287-53d7-4b3d-b708-c519cf6829c8 rd_NO_LUKS
   KEYBOARDTYPE=pc KEYTABLE=us
   netroot=iscsi:@169.254.0.2::3260:iface1:eth0::iqn.2015-02.oracle.boot:uefi
   rd_NO_MD SYSFONT=latarcyrheb-sun16 ifname=eth0:90:e2:ba:a2:e3:80
   crashkernel=auto iscsi_initiator=iqn.2015-02.
   rd_NO_LVM ip=eth0:dhcp
   rd_NO_DM LANG=en_US.UTF-8 console=tty0 console=ttyS0,9600 iommu=on
```

The following command returns what is being uploaded to the cmdline file.

```
cat /tmp/cmdline
```

A typical response resembles the following.

```
ro root=UUID=8079e287-53d7-4b3d-b708-c519cf6829c8 rd_NO_LUKS
   KEYBOARDTYPE=pc KEYTABLE=us
   netroot=iscsi:@169.254.0.2::3260:iface1:eth0::iqn.2015-02.oracle.boot:uefi
   rd_NO_MD SYSFONT=latarcyrheb-sun16 ifname=eth0:90:e2:ba:a2:e3:80
   crashkernel=auto iscsi_initiator=iqn.2015-02.
   rd_NO_LVM ip=eth0:dhcp
   rd_NO_DM LANG=en_US.UTF-8 console=tty0 console=ttyS0,9600 iommu=on
```
The following commands update the cmdline and initrd files, and then activate the changes.

```bash
CKSUM=`md5sum /tmp/cmdline | cut -d ' ' -f 1`
sudo curl -X PUT --data-binary @/tmp/cmdline -H "Content-MD5: $CKSUM"
http://169.254.0.3/cmdline

CKSUM=`md5sum /boot/initramfs-3.8.13-118.8.1.el7uek.x86_64.img | cut -d ' ' -f 1`
sudo curl -X PUT --data-binary @/boot/initramfs-3.8.13-118.8.1.el7uek.x86_64.img -H "Content-MD5: $CKSUM"
http://169.254.0.3/initrd

sudo curl -X POST http://169.254.0.3/activate
```

### Managing Key Pairs on Linux Instances

Instances launched using Oracle Linux, CentOS, or Ubuntu images use an SSH key pair instead of a password to authenticate a remote user (see Security Credentials on page 179). A key pair consists of a private key and public key. You keep the private key on your computer and provide the public key when you create an instance. When you connect to the instance using SSH, you provide the path to the private key in the SSH command.

You can have as many key pairs as you want, or you can keep it simple and use one key pair for all or several of your instances.

If you're using OpenSSH to connect to an instance, you can use a key pair that is generated by Oracle Cloud Infrastructure at the time that you create the instance. OpenSSH should be installed on UNIX-based systems (including Linux and OS X), Windows 10, and Windows Server 2019.

To create your own key pairs, you can use a third-party tool such as OpenSSH on UNIX-style systems (including Linux, Solaris, BSD, and OS X) or PuTTY Key Generator on Windows.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone who has access to the private key can connect to the instance. Store the private key in a secure location.</td>
</tr>
</tbody>
</table>

### Required SSH Public Key Format

If you provide your own key pair, it must use the OpenSSH format.

A public key has the following format:

```
<key_type> <public_key> <optional_comment>
```

For example, an RSA public key looks like this:

```
ssh-rsa AAAAB3BzaC1yc2EAAAADAQABAAABAQD9BrwrUilDki6P0+j2hwsjS2muM...
...yXDus/5Dr== rsa-key-20201202
```

For Oracle-provided images, these SSH key types are supported: RSA, DSA, DSS, ECDSA, and Ed25519. If you bring your own image, you're responsible for managing the SSH key types that are supported.

For RSA, DSS, and DSA keys, a minimum of 2048 bits is recommended. For ECDSA keys, a minimum of 256 bits is recommended.
Prerequisites

- If you're using a UNIX-style system, you probably already have the `ssh-keygen` utility installed. To determine whether it's installed, type `ssh-keygen` on the command line. If it's not installed, you can download OpenSSH for UNIX from [http://www.openssh.com/portable.html](http://www.openssh.com/portable.html) and install it.
- If you're using a Windows operating system, you will need PuTTY and the PuTTY Key Generator. Download PuTTY and PuTTYgen from [http://www.putty.org](http://www.putty.org) and install them.

Creating an SSH Key Pair on the Command Line

1. Open a shell or terminal for entering the commands.
2. At the prompt, enter `ssh-keygen` and provide a name for the key when prompted. Optionally, include a passphrase.

   The keys will be created with the default values: RSA keys of 2048 bits.

Alternatively, you can type a complete `ssh-keygen` command, for example:

```
ssh-keygen -t rsa -N "" -b 2048 -C "<key_name>" -f <path/root_name>
```

The command arguments are shown in the following table:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t rsa</code></td>
<td>Use the RSA algorithm.</td>
</tr>
<tr>
<td><code>-N &quot;&lt;passphrase&gt;&quot;</code></td>
<td>A passphrase to protect the use of the key (like a password). If you don't want to set a passphrase, don't enter anything between the quotes. A passphrase is not required. You can specify one as a security measure to protect the private key from unauthorized use. If you specify a passphrase, when you connect to the instance you must provide the passphrase, which typically makes it harder to automate connecting to an instance.</td>
</tr>
<tr>
<td><code>-b 2048</code></td>
<td>Generate a 2048-bit key. You don't have to set this if 2048 is acceptable, as 2048 is the default. A minimum of 2048 bits is recommended for SSH-2 RSA.</td>
</tr>
<tr>
<td><code>-C &quot;&lt;key_name&gt;&quot;</code></td>
<td>A name to identify the key.</td>
</tr>
<tr>
<td><code>-f &lt;path/root_name&gt;</code></td>
<td>The location where the key pair will be saved and the root name for the files.</td>
</tr>
</tbody>
</table>

Creating an SSH Key Pair Using PuTTY Key Generator

1. Find `puttygen.exe` in the PuTTY folder on your computer, for example, `C:\Program Files (x86)\PuTTY`. Double-click `puttygen.exe` to open it.
2. Specify a key type of SSH-2 RSA and a key size of 2048 bits:
   - In the **Key** menu, confirm that the default value of **SSH-2 RSA key** is selected.
   - For the **Type of key to generate**, accept the default key type of **RSA**.
   - Set the **Number of bits in a generated key** to 2048 if it is not already set.
3. Click **Generate**.
4. Move your mouse around the blank area in the PuTTY window to generate random data in the key.

When the key is generated, it appears under **Public key for pasting into OpenSSH authorized_keys file**.

5. A Key comment is generated for you, including the date and time stamp. You can keep the default comment or replace it with your own more descriptive comment.

6. Leave the Key passphrase field blank.

7. Click Save private key, and then click Yes in the prompt about saving the key without a passphrase.

The key pair is saved in the PuTTY Private Key (PPK) format, which is a proprietary format that works only with the PuTTY tool set.

You can name the key anything you want, but use the .ppk file extension. For example, mykey.ppk.

8. Select all of the generated key that appears under **Public key for pasting into OpenSSH authorized_keys file**, copy it using Ctrl + C, paste it into a text file, and then save the file in the same location as the private key.

(Do not use Save public key because it does not save the key in the OpenSSH format.)

You can name the key anything you want, but for consistency, use the same name as the private key and a file extension of .pub. For example, mykey.pub.

9. Write down the names and location of your public and private key files. You will need the public key when launching an instance. You will need the private key to access the instance via SSH.

Now that you have a key pair, you're ready to launch instances as described in Creating an Instance on page 695.

**Creating an Instance**

Use the steps in this topic to create a bare metal or virtual machine (VM) Compute instance.

**Tip:**

If this is your first time creating an instance, consider following the Getting Started Tutorial for a guided workflow through the steps required to create an instance.

When you create an instance, the instance is automatically attached to a virtual network interface card (VNIC) in the cloud network's subnet and given a private IP address from the subnet's CIDR. You can let the IP address be automatically assigned, or you can specify a particular address of your choice. The private IP address lets instances within the cloud network communicate with each other. If you've set up the cloud network for DNS, instances can instead use fully qualified domain names (FQDNs).

If the subnet is public, you can optionally assign the instance a public IP address. A public IP address is required to communicate with the instance over the internet, and to establish a Secure Shell (SSH) or Remote Desktop Protocol (RDP) connection to the instance from outside the cloud network.

**Note:**

Partner images and pre-built Oracle enterprise images are not available in Government Cloud realms.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

**Tip:**

When you create an instance, several other resources are involved, such as an image, a cloud network, and a subnet. Those other resources can be in the same **compartment** with the instance or in other compartments. You must have the required level of access to each of the compartments involved in
In order to launch the instance. This is also true when you attach a volume to an instance; they don't have to be in the same compartment, but if they're not, you need the required level of access to each of the compartments.

For administrators: The simplest policy to enable users to create instances is listed in Let users launch compute instances on page 2143. It gives the specified group general access to manage instances and images, along with the required level of access to attach existing block volumes to the instances. If the group needs to create block volumes, they'll need the ability to manage block volumes (see Let volume admins manage block volumes, backups, and volume groups on page 2146).

To require that legacy instance metadata service endpoints are disabled on any new instances that are created, use the following policy:

```
Allow group InstanceLaunchers to manage instances in compartment ABC where request.instanceOptions.areLegacyEndpointsDisabled= 'true'
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Partner Image Catalog**

If the group needs to create instances based on partner images, they'll need the manage permission for app-catalog-listing to create subscriptions to images from the Partner Image catalog. See Let users list and subscribe to images from the Partner Image catalog on page 2145.

**Security Zones**

Security Zones ensure that your cloud resources comply with Oracle security principles. If any operation on a resource in a security zone compartment violates a policy for that security zone, then the operation is denied.

The following security zone policies affect your ability to create instances:

- The boot volume for a compute instance in a security zone must also be in a security zone.
- A compute instance that isn't in a security zone can't use a boot volume that is in a security zone.
- A compute instance in a security zone must use subnets that are also in a security zone.
- All compute instances in a security zone must be created using an Oracle-provided image. You can't create a compute instance from a custom image in a security zone.

**Recommended Networking Launch Types**

When you launch a VM instance, by default, Oracle Cloud Infrastructure chooses a recommended networking type for the VNIC based on the instance shape and OS image. The networking interface handles functions such as disk input/output and network communication. The following options are available:

- **Paravirtualized networking**: For general purpose workloads such as enterprise applications, microservices, and small databases. Paravirtualized networking also provides increased flexibility to use the same image across different hardware platforms. Linux images with paravirtualized networking support live migration during infrastructure maintenance.
- **Hardware-assisted (SR-IOV) networking**: Single root input/output virtualization. For low-latency workloads such as video streaming, real-time applications, and large or clustered databases. Hardware-assisted (SR-IOV) networking uses the VFIO driver framework.

**Note:**

On Windows Server 2012 R2 images, SR-IOV networking is only supported on the VM.Standard2 and VM.DenseIO2 shapes.

The following table lists the default and supported networking types for VM shapes.
<table>
<thead>
<tr>
<th>Shape series</th>
<th>Default Networking Type</th>
<th>Supported Networking Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard1</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.Standard2</td>
<td>Paravirtualized</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.Standard.E2</td>
<td>Paravirtualized</td>
<td>Paravirtualized only</td>
</tr>
<tr>
<td>VM.Standard.E3</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Due to driver support, the Windows Server 2012 platform image supports paravirtualized networking only.</td>
</tr>
<tr>
<td>VM.DenseIO1</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.DenseIO2</td>
<td>Paravirtualized</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.GPU2</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.GPU3</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
</tbody>
</table>

To use paravirtualized networking, you must also use an image that supports paravirtualized networking. Paravirtualized networking is supported on these Oracle-provided images:

- **Oracle Linux 8**: All images.
- **Oracle Linux 7, Oracle Linux 6**: Images published in March 2019 or later.
- **CentOS 8**: All images.
- **CentOS 7**: Images published in July 2019 or later.
- **Ubuntu 18.04, Ubuntu 16.04**: Images published in March 2019 or later.
- **Windows Server 2019**: All images.
- **Windows Server 2016**: Images published in August 2019 or later.

SR-IOV networking is supported on all Oracle-provided images, except for Windows Server 2019 when launched using a VM.Standard2 shape. On Windows Server 2012 R2, SR-IOV networking is only supported on the VM.Standard2 and VM.DenseIO2 shapes.

You can create an instance that uses a specific networking type instead of the default. However, depending on compatibility between the shape and image that you choose, the instance might not launch properly. You can test whether it succeeded by connecting to the instance. If the connection fails, the networking type is not supported. Relaunch the instance using a supported networking type.

**Creating a Linux Instance**

Use the following steps to create a Linux instance.

**Prerequisites**

Before you start, you need these things:

- If you want to use your own Secure Shell (SSH) key to connect to the instance using SSH, you need the public key from the SSH key pair that you plan to use. The key must be in OpenSSH format. For more information, see Managing Key Pairs on Linux Instances on page 693.

**To create a Linux instance**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click Create Instance.
3. Enter a name for the instance. You can add or change the name later. The name doesn't need to be unique, because an Oracle Cloud Identifier (OCID) uniquely identifies the instance. Avoid entering confidential information.

4. Select the compartment to create the instance in.

   The other resources that you choose can come from different compartments.

5. In the **Placement and hardware** section, make the following selections:

   a. Select the **Availability domain** that you want to create the instance in.

      **Note:**

      If you're creating an instance from a boot volume, you must create the instance in the same availability domain as the boot volume.

   b. **Choose a fault domain**: The fault domain to use for the instance. If you do not specify the fault domain, the system selects one for you. To change the fault domain for a VM instance after you create the instance, edit the fault domain. For more information, see Fault Domains on page 182 and Best Practices for Your Compute Instance on page 594.

   c. By default, an Oracle Linux 7.x **image** is used to boot the instance. To select a different image or a boot volume, in the **Image** section, click **Change Image**. Then, select an **Image source** from the list. The following options are available:

      - **Platform Images**: Pre-built images for Oracle Cloud Infrastructure. To select a different OS version or image build, select the check box next to an image, and then select a value from the lists in the row for the image. To see which shapes are compatible with an OS version and image build, click **Advanced Options**. For more information about platform images, see Oracle-Provided Images on page 629.
      - **Oracle Images**: Pre-built Oracle enterprise images and solutions enabled for Oracle Cloud Infrastructure.
      - **Partner Images**: Trusted third-party images published by Oracle partners. Click the down arrow in the row for an image to view more details about the image, or to change the image build. For more information, see Overview of Marketplace on page 2650 and Working with Listings on page 2651.
      - **Custom Images**: Custom images created or imported into your Oracle Cloud Infrastructure environment. For more information, see Managing Custom Images on page 665.
      - **Boot Volumes**: Boot volumes that are available for creating a new instance in your Oracle Cloud Infrastructure environment. For more information, see Boot Volumes on page 609.
      - **Image OCID**: Create an instance using a specific version of an image by providing the image **OCID**. To determine the image OCID for Oracle-provided images, see Oracle-Provided Image Release Notes.

   Choose an image or boot volume, and then click **Select Image**.

   d. In the **Shape** section, click **Change Shape**. Then, do the following:

      1. In the **Instance type** section, select **Virtual Machine** or **Bare Metal Machine**.
      2. If you're creating a virtual machine, in the **Shape series** section, select a processor group, and then choose a **shape**. The following options are available:

         - **AMD Rome**: The **flexible shapes**, which uses the current generation AMD processor and has a customizable number of OCPUs and amount of memory.

         - For **Number of OCPUs**, choose the number of OCPUs that you want to allocate to this instance by dragging the slider. You can select from 1 to 64 OCPUs.

         - For **Amount of memory (GB)**, choose the amount of memory that you want to allocate to this instance by dragging the slider. The amount of memory allowed is based on the number of OCPUs selected. For each OCPU, you can select up to 64 GB of memory, with a maximum of 1024 GB total. The minimum amount of memory allowed is either 1 GB or a value matching the number
of OCPUs, whichever is greater. For example, if you select 25 OCPUs, the minimum amount of memory allowed is 25 GB.

The other resources scale proportionately.

- **Intel Skylake**: Standard shapes that use the current generation Intel processor and have a fixed number of OCPUs.
- **Specialty and Legacy**: Standard shapes with previous generation Intel and AMD processors, the Always Free VM.Standard.E2.1.Micro shape, Dense I/O shapes, GPU shapes, and HPC shapes.

If a shape is disabled, it means that the shape is either incompatible with the image that you selected previously, or not available in the current availability domain. If you don't see a shape, it means that you don't have service limits for the shape. You can request a service limit increase.

For more information about shapes, see Compute Shapes on page 655.

3. Click **Select Shape**.

6. In the **Networking** section, decide whether you want to **Select an existing virtual cloud network**, **Create a new virtual cloud network and subnet**, or **Enter a subnet OCID**, and then configure the network details for the instance.

**Select existing virtual cloud network**

Make the following selections:

- **Virtual cloud network in <compartment_name>**: Select the cloud network. If necessary, click **Change compartment** to switch to the compartment that contains the cloud network.
- **Subnet**: A subnet within the cloud network that the instance is attached to. The subnets are either public or private. Private means the instances in that subnet can't have public IP addresses. For more information, see Access to the Internet on page 2752. Subnets can also be either AD-specific or regional (regional ones have "regional" after the name). We recommend using regional subnets. For more information, see About Regional Subnets on page 2822.

If choosing **Select existing subnet**, for **Subnet in <compartment_name>**, select the subnet. If necessary, click **Change compartment** to switch to the compartment that contains the correct subnet.

If choosing **Create new public subnet**, enter the following:

- **New subnet name**: A friendly name for the subnet. It doesn't have to be unique, and it cannot be changed later in the Console. You can change it with the API. Avoid entering confidential information.
- **Create in compartment**: Specify the compartment where you want to put the subnet.
- **CIDR block**: A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). Make sure it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You cannot change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.

**Create new virtual cloud network and subnet**

Make the following selections:

- **New virtual cloud network name**: A friendly name for the network. Avoid entering confidential information.
- **Create in compartment**: Specify the compartment where you want to put the new network.
- **Subnet**: A subnet within the cloud network to attach the instance to. The subnets are either public or private. Private means the instances in that subnet can't have public IP addresses. For more information, see Access to the Internet on page 2752. Subnets can also be either AD-specific or regional (regional ones have "regional"
Compute

after the name). We recommend using regional subnets. For more information, see About Regional Subnets on page 2822.

Leave Create new public subnet selected, and enter the following:

- **Subnet name**: A friendly name for the subnet. It doesn't have to be unique, and it cannot be changed later in the Console. You can change it with the API. Avoid entering confidential information.
- **Create in compartment**: Specify the compartment where you want to put the subnet.
- **CIDR block**: A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). Make sure it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You cannot change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.

**Enter subnet OCID**

For Subnet OCID, enter the subnet OCID.

7. If the subnet is public, you can optionally assign the instance a public IP address. A public IP address makes the instance accessible from the internet. Select the Assign a public IPv4 address option. For more information, see Access to the Internet on page 2752.

8. In the Add SSH keys section, generate an SSH key pair or upload your own public key. Select one of the following options:

- **Generate SSH keys**: Oracle Cloud Infrastructure generates an RSA key pair for the instance. Click Save Private Key, and then save the private key on your computer. Optionally, click Save Public Key and then save the public key.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone who has access to the private key can connect to the instance.</td>
</tr>
<tr>
<td>Store the private key in a secure location.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use a key pair that is generated by Oracle Cloud Infrastructure, you must access the instance from a system that has OpenSSH installed. UNIX-based systems (including Linux and OS X), Windows 10, and Windows Server 2019 should have OpenSSH. For more information, see Managing Key Pairs on Linux Instances on page 693.</td>
</tr>
</tbody>
</table>

- **Choose SSH key files**: Upload the public key portion of your key pair. Either browse to the key file that you want to upload, or drag and drop the file into the box. To provide multiple keys, press and hold down the Command key (on Mac) or the CTRL key (on Windows) while selecting files.

- **Paste SSH keys**: Paste the public key portion of your key pair in the box.

- **No SSH keys**: Select this option only if you do not want to connect to the instance using SSH. You cannot provide a public key or save the key pair that is generated by Oracle Cloud Infrastructure after the instance is created.

9. In the Boot volume section, configure the size and encryption options for the instance's boot volume:

- To specify a custom size for the boot volume, select the Specify a custom boot volume size check box. Then, enter a custom size from 50 GB to 32 TB. The specified size must be larger than the default boot volume size for the selected image. See Custom Boot Volume Sizes on page 610 for more information.

- For VM instances, you can optionally select the Use in-transit encryption check box. See Block Volume Encryption on page 504 for more information. If you are using your own Vault service encryption key for the boot volume, then this key is also used for in-transit encryption. Otherwise, the Oracle-provided encryption key is used.

- Boot volumes are encrypted by default, but you can optionally use your own Vault service encryption key to encrypt the data in this volume. To use the Vault service for your encryption needs, select the Encrypt this volume with a key that you manage check box. Then, select the Vault compartment and Vault that contain the master encryption key you want to use. Also select the Master encryption key compartment and Master
encryption key. For more information about encryption, see Overview of Vault on page 3952. If you enable this option, this key is used for both data at rest encryption and in-transit encryption.

- The Block Volume elastic performance feature lets you change the volume performance for boot volumes. When you create an instance, its boot volume is configured with the default volume performance set to Balanced. After you launch the instance, you can modify the performance setting. For steps to modify the performance setting, see Changing the Performance of a Volume on page 582. For more information about this feature, see Block Volume Elastic Performance on page 581.

10. (Optional) To configure advanced networking and management settings, click Show Advanced Options. The following options are available:

- On the Management tab, you can configure the following:
  - **Require an authorization header:** Select this check box to require that all requests to the instance metadata service (IMDS) use the version 2 endpoint and include an authorization header. Requests to IMDSv1 are denied. The image must support IMDSv2. For more information, see Getting Instance Metadata on page 757.
  - **Initialization Script:** User data to be used by cloud-init to run custom scripts or provide custom cloud-init configuration. Browse to the file that you want to upload, or drag and drop the file into the box. The file or script does not need to be base64-encoded, because the Console performs this encoding when the information is submitted. For information about how to take advantage of user data, see the cloud-init documentation. The total maximum size for user data and other metadata that you provide is 32,000 bytes.
  - **Restore instance lifecycle state after infrastructure maintenance:** By default, if a VM instance is running when a maintenance event affects the underlying infrastructure, the instance is rebooted after it is recovered. Clear this check box if you want the instance to be recovered in the stopped state.
  - **Tagging:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- On the Networking tab, you can configure the following:
  - **Private IP Address:** An available private IP address of your choice from the subnet's CIDR. If you don't specify a value, the private IP address is automatically assigned.
  - **Hostname:** A hostname to be used for DNS within the cloud network. Available only if the VCN and subnet both have DNS labels. For more information, see DNS in Your Virtual Cloud Network on page 2910.
  - **Launch Options:** The networking launch type. Available only for VMs. For more information, see Recommended Networking Launch Types on page 696.

- On the Placement tab, you can choose to launch the instance on a dedicated virtual machine host. This lets you run the instance in isolation, so that it is not running on shared infrastructure. To do this, select the Dedicated host option, and then select a dedicated virtual machine host from the drop-down list. Before you can place an instance on a dedicated virtual machine host, you must create a dedicated virtual machine host in the same availability domain and fault domain as the instance. You can only place an instance on a dedicated virtual machine host at the time that you create the instance. For more information, see Dedicated Virtual Machine Hosts on page 729.

- On the Oracle Cloud Agent tab, choose which plugins you want to enable when the instance is launched. Plugins collect performance metrics, install OS updates, and perform other instance management tasks. For more information, see Managing Plugins with Oracle Cloud Agent on page 740.

Important:

Be aware of the following:

- After you create the instance, you might need to perform additional configuration tasks before you can use each plugin.
- Oracle Autonomous Linux instances cannot be managed by the OS Management service. See this known issue for more information.
11. Click **Create**.

To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

After the instance is provisioned, details about it appear in the instance list. To view more details, including IP addresses, click the instance name.

When the instance is fully provisioned and running, you can connect to it using SSH as described in Connecting to an Instance on page 733.

You also can attach a volume to the instance, provided the volume is in the same availability domain. For background information about volumes, see Overview of Block Volume on page 500.

For steps to let additional users connect to the instance, see Adding Users on an Instance on page 737.

**Creating a Windows Instance**

Use the following steps to create a Windows instance.

**Prerequisites**

Before you start, you need these things:

- A VCN security rule that enables Remote Desktop Protocol (RDP) access so that you can connect to your instance. Specifically, you need a stateful ingress rule for TCP traffic on destination port 3389 from source 0.0.0.0/0 and any source port. For more information, see Security Rules on page 2833. You can implement...
To enable RDP access

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you’re not sure which compartment to use, contact an administrator.
3. Click the cloud network that you’re interested in.
4. To add the rule to a network security group that the instance belongs to:
   a. Under **Resources**, click **Network Security Groups**. Then click the network security group that you're interested in.
   b. Click **Add Rules**.
   c. Enter the following values for the rule:
      - **Stateless**: Leave the check box cleared.
      - **Source Type**: CIDR
      - **Source CIDR**: 0.0.0.0/0
      - **IP Protocol**: RDP (TCP/3389)
      - **Source Port Range**: All
      - **Destination Port Range**: 3389
      - **Description**: An optional description of the rule.
   d. When done, click **Add**.
5. Or, to add the rule to a security list that is used by the instance's subnet:
   a. Under **Resources**, click **Security Lists**. Then click the security list you're interested in.
   b. Click **Add Ingress Rules**.
   c. Enter the following values for the rule:
      - **Stateless**: Leave the check box cleared.
      - **Source Type**: CIDR
      - **Source CIDR**: 0.0.0.0/0
      - **IP Protocol**: RDP (TCP/3389)
      - **Source Port Range**: All
      - **Destination Port Range**: 3389
      - **Description**: An optional description of the rule.
   d. When done, click **Add Ingress Rules**.

To create a Windows instance

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click **Create Instance**.
3. Enter a name for the instance. You can add or change the name later. The name doesn't need to be unique, because an Oracle Cloud Identifier (OCID) uniquely identifies the instance. Avoid entering confidential information.
   **Important:**
   Use only these ASCII characters in the instance name: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and hyphens (-). See this [known issue](#) for more information.
4. Select the compartment to create the instance in.
   The other resources that you choose can come from different compartments.
5. In the **Placement and hardware** section, make the following selections:

   a. Select the **Availability domain** that you want to create the instance in.

   ![](image)

   **Note:**
   
   If you're creating an instance from a boot volume, you must create the instance in the same availability domain as the boot volume.

   b. **Choose a fault domain**: The fault domain to use for the instance. If you do not specify the fault domain, the system selects one for you. To change the fault domain for a VM instance after you create the instance, edit the fault domain. For more information, see **Fault Domains** on page 182 and **Best Practices for Your Compute Instance** on page 594.

   c. In the **Image** section, you choose the **image** that's used to boot the instance. Click **Change Image**. Then, select an **Image source** from the list. The following options are available:

   - **Platform Images**: Pre-built images for Oracle Cloud Infrastructure. To select a different OS version or image build, select the check box next to an image, and then select a value from the lists in the row for the image. To see which shapes are compatible with an OS version and image build, click **Advanced Options**. For more information about platform images, see **Oracle-Provided Images** on page 629.
   
   - **Oracle Images**: Pre-built Oracle enterprise images and solutions enabled for Oracle Cloud Infrastructure.
   
   - **Partner Images**: Trusted third-party images published by Oracle partners. Click the down arrow in the row for an image to view more details about the image, or to change the image build. For more information, see **Overview of Marketplace** on page 2650 and **Working with Listings** on page 2651.
   
   - **Custom Images**: Custom images created or imported into your Oracle Cloud Infrastructure environment. For more information, see **Managing Custom Images** on page 665.
   
   - **Boot Volumes**: Boot volumes that are available for creating a new instance in your Oracle Cloud Infrastructure environment. For more information, see **Boot Volumes** on page 609.
   
   - **Image OCID**: Create an instance using a specific version of an image by providing the image **OCID**. To determine the image OCID for Oracle-provided images, see **Oracle-Provided Image Release Notes**.

   Choose an image or boot volume, and then click **Select Image**.

   d. In the **Shape** section, click **Change Shape**. Then, do the following:

   1. In the **Instance type** section, select **Virtual Machine** or **Bare Metal Machine**.
   2. If you're creating a virtual machine, in the **Shape series** section, select a processor group, and then choose a **shape**. The following options are available:

   - **AMD Rome**: The **flexible shapes**, which uses the current generation AMD processor and has a customizable number of OCPUs and amount of memory.

     - For **Number of OCPUs**, choose the number of OCPUs that you want to allocate to this instance by dragging the slider. You can select from 1 to 64 OCPUs.
     
     - For **Amount of memory (GB)**, choose the amount of memory that you want to allocate to this instance by dragging the slider. The amount of memory allowed is based on the number of OCPUs selected. For each OCPU, you can select up to 64 GB of memory, with a maximum of 1024 GB total. The minimum amount of memory allowed is either 1 GB or a value matching the number...
of OCPUs, whichever is greater. For example, if you select 25 OCPUs, the minimum amount of memory allowed is 25 GB.

The other resources scale proportionately.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Windows Server 2019 instances using the VM.Standard.E3.Flex shape, allocate a maximum of 32 OCPUs to the instance. See this known issue for more information.</td>
</tr>
</tbody>
</table>

- **Intel Skylake**: Standard shapes that use the current generation Intel processor and have a fixed number of OCPUs.

- **Specialty and Legacy**: Standard shapes with previous generation Intel and AMD processors, the Always Free VM.Standard.E2.1.Micro shape, Dense I/O shapes, GPU shapes, and HPC shapes.

If a shape is disabled, it means that the shape is either incompatible with the image that you selected previously, or not available in the current availability domain. If you don't see a shape, it means that you don't have service limits for the shape. You can request a service limit increase.

For more information about shapes, see Compute Shapes on page 655.

3. Click Select Shape.

6. In the Networking section, decide whether you want to Select an existing virtual cloud network, Create a new virtual cloud network and subnet, or Enter a subnet OCID, and then configure the network details for the instance.

**Select existing virtual cloud network**

Make the following selections:

- **Virtual cloud network in <compartment_name>**: Select the cloud network. If necessary, click Change compartment to switch to the compartment that contains the cloud network.

- **Subnet**: A subnet within the cloud network that the instance is attached to. The subnets are either public or private. Private means the instances in that subnet can't have public IP addresses. For more information, see Access to the Internet on page 2752. Subnets can also be either AD-specific or regional (regional ones have "regional" after the name). We recommend using regional subnets. For more information, see About Regional Subnets on page 2822.

If choosing Select existing subnet, for Subnet in <compartment_name>, select the subnet. If necessary, click Change compartment to switch to the compartment that contains the correct subnet.

If choosing Create new public subnet, enter the following:

- **New subnet name**: A friendly name for the subnet. It doesn't have to be unique, and it cannot be changed later in the Console. You can change it with the API. Avoid entering confidential information.

- **Create in compartment**: Specify the compartment where you want to put the subnet.

- **CIDR block**: A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). Make sure it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You cannot change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.

**Create new virtual cloud network and subnet**

Make the following selections:

- **New virtual cloud network name**: A friendly name for the network. Avoid entering confidential information.

- **Create in compartment**: Specify the compartment where you want to put the new network.

- **Subnet**: A subnet within the cloud network to attach the instance to. The subnets are either public or private. Private means the instances in that subnet can't have public IP addresses. For more information, see Access to the Internet on page 2752. Subnets can also be either AD-specific or regional (regional ones have "regional"
after the name). We recommend using regional subnets. For more information, see About Regional Subnets on page 2822.

Leave Create new public subnet selected, and enter the following:

- **Subnet name**: A friendly name for the subnet. It doesn't have to be unique, and it cannot be changed later in the Console. You can change it with the API. Avoid entering confidential information.
- **Create in compartment**: Specify the compartment where you want to put the subnet.
- **CIDR block**: A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). Make sure it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You cannot change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.

**Enter subnet OCID**

For Subnet OCID, enter the subnet OCID.

7. If the subnet is public, you can optionally assign the instance a public IP address. A public IP address makes the instance accessible from the internet. Select the Assign a public IPv4 address option. For more information, see Access to the Internet on page 2752.

8. In the **Boot volume** section, configure the size and encryption options for the instance's boot volume:

- To specify a custom size for the boot volume, select the Specify a custom boot volume size check box. Then, enter a custom size from 50 GB (256 GB for Oracle-provided Windows images) to 32 TB. The specified size must be larger than the selected image's default boot volume size. See Custom Boot Volume Sizes on page 610 for more information.
- For VM instances, you can optionally select the Use in-transit encryption check box. See Block Volume Encryption on page 504 for more information. If you are using your own Vault service encryption key for the boot volume, then this key is also used for in-transit encryption. Otherwise, the Oracle-provided encryption key is used.
- Boot volumes are encrypted by default, but you can optionally use your own Vault service encryption key to encrypt the data in this volume. To use the Vault service for your encryption needs, select the Encrypt this volume with a key that you manage check box. Then, select the Vault compartment and Vault that contain the master encryption key you want to use. Also select the Master encryption key compartment and Master encryption key. For more information about encryption, see Overview of Vault on page 3952.
- The Block Volume elastic performance feature lets you change the volume performance for boot volumes. When you create an instance, its boot volume is configured with the default volume performance set to Balanced. After you launch the instance, you can modify the performance setting. For steps to modify the performance setting, see Changing the Performance of a Volume on page 582. For more information about this feature, see Block Volume Elastic Performance on page 581.

9. (Optional) To configure advanced networking and management settings, click Show Advanced Options. The following options are available:

- On the Management tab, you can configure the following:
  - **Choose a fault domain**: The fault domain to use for the instance. If you do not specify the fault domain, the system selects one for you. You can change the fault domain for a VM instance after you create the instance. For more information about fault domains, see Fault Domains on page 182 and Best Practices for Your Compute Instance on page 594.
  - **Require an authorization header**: Select this check box to require that all requests to the instance metadata service (IMDS) use the version 2 endpoint and include an authorization header. Requests to IMDSv1 are denied. The image must support IMDSv2. For more information, see Getting Instance Metadata on page 757.
  - **Initialization Script**: User data to be used by cloudbase-init to run custom scripts or provide custom cloudbase-init configuration. Browse to the file that you want to upload, or drag and drop the file into the box. The file or script does not need to be base64-encoded, because the Console performs this encoding when the information is submitted. For information about how to take advantage of user data, see the...
cloudbase-init documentation. The total maximum size for user data and other metadata that you provide is 32,000 bytes.

Caution:

Do not include anything in the script that could trigger a reboot, because this could impact the instance launch and cause it to fail. Any actions requiring a reboot should only be performed once the instance state is Running.

- **Restore instance lifecycle state after infrastructure maintenance**: By default, if a VM instance is running when a maintenance event affects the underlying infrastructure, the instance is rebooted after it is recovered. Clear this check box if you want the instance to be recovered in the stopped state.

- **Tagging**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- On the Networking tab, you can configure the following:
  - **Private IP address**: An available private IP address of your choice from the subnet's CIDR. If you don’t specify a value, the private IP address is automatically assigned.
  - **Hostname**: A hostname to be used for DNS within the cloud network. Available only if the VCN and subnet both have DNS labels. For more information, see DNS in Your Virtual Cloud Network on page 2910.
  - **Launch Options**: The networking launch type. Available only for VMs. For more information, see Recommended Networking Launch Types on page 696.

- On the Placement tab, you can choose to launch the instance on a dedicated virtual machine host. This lets you run the instance in isolation, so that it is not running on shared infrastructure. To do this, select the Dedicated host option, and then select a dedicated virtual machine host from the drop-down list. Before you can place an instance on a dedicated virtual machine host, you must create a dedicated virtual machine host in the same availability domain and fault domain as the instance. You can only place an instance on a dedicated virtual machine host at the time you create the instance. For more information, see Dedicated Virtual Machine Hosts on page 729.

- On the Oracle Cloud Agent tab, choose which plugins you want to enable when the instance is launched. Plugins collect performance metrics, install OS updates, and perform other instance management tasks. For more information, see Managing Plugins with Oracle Cloud Agent on page 740.

Important:

After you create the instance, you might need to perform additional configuration tasks before you can use each plugin.

10. Click Create.

To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

After the instance is provisioned, details about it appear in the instance list. To view more details, including IP addresses and the initial Windows password, click the instance name.

When the instance is fully provisioned and running, you can connect to it using Remote Desktop as described in Connecting to an Instance on page 733.

You also can attach a volume to the instance, provided the volume is in the same availability domain. For background information about volumes, see Overview of Block Volume on page 500.

For steps to let additional users connect to the instance, see Adding Users on an Instance on page 737.
Managing Tags for an Instance

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

To manage tags for an instance

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click the Tags tab to view or edit the existing tags. Or click More Actions, and then click Add tags to add new ones.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage instances:

- ListInstances
- LaunchInstance
- GetInstance
- UpdateInstance
- TerminateInstance
- GetInstanceDefaultCredentials

You can also launch instances from images that are published by Oracle partners in the Partner Image catalog. Use these APIs to work with the Partner Image catalog listings:

- AppCatalogListing
- AppCatalogListingResourceVersion
- AppCatalogListingResourceVersionAgreements
- AppCatalogListingResourceVersionSummary
- AppCatalogListingSummary
- AppCatalogSubscription

Managing Compute Instances

You can simplify the management of your Compute instances using resources such as instance configurations and instance pools.

An instance configuration is a template that defines the settings to use when creating Compute instances.

An instance pool is a group of instances within the same region that are created from the same instance configuration and managed as a group.

Instance Configurations

An instance configuration defines the settings to use when creating Compute instances, including details such as the base image, shape, and metadata. You can also specify the associated resources for the instance, such as block volume attachments and network configuration.

For steps to create an instance configuration, see Creating an Instance Configuration on page 710.

To modify an existing instance configuration, create a new instance configuration with the desired settings.

For steps to delete an instance configuration, see Deleting an Instance Configuration on page 717.

Use these API operations to work with instance configurations:

- CreateInstanceConfiguration
• **DeleteInstanceConfiguration**
• **GetInstanceConfiguration**
• **UpdateInstanceConfiguration**
• **ListInstanceConfigurations**

**Instance Pools**

Instance pools let you create multiple Compute instances from the same instance configuration, within the same region. They also enable integration with other services, such as the Load Balancing service and IAM service, making it easier to manage groups of instances.

You create an instance pool using an existing instance configuration. For steps, see Creating an Instance Pool on page 711.

You can automatically adjust the number of instances in an instance pool based on performance metrics or a schedule. To do this, you enable autoscaling for the instance pool. For background information and steps, see Autoscaling on page 718.

After you have created an instance pool, you can update the size and attach or detach load balancers from the Console. To update additional settings, you need to use the CLI, API, or SDKs.

If you need to update the instance configuration, create a new instance configuration and then update the instance pool to use the new instance configuration. For more information, see Updating an Instance Pool on page 713.

A cluster network is a special kind of instance pool that is designed for massive, high-performance computing jobs. For more information, see Managing Cluster Networks on page 726.

For steps to delete an instance pool, see Deleting an Instance Pool on page 718.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you delete an instance pool all of its resources will be permanently deleted, including associated instances, attached boot volumes, and block volumes.</td>
</tr>
</tbody>
</table>

**Instance Pool Lifecycle States**

The following list describes the different lifecycle states for instance pools.

- **Provisioning**: When you create an instance pool, this is the first state the instance pool is in. Instances for the instance pool are being configured based on the specified instance configuration.
- **Starting**: The instances are being launched. At this point, the only action you can take is to terminate the instance pool.
- **Running**: The instances are created and running.
- **Stopped**: The instances are in the process of being shut down.
- **Stopped**: The instances are shut down.
- **Scaling**: After an instance pool has been created, if you update the instance pool size, it will go into this state while creating instances (for increases in pool size) or terminating instances (for decreases in pool size). At this point, the only action you can take is to terminate the instance pool.
- **Terminating**: The instances and associated resources are being terminated.
- **Terminated**: The instance pool, all its instances and associated resources are terminated.

When working with instance configurations and instance pools, keep the following in mind:

- You can't delete an instance configuration if it is associated with at least one instance pool.
- You can use the same instance configuration for multiple instance pools. However, an instance pool can have only one instance configuration associated with it.
- If the instance pool has been in the scaling or provisioning state for an extended period of time, it might be because the number of instances that were requested has exceeded your tenancy's service limits for that
availability domain. For information about how to check your service limits, and steps to request a service limit increase, see Service Limits on page 215. If this occurs, you need to terminate the instance pool and re-create it.

- If you modify the instance configuration for an instance pool, existing instances that are part of that pool will not change. Any new instances that are created after you modify the instance configuration will use the new instance configuration. New instances will not be created unless you have increased the size of the instance pool or terminate existing instances.
- If you decrease the size of an instance pool, the oldest instances are terminated first.

Use these API operations to manage instance pools:

- CreateInstancePool
- GetInstancePool
- ResetInstancePool
- SoftresetInstancePool
- StartInstancePool
- StopInstancePool
- TerminateInstancePool
- UpdateInstancePool
- ListInstancePools
- ListInstancePoolInstances
- AttachLoadBalancer
- DetachLoadBalancer
- GetInstancePoolLoadBalancerAttachment

Creating an Instance Configuration

Instance configurations let you define the settings to use when creating Compute instances.

You use an instance configuration when you want to create one or more instances in an instance pool. For background information about instance pools, see Managing Compute Instances on page 708.

You can also use an instance configuration to launch individual instances that are not part of a pool. To do this, use the SDKs, command line interface (CLI), or API.

In the Console, you create an instance configuration using an existing Compute instance as a template. If you want to create an instance configuration by specifying a list of configuration settings, use the SDKs, CLI, or API.

When you create an instance configuration using an existing instance as a template, be aware of the following information:

- The instance configuration does not include any information from the instance's boot volume, such as installed applications, binaries, and files on the instance. To create an instance configuration that includes the custom setup from an instance, you must first create a custom image from the instance, and then use the custom image to launch a new instance. Finally, create the instance configuration based on the instance that you created from the custom image.
- The instance configuration does not include the contents of any block volumes that are attached to the instance. To include block volume contents with an instance configuration, first create a backup of the attached block volumes. Then, use the SDKs, CLI, or API to create the instance configuration, specifying the block volume backups in the list of configuration settings.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to instance pools and instance configurations, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.
Tagging Resources

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

Using the Console

To create an instance configuration

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance whose image you want to use as a template to create the instance configuration.
3. Click More Actions, and then click Create Instance Configuration.
4. Select the compartment you want to create the instance configuration in.
5. Specify a name for the instance configuration. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
6. Show Tagging Options: Optionally, you can add tags. If you have permissions to create a resource, you also have permissions to add free-form tags to that resource. To add a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should add tags, skip this option (you can add tags later) or ask your administrator.
7. Click Create Instance Configuration.

To manage tags for an instance configuration

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Configurations.
2. Click the instance configuration that you're interested in.
3. Click the Tags tab to view or edit the existing tags. Or click Add tags to add new ones.

For more information, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the CreateInstanceConfiguration operation to create an instance configuration.

Creating an Instance Pool

Use instance pools to create multiple compute instances from the same configuration, within the same region. You can manage the instances in an instance pool as a group. For more information about instance pools and instance configurations, see Managing Compute Instances on page 708.

Optionally, you can associate one or more load balancers with an instance pool. If you do this, when you add an instance to the instance pool, the instance is automatically added to the load balancer's backend set. After the instance reaches a healthy state (the instance is listening on the configured port number), incoming traffic is automatically routed to the new instance. For background information about the Load Balancing service, see Overview of Load Balancing on page 2480.

Instance pools are supported for virtual machine (VM) and bare metal instances.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to instance pools and instance configurations, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.
Tagging Resources
You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

Distributing Instances Across Fault Domains for High Availability
By default, the instances in a pool are distributed across all fault domains in a best-effort manner based on capacity. If capacity isn't available in one fault domain, the instances are placed in other fault domains to allow the instance pool to launch successfully.

In a high availability scenario, you can require that the instances in a pool are evenly distributed across each of the fault domains that you specify. When sufficient capacity isn't available in one of the fault domains, the instance pool will not launch or scale successfully, and a work request for the instance pool will return an “out of capacity” error. To fix the capacity error, either wait for capacity to become available, or use the UpdateInstancePool operation to update the placement configuration (the availability domain and fault domain) for the instance pool.

Prerequisites
Before you can create an instance pool, you need:

- An instance configuration. An instance configuration is a template that defines the settings to use when creating instances. When you create the instance pool, monitoring will be enabled by default on instances that support monitoring, regardless of the settings in the instance configuration. For more information, see Creating an Instance Configuration on page 710.

  Note:
  You cannot create an instance pool from an instance configuration where the image source is a boot volume.

- If you want to associate the instance pool with a load balancer, you need a load balancer and backend set. For steps to create a load balancer, see Managing Load Balancers on page 2494.

Using the Console
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click Create Instance Pool.
3. On the Add Basic Details page, do the following:
   a. Select the compartment to create the instance pool in.
   b. Enter a name for the instance pool. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   c. Select the Instance configuration that you want to use.
   d. Specify the targeted Number of instances for the instance pool.
   e. Show Tagging Options: Optionally, you can add tags. If you have permissions to create a resource, you also have permissions to add free-form tags to that resource. To add a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should add tags, skip this option (you can add tags later) or ask your administrator.
4. Click Next.
5. On the Configure Pool Placement page, select the location where you want to place the instances. Do the following:
   a. Select the Availability domain to launch the instances in.
   b. For the Fault domains box, do one of the following things:
      - If you want the system to make a best effort to distribute instances across fault domains based on capacity, leave the box blank.
      - If you want to require that the instances in the pool are distributed evenly in one or more fault domains, select the fault domains to place the instances in. The pool will not launch or scale successfully if sufficient
Compute capacity is unavailable in the selected fault domains. For more information, see Distributing Instances Across Fault Domains for High Availability on page 712.

c. In the Primary VNIC section, configure the network details for the instances:

- **Virtual cloud network:** The virtual cloud network (VCN) to create the instances in.
- **Subnet:** A subnet within the cloud network to attach the instances to. The subnets are either public or private. Private means the instances in that subnet can't have public IP addresses. For more information, see Access to the Internet on page 2752. Subnets can also be either AD-specific or regional (regional ones have "regional" after the name). We recommend using regional subnets. For more information, see About Regional Subnets on page 2822.

d. If secondary VNICs are defined by the instance configuration, a Secondary VNIC section appears. Select the secondary VCN and subnet for the instance pool.

e. If you want the instance pool to create instances in more than one availability domain, click + Another Availability Domain. Then, repeat the previous steps.

6. If you want to associate a load balancer with the instance pool, select the Attach a load balancer check box. Then, do the following:

   a. Select the Load balancer to associate with the instance pool.
   b. Select the Backend set on the load balancer to add instances to.
   c. In the Port box, enter the server port on the instances to which the load balancer must direct traffic. This value applies to all instances that use this load balancer attachment.
   d. In the VNIC list, select the VNIC to use when adding the instance to the backend set. Instances that belong to a backend set are also called backend servers. The private IP address is used. This value applies to all instances that use this load balancer attachment.
   e. If you want to associate additional load balancers with the instance pool, click + Another Load Balancer. Then, repeat the previous steps. Do this for each additional load balancer you want to associate with the instance pool.

For background information about load balancers, see Overview of Load Balancing on page 2480.

7. Click Next.

8. Review the instance pool details, and then click Create.

   To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to create and manage instance pools:

- CreateInstancePool
- AttachLoadBalancer
- DetachLoadBalancer
- GetInstancePoolLoadBalancerAttachment

Updating an Instance Pool

You can update the number of instances for an instance pool.

Optionally, you can associate a load balancer with an instance pool. If you do this, when you add an instance to the instance pool, the instance is automatically added to the load balancer's backend set. After the instance reaches a healthy state (the instance is listening on the configured port number), incoming traffic is automatically routed to the new instance. For background information about the Load Balancing service, see Overview of Load Balancing on page 2480.

To update other settings for an instance pool, use the command line interface (CLI), SDKs, or REST APIs.
Compute

You can automatically adjust the number of instances in an instance pool based on performance metrics or a schedule. To do this, you enable autoscaling for the instance pool. For background information and steps, see Autoscaling on page 718.

See Managing Compute Instances on page 708 for more information about instance pools and instance configurations.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to instance pools and instance configurations, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.

**Tagging Resources**

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

**Using the Console**

*To update the instance pool size*

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the name of the instance pool that you're interested in.
3. Click Edit.
4. Specify the updated number of instances for the instance pool, and then click Save Changes.

When you update the instance pool size, it triggers a scaling event. Keep the following in mind:

- If the instance pool lifecycle state is **RUNNING**, the instance pool will create new instances or terminate existing instances at that time, to match the new size of the instance pool. Instances are terminated in the order that they were created, first-in, first-out.
- If the instance pool lifecycle state is **STOPPED**, for an increase in size, new instances will be configured for the instance pool, but won’t be launched. For a decrease in size, the instances will be terminated.

To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

**Important:**

If the instance pool has been in the scaling or provisioning state for an extended period of time, it may be because the number of instances requested has exceeded your tenancy’s service limits for that shape and availability domain. Check your tenancy’s service limits for Compute.

To attach a load balancer to an instance pool

You must have a load balancer and backend set to associate with the instance pool. For steps to create a load balancer, see Managing Load Balancers on page 2494.

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the name of the instance pool that you're interested in.
4. Click **Attach a Load Balancer**.
5. Enter the following:
   - **Load balancer**: The load balancer to associate with the instance pool.
   - **Backend set**: The name of the backend set on the load balancer to add instances to.
   - **Port**: The server port on the instances to which the load balancer must direct traffic. This value applies to all instances that use this load balancer attachment.
   - **VNIC**: The VNIC to use when adding the instance to the backend set. Instances that belong to a backend set are also called backend servers. The private IP address is used. This value applies to all instances that use this load balancer attachment.
6. Click **Attach**.
   
   To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.
7. If you want to associate additional load balancers with the instance pool, click + **Another Load Balancer**. Then, repeat the previous steps. Do this for each additional load balancer you want to associate with the instance pool.

**To detach a load balancer from an instance pool**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instance Pools**.
2. Click the name of the instance pool that you're interested in.
3. Under **Resources**, click **Load Balancers**.
4. Click the Actions icon (three dots) for the load balancer you want to detach.
5. Click **Detach Load Balancer**, and then click **Detach** to confirm.
   
   To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

**To manage tags for an instance pool**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instance Pools**.
2. Click the instance pool that you're interested in.
3. Click the **Tags** tab to view or edit the existing tags. Or click **More Actions**, and then click **Add tags** to add new ones.
   
   For more information, see Resource Tags on page 211.

**Using the API**
To update other instance pool configuration settings, use the CLI, SDKs, or REST APIs. For information about using the CLI, see Command Line Interface (CLI) on page 4192. For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For instance pool configuration settings, such as the instance configuration, display name, tags, or availability domain selections, use the **UpdateInstancePool** operation.

To manage the load balancers that are associated with an instance pool, use the **AttachLoadBalancer** and **DetachLoadBalancer** operations.

To update the configuration that is used by an instance pool when creating instances, you can do either of the following things:
- Create a new instance configuration with the desired settings. You can do this using the Console. For steps, see Creating an Instance Configuration on page 710. To do this using the API, use the CreateInstanceConfiguration operation.
- Update the existing instance configuration for the instance pool. You can only update the display name and tags of existing instance configurations. For any other updates, create a new instance configuration with the settings you want to use. To update the display name or tags, use the UpdateInstanceConfiguration operation. You cannot use the Console to update instance configuration settings.
Stopping and Starting the Instances in an Instance Pool

You can stop and start the instances in an instance pool as needed to update software or resolve error conditions.

Stopping or Restarting an Instance Using the Instance's OS

In addition to using the API and Console, you can stop and restart instances using the commands available in the operating system when you are logged in to the instance. Stopping an instance using the instance's OS does not stop billing for that instance. If you stop the instances in an instance pool this way, be sure to also stop the instance pool from the Console or API.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to instance pools and instance configurations, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Resource Billing for Stopped Instances

For both VM and bare metal instances, billing depends on the shape that you use to create the instance:

- **Standard shapes**: Stopping an instance pool pauses billing. However, stopped instances continue to count toward your service limits.
- **Dense I/O shapes**: Billing continues for stopped instance pools because the NVMe storage resources are preserved. Related resources continue to count toward your service limits. To halt billing and remove related resources from your service limits, you must terminate the instance pool.
- **GPU shapes**: Billing continues for stopped instance pools because GPU resources are preserved. Related resources continue to count toward your service limits. To halt billing and remove related resources from your service limits, you must terminate the instance pool.
- **HPC shapes**: Billing continues for stopped instance pools because the NVMe storage resources are preserved. Related resources continue to count toward your service limits. To halt billing and remove related resources from your service limits, you must terminate the instance pool.

Stopping an instance using the instance's OS does not stop billing for that instance. If you stop the instances in an instance pool this way, be sure to also stop the instance pool from the Console or API.

For more information about Compute pricing, see Compute Pricing. For more information about how instances running Microsoft Windows Server are billed when they are stopped, see How am I charged for Windows Server on Oracle Cloud Infrastructure? on page 805.

Using the Console

**To start all instances in a pool**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the instance pool that you're interested in.
3. Click Start.

**To stop all instances in a pool**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the instance pool that you're interested in.
3. Click Stop.
4. Click **Stop** again.

   The instances are shut down immediately, without waiting for the operating system to respond.

**To reboot all instances in a pool**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instance Pools**.
2. Click the instance pool that you're interested in.
3. Click **Reboot**.
4. By default, the Console gracefully restarts the instances by sending a shutdown command to the operating system. After waiting 15 minutes for the OS to shut down, the instances are powered off and then powered back on.

   **Note:**

   If the applications that run on the instances take more than 15 minutes to shut down, they could be improperly stopped, resulting in data corruption. To avoid this, **shut down the instances using the commands available in the OS** before you restart the instance using the Console.

   If you want to reboot the instances immediately, without waiting for the OS to respond, select the **Force reboot the instance pool by immediately powering off every instance in the pool, then powering them back on** checkbox.

5. Click **Reboot Instance Pool**.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage the lifecycle state of the instances in an instance pool, use these operations:

- StartInstancePool
- StopInstancePool
- ResetInstancePool
- SoftresetInstancePool

**Deleting an Instance Configuration**

You can permanently delete instance configurations that you no longer need.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to instance pools and instance configurations, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.

**Using the Console**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instance Configurations**.
2. Click the instance configuration that you're interested in.
3. Click **Delete**, and then confirm when prompted.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the **DeleteInstanceConfiguration** operation to delete an instance configuration.
Deleting an Instance Pool

You can permanently delete instance pools that you no longer need.

Caution:
When you delete an instance pool, the resources that were created by the pool are permanently deleted, including associated instances, attached boot volumes, and block volumes.

If an autoscaling configuration applies to the instance pool, the autoscaling configuration will be deleted asynchronously after the pool is deleted. You can also manually delete the autoscaling configuration.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to instance pools and instance configurations, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the instance pool that you're interested in.
3. Click More Actions, and then click Terminate.
4. Confirm when prompted.

To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the TerminateInstancePool operation to delete an instance pool.

Autoscaling

Autoscaling lets you automatically adjust the number of Compute instances in an instance pool. This helps you provide consistent performance for your end users during periods of high demand, and helps you reduce your costs during periods of low demand.

You can apply the following types of autoscaling to an instance pool:

- **Metric-based autoscaling**: An autoscaling action is triggered when a performance metric meets or exceeds a threshold.
- **Schedule-based autoscaling**: Autoscaling events take place at the specific times that you schedule.

Autoscaling is supported for virtual machine (VM) and bare metal instance pools that use Standard, DenseIO, and GPU shapes.

How Autoscaling Works: the Basics

You use autoscaling configurations to automatically manage the size of your instance pools. When autoscaling automatically provisions instances in an instance pool, the pool *scales out*. When autoscaling removes instances from the pool, the pool *scales in*.

When an instance pool scales in, instances are terminated in this order: the number of instances is balanced across availability domains, and then balanced across fault domains. Finally, within a fault domain, the oldest instance is terminated first.
An autoscaling configuration includes one or more autoscaling policies. These policies define the criteria that trigger autoscaling actions and the actions to take. Each autoscaling configuration can either have one metric-based autoscaling policy, or multiple schedule-based autoscaling policies. You can add a maximum of 50 schedule-based autoscaling policies to an autoscaling configuration.

Each instance pool can have only one autoscaling configuration.

**Metric-Based Autoscaling**

In metric-based autoscaling, you choose a performance metric to monitor, and set thresholds that the performance metric must reach to trigger an autoscaling event. When system usage meets a threshold, autoscaling dynamically resizes the instance pool in near-real time. As load increases, the pool scales out. As load decreases, the pool scales in.

**Tip:**

Avoid changing the value assigned to the initial number of instances after the pool has scaled. Lowering this value after the number of instances in the pool size has increased will cause instances in the pool to terminate. If you need to change this value, the new value should equal or exceed the number of instances currently in the pool.

Metric-based autoscaling relies on performance metrics that are collected by the Monitoring service, such as CPU utilization. These performance metrics are aggregated into one-minute time periods and then averaged across all instances in the instance pool. When three consecutive values (that is, the average metrics for three consecutive minutes) meet the threshold, an autoscaling event is triggered.

A cooldown period between metric-based autoscaling events lets the system stabilize at the updated level. The cooldown period starts when the instance pool reaches the Running state. Autoscaling continues to evaluate performance metrics during the cooldown period. When the cooldown period ends, autoscaling adjusts the instance pool's size again if needed.

**Schedule-Based Autoscaling**

Schedule-based autoscaling is ideal for instance pools where demand behaves predictably based on a schedule, such as a month, date, or time of day. Schedules can be recurring or one-time. For example:

- An instance pool has heavy use during business hours. The pool has lighter use on evenings and weekends. You can schedule the pool to scale out on weekday mornings, and to scale in on weekday evenings.
- An instance pool has high demand on New Years Eve. You can schedule the pool to scale out every year on December 30, and to scale in on January 2.
- You’re releasing a new application that runs in the instance pool, and expect that many people will start using the application after the public announcement. In advance, you can schedule the pool to scale out on the day of release.

A schedule-based autoscaling configuration can have multiple autoscaling policies, each with a different schedule and target pool size. If you want to configure scale-in and scale-out events, you must create at least two separate policies. One policy defines the target pool size and schedule for scaling in. The other policy defines the target pool size and schedule for scaling out.

After a schedule-based autoscaling policy is executed, the instance pool stays at the target pool size until something else changes the pool size, such as a different autoscaling policy. However, if you manually change the pool size, schedule-based autoscaling does not readjust the pool size until the next scheduled autoscaling policy is executed.

You define autoscaling schedules using cron expressions. Autoscaling uses the Quartz cron implementation. You can use an online cron expression generator to verify your cron expressions; one example is FREEFORMATTER.

Provide all times in UTC.

**Note:**

Schedule-based autoscaling configurations include an attribute for cooldown period, which you'll see in the Console and when using the API, SDKs, and...
About Cron Expressions

A cron expression is a string composed of six or seven fields that represent the different parts of a schedule, such as hours or days of the week. Cron expressions use this format:

<second> <minute> <hour> <day of month> <month> <day of week> <year>

The following table lists the values and special characters that are allowed for each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Allowed Values</th>
<th>Allowed Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td><strong>Note:</strong> When using the API, CLI, or SDKs for autoscaling, you must specify 0 as the value for seconds, even though other values will create a valid cron expression. You don't need to provide any value for seconds when using the Console.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minute</td>
<td>0-59</td>
<td>* - , /</td>
</tr>
<tr>
<td>Hour</td>
<td>0-23</td>
<td>* - , /</td>
</tr>
<tr>
<td>Day of the month</td>
<td>1-31</td>
<td>* - , ? / L W</td>
</tr>
<tr>
<td>Month</td>
<td>1-12 or JAN-DEC</td>
<td>* - , /</td>
</tr>
<tr>
<td>Day of the week</td>
<td>1-7 or SUN-SAT</td>
<td>* - , ? / L #</td>
</tr>
<tr>
<td>Year</td>
<td>1970-2099</td>
<td>* - , /</td>
</tr>
</tbody>
</table>

The special characters are described in the following table.

<table>
<thead>
<tr>
<th>Special Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Indicates all values for a field.</td>
<td>* in the month field means every month.</td>
</tr>
<tr>
<td>-</td>
<td>Indicates a range of values.</td>
<td>8-17 in the hour field means hours 8 through 17, or 8 a.m. through 5 p.m.</td>
</tr>
<tr>
<td>,</td>
<td>Indicates multiple values.</td>
<td>3,5 in the day-of-the-week field means Tuesday and Thursday.</td>
</tr>
<tr>
<td>?</td>
<td>Indicates no specific values.</td>
<td>0 0 10 ? * MON * means 10 a.m. on every Monday.</td>
</tr>
<tr>
<td>/</td>
<td>Use n/m to indicate increments. The value before the slash is the start time, and the number after the slash is the value to increment by.</td>
<td>0/20 in the minute field means the minutes 0, 20, and 40.</td>
</tr>
<tr>
<td>Special Character</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>L</td>
<td>Last day of the week or last day of the month. Use <code>xL</code> in the day-of-the-week field to indicate the last <code>x</code> day of the month. Use <code>L-n</code> in the day-of-the-month field to indicate an offset of <code>n</code> days from the last day of the month. Do not use <code>L</code> with multiple values or a range of values.</td>
<td>L in the day-of-the-month field means January 31, February 28 in non-leap years, and so on. 6L in the day-of-the-week field means the last Friday of the month. L-5 means 5 days before the last day of the month.</td>
</tr>
<tr>
<td>W</td>
<td>The weekday (Monday - Friday) that is nearest to the given day. The value does not cross months. Do not use <code>W</code> with multiple values or a range of values.</td>
<td>10W means the nearest weekday to the 10th of the month. If the 10th is a Saturday, it means Friday the 9th. If the 10th is a Sunday, it means Monday the 11th. If the 10th is a Wednesday, it means Wednesday the 10th.</td>
</tr>
<tr>
<td>#</td>
<td>Use <code>x#n</code> to indicate the <code>n</code>th <code>x</code> day of the month.</td>
<td>5#2 means the second Thursday of the month.</td>
</tr>
</tbody>
</table>
Example Cron Expressions

Use these example cron expressions as a starting point to create your own autoscaling schedules. Combine each cron expression with a target pool size to create an autoscaling policy. Then, include one or more autoscaling policies in an autoscaling configuration.

Goal: A one-time schedule with only one scaling event. At 11:00 p.m. on December 31, 2020, scale an instance pool to 100 instances. You'll need one autoscaling policy.

- Policy 1:
  - **Target pool size:** 100 instances
  - **Execution time:** 11:00 p.m. on the 31st day of December, in 2020
  - **Cron expression:** 0 0 23 31 12 ? 2020

Goal: A one-time schedule with a scale-out event and a scale-in event. At 10:00 a.m. on March 1, 2021, scale out to 75 instances. At 4 p.m. on March 7, 2021, scale in to 30 instances. You'll need two autoscaling policies.

- Policy 1 - scale out:
  - **Target pool size:** 75 instances
  - **Execution time:** 10:00 a.m. on the 1st day of March, in 2021
  - **Cron expression:** 0 0 10 1 3 ? 2021

- Policy 2 - scale in:
  - **Target pool size:** 30 instances
  - **Execution time:** 4:00 p.m. on the 7th day of March, in 2021
  - **Cron expression:** 0 0 16 7 3 ? 2021

Goal: A recurring daily schedule. On weekday mornings at 8:30 a.m., scale out to 10 instances. On weekday evenings at 6 p.m., scale in to two instances. You'll need two autoscaling policies.

- Policy 1 - morning scale out:
  - **Target pool size:** 10 instances
  - **Execution time:** 8:30 a.m. on every Monday through Friday, in every month, in every year
  - **Cron expression:** 0 30 8 ? * MON-FRI *

- Policy 2 - evening scale in:
  - **Target pool size:** 2 instances
  - **Execution time:** 6:00 p.m. on every Monday through Friday, in every month, in every year
  - **Cron expression:** 0 0 18 ? * MON-FRI *

Goal: A recurring weekly schedule. On Tuesdays and Thursdays, scale the pool to 30 instances. On all other days of the week, scale the pool to 20 instances. You'll need two autoscaling policies.

- Policy 1 - Tuesday and Thursday:
  - **Target pool size:** 30 instances
  - **Execution time:** 1 a.m. on every Tuesday and Thursday, in every month, in every year
  - **Cron expression:** 0 0 1 ? * TUE,THU *

- Policy 2 - all other days:
  - **Target pool size:** 20 instances
  - **Execution time:** 1 a.m. on Sunday through Monday, Wednesday, and Friday though Saturday, in every month, in every year
  - **Cron expression:** 0 0 1 ? * SUN-MON,WED,FRI-SAT *

Goal: A recurring monthly schedule. On all days of the month, set the pool size to 20 instances. On the 15th day of the month, scale out to 40 instances. You'll need two autoscaling policies.

- Policy 1 - daily pool size:
Compute

- **Target pool size**: 20 instances
- **Execution time**: Midnight on every day, in every month, in every year
- **Cron expression**: `0 0 0 * * ? *`
- Policy 2 - scale out:
  - **Target pool size**: 40 instances
  - **Execution time**: 12:05 a.m. on the 15th day of the month, in every month, in every year
  - **Cron expression**: `0 5 0 15 * ? *`

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to autoscaling configurations, see [Let users manage Compute autoscaling configurations](#) on page 2145.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see [Resource Tags](#) on page 211.

**Prerequisites**

- You have an instance pool. Optionally, you can attach a load balancer to the instance pool.
- For metric-based autoscaling, monitoring is enabled on the instances in the instance pool, and the Monitoring service is receiving metrics that are emitted by the instance. When you initially create an instance pool using instances that support monitoring, monitoring is enabled by default, regardless of the settings in the pool’s instance configuration.
- You have sufficient service limits to create the maximum number of instances that you want to scale to.

**Using the Console**

To create a metric-based autoscaling configuration

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Autoscaling Configurations.
2. Click Create Autoscaling Configuration.
3. On the Add Basic Details page, do the following:
   a. Enter a name for the autoscaling configuration. Avoid entering confidential information.
   b. Select the compartment to create the autoscaling configuration in.
   c. Select the Instance pool to apply the autoscaling configuration to.
   d. Show Tagging Options: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
4. Click Next.
5. On the **Configure Autoscaling Policy** page, select **Metric-Based Autoscaling**. Then, do the following:
   
a. Enter a name for the autoscaling policy. Avoid entering confidential information.
   
b. In the **Cooldown in seconds** box, enter the minimum amount of time to wait between scaling events. The cooldown period gives the system time to stabilize before rescaling. The minimum value is 300 seconds, which is also the default.
   
c. Select the **Performance metric** that triggers an increase or decrease in the number of instances in the instance pool.
   
d. In the **Scale-out rule** area, specify the threshold that the performance metric must reach to increase the pool size. Select a **Scale-out operator** and **Threshold percentage**. Then, enter the **Number of instances to add** to the pool.
   
   For example, when CPU utilization is greater than 90%, add 10 instances to the pool.
   
e. In the **Scale-in rule** area, specify the threshold that the performance metric must reach to decrease the pool size. Select a **Scale-in operator** and **Threshold percentage**. Then, enter the **Number of instances to remove** from the pool.
   
   For example, when CPU utilization is less than 20%, remove 5 instances from the pool.
   
f. In the **Scaling limits** area, specify the number of instances in the instance pool:
   
   - **Minimum number of instances**: The minimum number of instances that the pool is allowed to decrease to.
   
   - **Maximum number of instances**: The maximum number of instances that the pool is allowed to increase to.

   **Important:**
   
   The number of instances that can be provisioned is also limited by your tenancy’s service limits.

   - **Initial number of instances**: The number of instances to launch in the instance pool immediately after autoscaling is enabled. After autoscaling retrieves performance metrics, the number of instances is automatically adjusted from this initial number to a number that is based on the scaling limits that you set.

6. Click **Next**.

7. Review the autoscaling configuration, and then click **Create**.

   Autoscaling runs. The cooldown period starts when the instance pool's state changes from **Scaling** to **Running**.

### To create a schedule-based autoscaling configuration

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.

2. Click **Create Autoscaling Configuration**.

3. On the **Add Basic Details** page, do the following:

   a. Enter a name for the autoscaling configuration. Avoid entering confidential information.

   b. Select the compartment to create the autoscaling configuration in.

   c. Select the **Instance pool** to apply the autoscaling configuration to.

   d. **Show Tagging Options**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

4. Click **Next**.
5. On the **Configure Autoscaling Policy** page, select **Schedule-Based Autoscaling**. Then, do the following:
   
a. Enter a name for the autoscaling policy. Avoid entering confidential information.
   
b. In the **Target pool size** box, enter the number of instances that the pool should scale to at the scheduled time.
   
   **Important:**
   
The number of instances that can be provisioned is also limited by your tenancy’s *service limits*.
   
c. In the **Execution schedule** area, define the schedule for implementing this autoscaling policy in UTC. Use a Quartz cron expression. For more information about cron expressions, see *About Cron Expressions* on page 720.
   
d. To schedule additional scaling events, click **+ Another Policy** and then repeat the previous steps.

6. When you're finished, click **Next**.

7. Review the autoscaling configuration, and then click **Create**.

   Autoscaling runs at the scheduled time.

### To edit an autoscaling configuration

You can change these characteristics of an autoscaling configuration:

- Name
- For metric-based autoscaling, the cooldown period between autoscaling actions

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.
2. Click the autoscaling configuration that you're interested in.
3. Click **Edit**.
5. Click **Save Changes**.

### To edit an autoscaling policy

You can change these characteristics of an autoscaling policy:

- Name
- For metric-based autoscaling:
  - Which performance metric triggers an autoscaling action
  - The minimum and maximum number of instances
  - The initial number of instances that the pool should have immediately after you update the autoscaling policy

   **Caution:**
   
   If you specify a smaller initial number of instances than the current pool size, instances will be terminated.

- Scale-out and scale-in operators and thresholds
- The number of instances to add or remove
- For schedule-based autoscaling, you can edit the target pool size or schedule for an existing policy, delete an existing policy, or add a new policy

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.
2. Click the autoscaling configuration that you're interested in.
3. In the **Autoscaling Policies** area, click **Edit**.
5. Click **Save Changes**.

### To enable or disable a schedule-based autoscaling policy

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.
2. Click the autoscaling configuration that you're interested in.
3. In the **Autoscaling Policies** area, under **Status**, toggle the **Enabled** or **Disabled** switch.

**To disable an autoscaling configuration**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.
2. Click the autoscaling configuration that you're interested in.
3. Click **Disable**, and then confirm when prompted.

**To delete an autoscaling configuration**
When you delete an autoscaling configuration, the instance pool remains in its most recent state.
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.
2. Click the autoscaling configuration that you're interested in.
3. Click **Delete**, and then confirm when prompted.

**To manage tags for an autoscaling configuration**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Autoscaling Configurations**.
2. Click the autoscaling configuration that you're interested in.
3. Click the **Tags** tab to view or edit the existing tags. Or click **Add Tags** to add new ones.

For more information, see **Resource Tags** on page 211.

**Using the API**
For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the **Autoscaling API** to manage autoscaling configurations and policies.

To update the autoscaling configuration with a new instance pool, create a new instance configuration and then point the instance pool to the new configuration:

- First, create a new instance configuration with the desired settings. You can do this using the Console. For steps, see **Creating an Instance Configuration** on page 710. To do this using the API, use the **CreateInstanceConfiguration** operation.
- Next, update the instance pool used in the autoscaling configuration to point to the new instance configuration. To do this using the API, use the **UpdateInstancePool** operation to change the `instanceConfigurationId`. You cannot use the Console to update the instance configuration used by the instance pool.

**Managing Cluster Networks**
A cluster network is a pool of high performance computing (HPC) instances or GPU instances that are connected with a high-bandwidth, ultra low-latency network. Each node in the cluster is a bare metal machine located in close physical proximity to the other nodes. A remote direct memory access (RDMA) network between nodes provides latency as low as single-digit microseconds, comparable to on-premises HPC clusters.

Cluster networks are designed for highly demanding parallel computing workloads. For example:

- Computational fluid dynamics simulations for automotive or aerospace modeling
- Financial modeling and risk analysis
- Biomedical simulations
- Trajectory analysis and design for space exploration
- Artificial intelligence and big data workloads

Cluster networks are built on top of the **instance pools** feature. Most operations in the instance pool are managed directly by the cluster network, though you can monitor and add tags to the underlying instance pool.
For more information about how to access and store the data that you want to process in your cluster networks, see FastConnect Overview on page 3173, Overview of File Storage on page 1920, Overview of Object Storage on page 3392, and Overview of Block Volume on page 500.

**Supported Shapes**

The following shapes support cluster networks:

- BM.HPC2.36
- BM.GPU4.8

Typically, to be able to create the multiple HPC or GPU instances that are contained in a cluster network, you must request a service limit increase.

**Supported Regions and Availability Domains**

Cluster networks are supported in the following regions:

- Regions in the Oracle Cloud Infrastructure commercial realm:
  - Australia East (Sydney)
  - Australia Southeast (Melbourne)
  - Germany Central (Frankfurt)
  - Japan Central (Osaka)
  - Japan East (Tokyo)
  - Netherlands Northwest (Amsterdam)
  - South Korea Central (Seoul)
  - UK South (London)
  - US East (Ashburn)
  - US West (Phoenix)
  - US West (San Jose)
- Regions in the Government Cloud realms:
  - UK Gov South (London)
  - US Gov East (Ashburn)

The availability domain that you create the cluster network in must have cluster network-capable hardware.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to cluster networks, see Let users manage Compute instance configurations, instance pools, and cluster networks on page 2144.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 21.
Prerequisites

Create an instance configuration for the instance pool that is managed by the cluster network. To do this:

1. **Create an instance** with the following settings:
   - **Image or operating system**: Click *Change Image*, and then click *Oracle Images*. Select the Oracle HPC cluster networking image.
   - **Shape**: Click *Change Shape*. Select *Bare Metal Machine*. Then, select either the BM.HPC2.36 shape or the BM.GPU4.8 shape.
     
     For more information about these shapes, see *Compute Shapes* on page 655.

2. **Create an instance configuration** using the instance that you created in the previous step as a template.

   Optionally, you can delete the instance after you create the instance configuration.

Using the Console

To create a cluster network

1. Open the navigation menu. Under *Core Infrastructure*, go to *Compute* and click *Cluster Networks*.

2. Click *Create Cluster Network*.

3. Enter a name for the cluster network. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.

4. Select the compartment to create the cluster network in.

5. Select the **Availability Domain** to run the cluster network in. Only the availability domains with cluster network-capable hardware can be selected.

6. In the **Configure networking** section, specify the network that you want to use to administer the cluster network. This network is separate from the closed RDMA network between nodes within the cluster. Enter the following information:
   
   - **Virtual cloud network**: The virtual cloud network (VCN) for the cluster network.
   - **Subnet**: The subnet for the cluster network.

7. In the **Configure instance pool** section, enter the following:
   
   - **Instance pool name**: A name for the instance pool that is managed by the cluster network. Avoid entering confidential information.
   
   - **Number of instances**: The number of instances in the pool.

   - **Instance configuration**: Select the instance configuration to use when creating the instances in the cluster network's instance pool, as described in the prerequisites.

8. **Show Tagging Options**: Optionally, you can add tags. If you have permissions to create a resource, you also have permissions to add free-form tags to that resource. To add a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see *Resource Tags* on page 211. If you are not sure if you should add tags, skip this option (you can add tags later) or ask your administrator.

9. Click *Create Cluster Network*.

   To track the progress of the operation, you can monitor the associated work request. For more information, see *Using the Console to View Work Requests* on page 260.

   For cluster networks with 10 or more instances, the cluster network is created if the required number of instances is available and at least 95% of the instances in the pool launch successfully. For cluster networks with less than 10 instances, all instances in the pool must launch successfully. If the cluster network fails to launch, wait a few minutes, and then try creating it again.

To edit the name of a cluster network

1. Open the navigation menu. Under *Core Infrastructure*, go to *Compute* and click *Cluster Networks*.

2. Click the cluster network that you're interested in.

3. Click *Edit Name*.

4. Enter a new name. Avoid entering confidential information.

5. Click *Save Changes*.
To manage tags for a cluster network

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Cluster Networks**.
2. Click the cluster network that you're interested in.
3. Click the **Tags** tab to view or edit the existing tags. Or click **Add Tags** to add new ones.

For more information, see **Resource Tags** on page 211.

To delete a cluster network

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you delete a cluster network, all of its resources are permanently deleted, including associated instances, attached boot volumes, and block volumes.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Cluster Networks**.
2. Click the cluster network that you're interested in.
3. Click **Terminate**, and then confirm when prompted.

   To track the progress of the operation, you can monitor the associated work request. For more information, see **Using the Console to View Work Requests** on page 260.

Using the API

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to work with cluster networks:

- `CreateClusterNetwork`
- `GetClusterNetwork`
- `ListClusterNetworks`
- `ListClusterNetworkInstances`
- `UpdateClusterNetwork`
- `ChangeClusterNetworkCompartment`
- `TerminateClusterNetwork`

Dedicated Virtual Machine Hosts

The Oracle Cloud Infrastructure Compute service's dedicated virtual machine host feature gives you the ability to run Compute virtual machine (VM) instances on dedicated servers that are a single tenant and not shared with other customers. This feature lets you meet compliance and regulatory requirements for isolation that prevent you from using shared infrastructure. You can also use this feature to meet node-based or host-based licensing requirements that require you to license an entire server.

**Support and Limitations**

When you create a dedicated virtual machine host, you select a shape for the host. For the available shapes and shape details for dedicated virtual machine hosts, see **Dedicated Virtual Machine Host Shapes** on page 660. Note that there is a difference between the number listed for billed OCPUs compared to available OCPUs. This is because four OCPUs are reserved for virtual machine management.

You are billed for the dedicated virtual machine host as soon as you create it, but you are not billed for any of the individual VM instances you place on it. You will still be billed for image licensing costs if they apply to the image you are using for the VM instances.

For instances launched on a dedicated virtual machine host, all of the VM.Standard2 shapes are supported. For details about these shapes, see **VM Shapes** on page 658. Most of the Compute service features for VM instances are supported for instances running on dedicated virtual machine hosts, however the following features are not supported:
• Instance configurations
• Instance pools
• Autoscaling

Reboot migration is also not supported for dedicated virtual machine hosts. In this scenario, you need to manually migrate the instance. See Moving an Instance with Manual Migration on page 775 for this process.

You can mix VM instances with different shapes on the same dedicated virtual machine host. This might impact the maximum number of instances you can place on the dedicated virtual machine host. For more information, see Optimizing Capacity on your Dedicated Virtual Machine Host on page 733.

Managing Dedicated Virtual Machine Hosts

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The simplest policy to enable users to work with dedicated virtual machine hosts is listed in Let users manage Compute dedicated virtual machine hosts on page 2145. It gives the specified group access to launch instances on dedicated virtual machine hosts and manage dedicated virtual machine hosts.

See Let users launch Compute instances on dedicated virtual machine hosts on page 2146 for an example of a policy that allows users to launch instances on dedicated virtual machine hosts without giving them full administrator access to dedicated virtual machine hosts.

Creating a Dedicated Virtual Machine Host

You must create a dedicated virtual machine host before you can place any instances on it. When creating the dedicated virtual machine host, you select an availability domain and fault domain to launch it in. All the VM instances that you place on the host will subsequently be created in this availability domain and fault domain. You also select a compartment when you create the dedicated virtual machine host, but you can move the host to a new compartment later without impacting any of the instances placed on it. You can also create the instances in a different compartment than the dedicated virtual machine host, or move them to difference compartments after they have been launched.

To create a dedicated virtual machine host using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Dedicated Virtual Machine Hosts.
2. Click Create Dedicated Virtual Machine Host.
3. Enter the following information:
   • **Compartment**: The compartment for the dedicated virtual machine host.
   • **Name**: A user-friendly name or description. Avoid entering confidential information.
   • **Availability Domain**: The availability domain for the dedicated virtual machine host.
   • **Shape**: The shape to use for the dedicated virtual machine host.
4. Optionally, click Show Advanced Options. Then enter the following information:
   • **Fault Domain**: The fault domain for the dedicated virtual machine host.
   • **Tags**: Optionally, you can add tags. If you have permissions to create a resource, you also have permissions to add free-form tags to that resource. To add a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should add tags, skip this option (you can add tags later) or ask your administrator.
5. Click Create.

To create a dedicated virtual machine host using the CLI
Open a command prompt and run:

```
oci compute dedicated-vm-host create --dedicated-vm-host-shape DVH.Standard2.52 --wait-for-state ACTIVE --display-name <display_name> --availability-domain <availability_domain> --compartment-id <compartment_ID>
```

It can take up to 15 minutes for the dedicated virtual machine host to be fully created. It must be in the ACTIVE state before you can launch an instance on it.

To query the current state of a dedicated virtual machine host using the CLI, run the following command:

```
oci compute dedicated-vm-host get --dedicated-vm-host-id <dedicatedVMhost_ID>
```

**Deleting a Dedicated Virtual Machine Host**

**To delete a dedicated virtual machine host using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Dedicated Virtual Machine Hosts.
2. Click the dedicated virtual machine host that you want to delete.
3. Click Delete, and then confirm when prompted.

If you try to delete a dedicated virtual machine host that still has running instances hosted on it, the delete operation will fail. You need to ensure that all of the instances hosted on it have been terminated. To check if there are any instances still running on the dedicated virtual machine host, go to the Details page for the dedicated virtual machine host, and click Hosted Instances in the Resources section. Perform this step for each compartment in your tenancy that has instances running on the dedicated virtual machine host. To change the compartment for the Host Instances list, select a different compartment from the Table Scope drop-down list.

**To delete a dedicated virtual machine host using the CLI**

Open a command prompt and run:

```
oci compute dedicated-vm-host delete --dedicated-vm-host-id <dedicated_VM_host_ID>
```

Before you can delete a dedicated machine host, all of the instances running on it must be terminated.

To list the instances running on a dedicated virtual machine host using the CLI, run the following command:

```
oci compute dedicated-vm-host list --compartment-id <compartment_ID> --dedicated-vm-host-id <dedicatedVMhost_ID>
```

Run this command for every compartment in your tenancy that has instances running on the dedicated virtual machine host that you want to delete.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations for working with dedicated virtual machine hosts:

- CreateDedicatedVmHost
- DeleteDedicatedVmHost
- ListDedicatedVmHosts
- ListDedicatedVmHostShapes
- ListDedicatedVmHostInstances
- ListDedicatedVmHostInstanceShapes
- UpdateDedicatedVmHost
Compute

- ChangeDedicatedVmHostCompartment

Instances on Dedicated Virtual Machine Hosts

Placing an Instance on a Dedicated Virtual Machine Host

You place an instance on a dedicated virtual machine host at the time that you create the instance. The steps are the same as creating a regular instance, you just need specify that you want to create the instance on a dedicated virtual machine host when you create the instance. See Creating an Instance on page 695 for the steps to create an instance. Once you get to the Advanced Options section of the form, use the following steps to place the instance on a dedicated virtual machine host.

To place an instance on a dedicated virtual machine host using the Console

1. Perform the initial steps to create an instance based on an image and shape type that support placement on a dedicated virtual machine, until the advanced options.
2. Click Show Advanced Options, and then click the Placement tab.
3. Select the Dedicated host option.
4. Select the dedicated virtual machine host that you want to place the instance on.

Note:

Only dedicated virtual machine hosts with sufficient capacity to launch an instance based on the shape you have specified are displayed in the list. If you have a dedicated virtual machine host and it does not appear in the list, you must do one of the following things to place the instance on that dedicated virtual machine host:

- Terminate instances you no longer need on the dedicated virtual machine host to make capacity available.
- Choose another smaller shape for the instance you are trying to place on the dedicated virtual machine host.
- Create a new dedicated virtual machine host to place the instance on.

For more information, see Optimizing Capacity on your Dedicated Virtual Machine Host on page 733.

5. Click Create.

If you’re using the CLI or REST API to create the instance, pass the dedicated virtual machine host OCID in the optional parameter dedicatedVmHostId when you use the LaunchInstance operation. If you try to launch an instance with a shape that requires more capacity than what is available on the dedicated virtual machine host you are trying to place it on, the launch operation will fail. To avoid this, you can use the ListDedicatedVmHosts operation and pass the shape you want to use when launching the instance in the InstanceShapeNameQueryParam parameter. This will return all the dedicated virtual machine hosts that you can place the instance on.

The following example demonstrates how to call this operation in the CLI to return all the dedicated virtual machine hosts with sufficient capacity for you to place an instance launched using the VM.Standard2.16 shape:

```bash
oci compute dedicated-vm-host list --compartment-id <compartment_ID> --instance-shape-name VM.Standard2.16
```

Auditing your Dedicated Virtual Machine Host

To fully meet requirements for some compliance scenarios, you might be required to validate that your instances are running on a dedicated virtual machine host and not using shared infrastructure. The Oracle Cloud Infrastructure Audit service provides you with the functionality to do this. Use the steps described in Viewing Audit Log Events on page 494 to access the log events for the dedicated virtual machine host.

The steps described in the To search log events section walk you through how to retrieve the log events with the data you need to verify that your instances are running on a dedicated virtual machine host. For this procedure:
• Ensure that you select the dedicated virtual machine host's compartment and not the compartment for the instances that are hosted on it.

• Use the dedicated virtual machine host's OCID as the search keyword.

After you have retrieved the log events for the dedicated virtual machine host, view the log event lower-level details, and check the contents of the `responsePayload` property. This property should contain the OCIDs for the instances that are running on the dedicated virtual machine host.

**Optimizing Capacity on your Dedicated Virtual Machine Host**

When you place an instance on a dedicated virtual machine host using the Console, only dedicated virtual machine hosts with sufficient capacity to launch an instance based on the shape that you have specified are displayed in the **Dedicated Virtual Machine Host** drop-down list. If you don't see your dedicated virtual machine host in the list, to understand why, it can help to understand how instances are launched in this scenario.

When you place instances on a dedicated virtual machine host, Oracle Cloud Infrastructure launches the instances in a manner to optimize performance. For example, a dedicated virtual machine host created based on the **DVH.Standard2.52** shape has two sockets with 24 cores configured per socket. Instances are placed so that each instance will only use resources local to a single physical socket. In scenarios where you are creating and terminating instances with a mix of shapes, this can result in an inefficient distribution of resources, meaning that not all OCPUs on a dedicated virtual machine host are available to be used. In this scenario, it might appear that a dedicated virtual machine has enough OCPUs to launch an additional instance on it, but the instance will fail to launch because of the distribution of existing instances.

In this example, if you are launching instances using a shape with 16 OCPUs on a dedicated virtual machine host, you can only launch a maximum of two instances using that shape. You cannot launch a third instance with 16 OCPUs, even though the remaining number of OCPUs showing for the dedicated virtual machine host is 16. You can launch additional instances using shapes with a smaller number of OCPUs.

When designing your cloud footprint, we recommend that you plan to always launch the largest instance first.

**Connecting to an Instance**

You can connect to a running instance by using a Secure Shell (SSH) or Remote Desktop connection. Most UNIX-style systems include an SSH client by default. Windows 10 and Windows Server 2019 systems should include the **OpenSSH client**, which you'll need if you created your instance using the SSH keys generated by Oracle Cloud Infrastructure. For other Windows versions, you can download a free SSH client called PuTTY from [http://www.putty.org](http://www.putty.org).

**Required IAM Policy**

To connect to a running instance with SSH, you don't need an IAM *policy* to grant you access. However, to SSH you need the public IP address of the instance (see Prerequisites on page 734 below). If there's a policy that lets you launch an instance, that policy probably also lets you get the instance's IP address. The simplest policy that does both is listed in Let users launch compute instances on page 2143.

For administrators: Here's a more restrictive policy that lets the specified group get the IP address of existing instances and use power actions on the instances (e.g., stop, start, etc.), but not launch or terminate instances. The policy assumes the instances and the cloud network are together in a single compartment (XYZ):

```
Allow group InstanceUsers to read virtual-network-family in compartment XYZ
Allow group InstanceUsers to use instance-family in compartment XYZ
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.
Prerequisites

You'll need the following information to connect to the instance:

- The public IP address of the instance. You can get the address from the Instance Details page in the Console. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances. Then, select your instance. Alternatively, you can use the Core Services API ListVnicAttachments and GetVnic operations.
- The default username for the instance. If you used an Oracle-provided Linux, CentOS, or Windows image to launch the instance, the username is opc. If you used the Ubuntu image to launch the instance, the username is ubuntu.
- For Linux instances: The full path to the private key portion of the SSH key pair that you used when you launched the instance. For more information about key pairs, see Managing Key Pairs on Linux Instances on page 693.
- For Windows instances: If you're connecting to the instance for the first time, you will need the initial password for the instance. You can get the password from the Instance Details page in the Console.

Connecting to a Linux Instance

You connect to a Linux instance using SSH.

To connect to a Linux instance from a Unix-style system

1. Use the following command to set the file permissions so that only you can read the file:

   ```bash
   chmod 400 <private_key_file>
   ```

   `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.

2. Use the following SSH command to access the instance.

   ```bash
   ssh -i <private_key_file> <username>@<public-ip-address>
   ```

   `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.

   `<username>` is the default username for the instance. For Oracle Linux and CentOS images, the default username is opc. For Ubuntu images, the default username is ubuntu.

   `<public-ip-address>` is your instance IP address that you retrieved from the Console.

To connect to a Linux instance from a Windows system using OpenSSH

If the instance uses a key pair that was generated by Oracle Cloud Infrastructure, use the following procedure.

1. If this is the first time you are using this key pair, you must set the file permissions so that only you can read the file. Do the following:

   a. In Windows Explorer, navigate to the private key file, right-click the file, and then click Properties.


   c. Ensure that the Owner is your user account.

   d. Click Disable Inheritance, and then select Convert inherited permissions into explicit permissions on this object.

   e. Select each permission entry that is not your user account and click Remove.

   f. Ensure that the access permission for your user account is Full control.

   g. Save your changes.
2. To connect to the instance, open Windows PowerShell and run the following command:

```
ssh -i <private_key_file> <username>@<public-ip-address>
```

<private_key_file> is the full path and name of the file that contains the private key associated with the instance you want to access.

$username is the default username for the instance. For Oracle Linux and CentOS images, the default username is opc. For Ubuntu images, the default username is ubuntu.

<public-ip-address> is your instance IP address that you retrieved from the Console.

To connect to a Linux instance from a Windows system using PuTTY

SSH private key files generated by Oracle Cloud Infrastructure are not compatible with PuTTY. If you are using a private key file generated during the instance creation process you need to convert the file to a .ppk file before you can use it with PuTTY to connect to the instance.

Convert a generated .key private key file:

1. Open PuTTYgen.
2. Click Load, and select the private key generated when you created the instance. The extension for the key file is .key.
3. Click Save private key.
4. Specify a name for the key. The extension for new private key is .ppk.
5. Click Save.

Connect to the Linux instance using a .ppk private key file:

If the instance uses a key pair that you created using PuTTY Key Generator, use the following procedure.

1. Open PuTTY.
2. In the Category pane, select Session and enter the following:
   - Host Name (or IP address):
     <username>@<public-ip-address>
     <username> is the default username for the instance. For Oracle Linux and CentOS images, the default username is opc. For Ubuntu images, the default username is ubuntu.
     <public-ip-address> is your instance public IP address that you retrieved from the Console
   - Port: 22
   - Connection type: SSH
3. In the Category pane, expand Window, and then select Translation.
4. In the Remote character set drop-down list, select UTF-8. The default locale setting on Linux-based instances is UTF-8, and this configures PuTTY to use the same locale.
5. In the Category pane, expand Connection, expand SSH, and then click Auth.
6. Click Browse, and then select your .ppk private key file.
7. Click Open to start the session.

If this is your first time connecting to the instance, you might see a message that the server's host key is not cached in the registry. Click Yes to continue the connection.

Tip:

If the connection fails, you may need to update your PuTTY proxy configuration.

Connecting to a Windows Instance

You can connect to a Windows instance using a Remote Desktop connection. Most Windows systems include a Remote Desktop client by default.
To enable Remote Desktop Protocol (RDP) access to the Windows instance, you need to add a stateful ingress security rule for TCP traffic on destination port 3389 from source 0.0.0.0/0 and any source port. You can implement this security rule in either a network security group that the Windows instance belongs to, or a security list that is used by the instance's subnet.

**To enable RDP access**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the cloud network that you're interested in.
4. To add the rule to a network security group that the instance belongs to:
   a. Under **Resources**, click **Network Security Groups**. Then click the network security group that you're interested in.
   b. Click **Add Rules**.
   c. Enter the following values for the rule:
      - **Stateless**: Leave the check box cleared.
      - **Source Type**: CIDR
      - **Source CIDR**: 0.0.0.0/0
      - **IP Protocol**: RDP (TCP/3389)
      - **Source Port Range**: All
      - **Destination Port Range**: 3389
      - **Description**: An optional description of the rule.
   d. When done, click **Add**.
5. Or, to add the rule to a security list that is used by the instance's subnet:
   a. Under **Resources**, click **Security Lists**. Then click the security list you're interested in.
   b. Click **Add Ingress Rules**.
   c. Enter the following values for the rule:
      - **Stateless**: Leave the check box cleared.
      - **Source Type**: CIDR
      - **Source CIDR**: 0.0.0.0/0
      - **IP Protocol**: RDP (TCP/3389)
      - **Source Port Range**: All
      - **Destination Port Range**: 3389
      - **Description**: An optional description of the rule.
   d. When done, click **Add Ingress Rules**.

**Connecting to a Windows Instance from a Remote Desktop Client**

1. Open the Remote Desktop client.
2. In the **Computer** field, enter the public IP address of the instance. You can retrieve the public IP address from the Console.
3. The **User name** is opc. Depending on the Remote Desktop client you are using, you might have to connect to the instance before you can enter this credential.
4. Click **Connect** to start the session.
5. Accept the certificate if you are prompted to do so.
6. If you are connecting to the instance for the first time, enter the initial password that was provided to you by Oracle Cloud Infrastructure when you launched the instance. You will be prompted to change the password as
soon as you log in. Your new password must be at least 12 characters long and must comply with Microsoft's password policy.

Otherwise, enter the password that you created. If you are using a custom image, you might need to know the password for the instance that the image was created from. For details about Windows custom images, see Creating Windows Custom Images on page 668.

7. Press Enter.

Troubleshooting the SSH Connection

If you're unable to connect to your instance using SSH, follow these troubleshooting steps to identify common problems.

- **Verify your connection:** In your terminal window, run `nc <public ip> 22`.
  - **If the SSH banner displays:** You successfully connected to your instance using SSH. The underlying problem might be related to permissions. As a next step, verify your credentials. If the credentials you're using to SSH to the instance are incorrect, the connection fails.
    
    For Linux instances, you need the full path to the private key portion of the SSH key pair that you used when you launched the instance. For more information about key pairs, see Managing Key Pairs on Linux Instances on page 693. For Windows instances, if you're connecting to the instance for the first time, you need the initial password for the instance. You can get the password from the Instance Details page in the Console.
  - **If the SSH banner does not display:** A network issue might be preventing the SSH connection from succeeding. Review the following suggestions.
    
    - **Add a public IP address:** If your connection is routed over the internet, your instance must have a public IP address in order for you to connect to the instance. Without a public IP address, the instance is not reachable. For more information about how to manage public IPv4 addresses on instances, see Public IP Addresses on page 2875.
    
    - **Verify the network security lists:** Oracle Cloud Infrastructure provisions each cloud network with a default set of security lists to permit SSH traffic. If the security list that permits SSH connections is removed, you can’t access your instance. Ensure a security list that opens port 22 is present. You can use the Console to view and manage your security lists. For more information about security lists, see Security Lists on page 2850.
    
    - **Confirm that SSH is running on the instance:** The steps for confirming that SSH is running vary depending on the operating system. Review the documentation for your operating system to find information explaining how to confirm that SSH is running.
    
    - **Capture serial console history:** To capture your instance's serial console data history, use the `console-history` resource in the CLI. This information can help determine the cause of connectivity problems. For more information, see `console-history` and Command Line Interface (CLI) on page 4192.

    When using the CLI to capture the instance's serial console data history, you need to include the following option to ensure that full history is captured. Without this option, the data might be truncated: `--length 10000000`.

    - **Connect to the serial console:** Serial console connections allow you to remotely troubleshoot malfunctioning instances. For more information, see Troubleshooting Instances Using Instance Console Connections on page 813.

Adding Users on an Instance

You can add additional users to a Compute instance.

If you created your instance using an Oracle-provided Linux or CentOS image, you can use SSH to access your instance from a remote host as the `opc` user. If you created your instance using the Ubuntu image, you can use SSH to access your instance from a remote host as the `ubuntu` user. After signing in, you can add users to the instance.

If you created your instance using an Oracle-provided Windows image, you can create new users after you sign in to the instance through a Remote Desktop client.
Creating Additional Users on a Linux Instance

If you do not want to share your SSH key, you can create additional SSH-enabled users for a Linux instance. At a high level, you do the following things:

- Generate SSH key pairs for the users offline.
- Add the new users.
- Append a public key to the `~/.ssh/authorized_keys` file for each new user.

**Tip:**

If you re-create an instance from an Oracle-provided image, users and SSH public keys that you added or edited manually (that is, users that weren’t defined in the machine image) must be added again.

If you need to edit the `~/.ssh/authorized_keys` file of a user on your instance, start a second SSH session before you make any changes to the file and ensure that it remains connected while you edit the file. If the `~/.ssh/authorized_keys` file becomes corrupted or you inadvertently make changes that lock you out of the instance, you can use the backup SSH session to fix or revert the changes. Before closing the backup SSH session, test all changes you made by logging in with the new or updated SSH key.

The new users then can SSH to the instance using the appropriate private keys.

To create an additional SSH-enabled user:

1. Generate an SSH key pair for the new user.
2. Copy the public key value to a text file for use later in this procedure.
3. Log in to the instance.
4. Become the root user:

   sudo su

5. Create the new user:

   useradd <new_user>

6. Create a .ssh directory in the new user’s home directory:

   mkdir /home/<new_user>/.ssh

7. Copy the SSH public key that you saved to a text file into the /home/new_user/.ssh/authorized_keys file:

   echo <public_key> > /home/<new_user>/.ssh/authorized_keys

8. Change the owner and group of the /home/username/.ssh directory to the new user:

   chown -R <new_user>:<group> /home/<new_user>/.ssh

9. To enable sudo privileges for the new user, run the visudo command and edit the /etc/sudoers file as follows:

   a. In /etc/sudoers, look for:

      %<username> ALL=(ALL) NOPASSWD: ALL

   b. Add the following line immediately after the preceding line:

      %<group> ALL=(ALL) NOPASSWD: ALL

The new user can now sign in to the instance.

Creating Additional Users on a Windows Instance

1. Log in to the instance using a Remote Desktop client.
2. On the Start menu, click Control Panel.
3. Click User Accounts, and then click User Accounts again.
4. Click Manage User Accounts.
5. Click Manage Another Account.
6. Click Add User Account.
7. Enter a User name and Password.
8. Confirm the password, and then create a Password hint.
9. Click Next.
10. Verify the account, and then click Finish.

The new user can now sign in to the instance.

Displaying the Console for an Instance

You can capture and display the serial console data for an instance. The data includes configuration messages that occur when the instance boots, such as kernel and BIOS messages, and is useful for checking the status of the instance or diagnosing problems. Note that the raw console data, including multi-byte characters, is captured.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message
that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to manage console history data. If the specified group doesn’t need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368.

Use these API operations to manage the serial console logs:

- CaptureConsoleHistory
- DeleteConsoleHistory
- GetConsoleHistory
- GetConsoleHistoryContent
- ListConsoleHistories

**Managing Plugins with Oracle Cloud Agent**

Oracle Cloud Agent is a lightweight process that manages plugins running on compute instances. Plugins collect performance metrics, install OS updates, and perform other instance management tasks.

To use plugins on an instance, the Oracle Cloud Agent software must be installed on the instance, the plugins must be enabled, and the plugins must be running. You might need to perform additional configuration tasks before you can use certain plugins.

**Supported Images**

**Oracle Cloud Agent:** Oracle Cloud Agent is supported on current Oracle-provided images and on custom images that are based on current Oracle-provided images. Oracle Cloud Agent is installed by default on current Oracle-provided images.

If you use an older Oracle-provided image, you must manually install the Oracle Cloud Agent software. Select an image dated after November 15, 2018 (except Ubuntu, which must be dated after February 28, 2019).

You might have success manually installing Oracle Cloud Agent on other images, though it has not been tested on other operating systems and there is no guarantee that it will work. Oracle Cloud Agent is not supported on Windows Server 2008 R2 custom images.

**Plugins:** Plugins are installed as part of Oracle Cloud Agent. The plugins that are supported for an instance depend on the version of Oracle Cloud Agent and on the image that you use to create the instance. To determine which plugins are supported for a particular image, use the Console to create an instance. Or, use the ListInstanceagentAvailablePlugins API operation, providing the OS name and OS version of the image.

**Available Plugins**

Each Oracle Cloud Agent plugin provides functionality related to compute instances. This functionality can enable features that are part of the Compute service, and features that are part of other services.

The following Oracle Cloud Agent plugins are available.

<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Description</th>
<th>Steps to Configure and Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute Instance Monitoring</td>
<td>Emits metrics about the instance's health, capacity, and performance. These metrics are consumed by the Monitoring service.</td>
<td>See Enabling Monitoring for Compute Instances on page 783 and Compute Instance Metrics on page 788.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Description</td>
<td>Steps to Configure and Use</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Compute Instance Run Command</td>
<td>Runs scripts within the instance to remotely configure, manage, and troubleshoot the instance.</td>
<td>See Running Commands on an Instance on page 752.</td>
</tr>
<tr>
<td>Custom Logs Monitoring</td>
<td>Ingests custom logs into the Logging service.</td>
<td>See Custom Logs on page 2619.</td>
</tr>
<tr>
<td>OS Management Service Agent</td>
<td>Manages updates and patches for the operating system environment on the instance.</td>
<td>See OS Management.</td>
</tr>
</tbody>
</table>

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to enable and disable individual plugins, as well as start and stop all plugins on an instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family. In addition, you must use the following policy to allow users to access the available plugins:

```
Allow group PluginUsers to read instance-agent-plugins in compartment ABC
```

If you're new to policies, see Getting started with policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Installing the Oracle Cloud Agent Software**

If you create an instance using a current Oracle-provided image or a custom image that's based on a current Oracle-provided image, then Oracle Cloud Agent is installed by default. No action is needed.

If you want to manually install the Oracle Cloud Agent software on an instance that uses another supported image, use the following steps.

**To manually install Oracle Cloud Agent on a legacy Linux instance**

1. Connect to the instance.
2. To download the Oracle Cloud Agent software, run one of the following scripts.

   **Oracle Autonomous Linux, Oracle Linux**

   a. To determine whether the Oracle Cloud Agent software is installed, run the following command:

      ```
      sudo yum info oracle-cloud-agent
      ```
      
      The command returns the Oracle Cloud Agent version that is currently installed.

   b. If Oracle Cloud Agent isn't installed, or if the installed version is not the latest version, install the latest version by running the following command:

      ```
      sudo yum install -y oracle-cloud-agent
      ```

      **Note:**

      If you don't have access to the yum repository that has Oracle Cloud Agent, run one of the following scripts.
### Oracle Linux 6.x

```
#!/bin/sh
cd ~
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/
  uKbXkuu61IVKkRdQhxpg9C4bvnaxr0dqatbtuzq2k2V0XZrQw2cKFuzla_9jRNQc/
  n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3749.el6.x86_64.rpm -v
```

### Oracle Autonomous Linux 7.x, Oracle Linux 7.x

```
#!/bin/sh
cd ~
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/
  U_9mEBnaTqVKe_HVI26djz88N4QXG0kDGTA3izpxKtc5OI44TuukvKzgVrlJP8B/
  n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el7.x86_64.rpm -v
```

### Oracle Linux 8.x

```
#!/bin/sh
cd ~
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/
  tbPX4bNOSItrr3rIe2DTPj6F8n51HFKaSS81LHejzAu35tNuhxxfgyzUmo0QKCL9/
  n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el8.x86_64.rpm -v
```

### CentOS 7.x

```
#!/bin/sh
cd ~
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/
  U_9mEBnaTqVKe_HVI26djz88N4QxG0kDGTA3izpxKtc5OI44TuukvKzgVrlJP8B/n/
  imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el7.x86_64.rpm -v
```

### CentOS 8.x

```
#!/bin/sh
cd ~
```
Compute

```bash
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/tbPX4bN0SLr3p3r3e2DtpJP6F8n5iHFkasaS81LHkejzAu35tNuhxxfgyzUmQKCL9/n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el8.x86_64.rpm -v
```

**Ubuntu 16.04, Ubuntu 18.04**

**Note:**

To install Oracle Cloud Agent on instances that use Ubuntu images, **Snapcraft** must be installed on the instance. Install Snapcraft by running the following commands, in sequence:

```
sudo apt update

sudo apt install snapd
```

```
sudo snap install oracle-cloud-agent --classic
```

This command installs and runs the Oracle Cloud Agent software.

3. To run the Oracle Cloud Agent software on the instance, enter one of the following commands.

**Oracle Linux**

```
sudo yum install -y <instance-agent-filename>
```

**CentOS**

```
sudo yum install -y <instance-agent-filename>
```

**Ubuntu**

No further action is needed. The command in the previous step installs and runs the software.

**To manually install Oracle Cloud Agent on a legacy Windows instance**

1. Connect to the instance.
2. Download the Oracle Cloud Agent software from the following URL:

   ```
   https://objectstorage.us-phoenix-1.oraclecloud.com/p/GvqT-zkjDRzemw0FP740k-uQHzAl130EeydBeEw_BezvpyfMGczffTCPjm0p/n/imagegen/b/agents/o/OracleCloudAgentSetup_v1.8.0.msi
   ```
3. As a user with administrative privileges, enter the following command to run the Oracle Cloud Agent software on the instance.

   ```
   msiexec /qb /i <instance-agent-filename>
   ```

**To install Oracle Cloud Agent using cloud-init when creating an instance using a legacy image**

If you want to install Oracle Cloud Agent on an instance that uses an older image as part of the instance launch, you can provide a cloud-init script (cloudbase-init on Windows instances) when you create the instance.

1. Follow the steps to [create an instance](#), until the advanced options.
2. Click **Show Advanced Options**.
3. On the Management tab, in the Initialization Script section, select Paste cloud-init script. Then, copy and paste one of the following scripts, depending on the image.

**Oracle Linux**

```
sudo yum install -y oracle-cloud-agent
```

**Note:**
If you don't have access to the yum repository that has Oracle Cloud Agent, copy and paste one of the following scripts.

**Oracle Linux 6.x**

```
#!/bin/sh
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/UkBxKkuUa6TVKkRdQhxp9C4bvnaxr0dqatbtuzq2k2V0XZrQw2cKFuz1a_9jRNQc/n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3749.el6.x86_64.rpm
yum install -y ~/oracle-cloud-agent-1.8.2-3749.el6.x86_64.rpm -v
```

**Oracle Linux 7.x**

```
#!/bin/sh
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/U_9mEBnaTqVKu_HVI26djsZ8N4QxG0kDGTA3izpxKTC5O144TuukvKz9Vr1JP8B/n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el7.x86_64.rpm -v
yum install -y ~/oracle-cloud-agent-1.8.2-3843.el7.x86_64.rpm -v
```

**Oracle Linux 8.x**

```
#!/bin/sh
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/tbPX4bN0SsLrp3rIe2DTPjP6F8n5iHFKaSS81LHejzAu35tNuhxxfgyzUm0QKCL9/n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el8.x86_64.rpm -v
yum install -y ~/oracle-cloud-agent-1.8.2-3843.el8.x86_64.rpm -v
```

**CentOS 7.x**

```
#!/bin/sh
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/U_9mEBnaTqVKu_HVI26djsZ8N4QxG0kDGTA3izpxKTC5O144TuukvKz9Vr1JP8B/n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el7.x86_64.rpm -v
yum install -y ~/oracle-cloud-agent-1.8.2-3843.el7.x86_64.rpm -v
```

**CentOS 8.x**

```
#!/bin/sh
curl -O https://objectstorage.us-phoenix-1.oraclecloud.com/p/tbPX4bN0SsLrp3rIe2DTPjP6F8n5iHFKaSS81LHejzAu35tNuhxxfgyzUm0QKCL9/n/imagegen/b/agents/o/oracle-cloud-agent-1.8.2-3843.el8.x86_64.rpm -v
```
yum install -y ~/oracle-cloud-agent-1.8.2-3843.el8.x86_64.rpm -v

Ubuntu 16.04, Ubuntu 18.04

**Note:**
To install Oracle Cloud Agent on instances that use Ubuntu images, Snapcraft must be installed on the instance. Install Snapcraft by running the following commands, in sequence:

```
sudo apt update
sudo apt install snapd
```

```
sudo snap install oracle-cloud-agent --classic
```


**Note:**
For legacy versions of Windows images, ensure that cloudbase-init is supported. See WinRM and cloudbase-init on Windows images.

```
#ps1_sysnative
cd \Users\opc\Desktop
Start-BitsTransfer -Source "https://objectstorage.us-phoenix-1.oraclecloud.com/p/GvqT-zkjDRzemw0FP740kJHxAl130EEyidJbeEw_BezvpszIMGczIffTCpnjm0p/n/imagegen/b/agents/o/OracleCloudAgentSetup_v1.8.0.msi" -Destination "c:\Users\opc\Desktop\OracleCloudAgentSetup.msi"
msiexec /i "c:\Users\opc\Desktop\OracleCloudAgentSetup.msi" /quiet /L*V /V "c:\Users\opc\Desktop\OracleCloudAgentSetup.log"
```

4. Click **Create**.

**Managing Plugins Using the Console**

**To see which plugins are enabled for an instance**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click the **Oracle Cloud Agent** tab.
   The list of plugins is displayed. Enabled plugins can have the following statuses:
   - **RUNNING**: The plugin is running.
   - **STOPPED**: The plugin is stopped.
   - **NOT_SUPPORTED**: The plugin is not supported on this platform.
   - **INVALID**: The plugin status is not recognizable by the service.

**To enable or disable a plugin**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click the **Oracle Cloud Agent** tab.
4. Toggle the **Enabled** or **Disabled** switch for the plugin.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality that depends on the plugin, such as monitoring, autoscaling, or OS management, will not work when the plugin is disabled.</td>
</tr>
</tbody>
</table>

It takes up to 10 minutes for the change to take effect.

5. If you enabled a plugin, if necessary, perform any configuration tasks that are required before you can use the plugin. For information about how to configure each plugin, see the documentation for each plugin in Available Plugins on page 740.

### To stop all plugins on an instance

You can stop all of the plugins that are running on an instance. Any individual plugins that are enabled on the instance remain enabled, but the plugin processes stop running. The plugin processes will only start running again after you restart all plugins.

For example, if you want to troubleshoot plugins, you can stop all plugins and then disable the plugins that you think might have an error. Reenable the plugins one-by-one, restarting the plugins after you enable each plugin, to determine which plugin has an issue. For more information about troubleshooting plugins, see Generating a Diagnostic File for Oracle Cloud Agent on page 751.

To stop all plugins on an instance:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click the **Oracle Cloud Agent** tab.
4. Click **Stop Plugins**.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality that depends on plugins, such as monitoring, autoscaling, and OS management, will not work when all plugins are stopped.</td>
</tr>
</tbody>
</table>

5. Click **Stop Plugins**.

It might take several minutes for all plugins to stop. Oracle Cloud Agent continues to run when plugins are stopped.

### To start all plugins on an instance

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click the **Oracle Cloud Agent** tab.
4. Click **Start Plugins**.

It takes up to 10 minutes for the plugins to restart.

### Managing Plugins Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage Oracle Cloud Agent plugins:

- In the Core Services API:
  - **LaunchInstance** - enables or disables plugins, or stops all plugins, when you create an instance.
  - **GetInstance** and **ListInstances** - gets information about which plugins are enabled on an instance (or a list of instances).
  - **UpdateInstance** - enables or disables individual plugins, and stops or starts all plugins, for an existing instance.
• In the Oracle Cloud Agent API:
  • `ListInstanceAgentAvailablePlugins` - lists the plugins that are available for all instances. You can filter the results based on the image that you plan to use to launch an instance.
  • `ListInstanceAgentPlugins` - gets information about the plugins that are available on an existing compute instance.
  • `GetInstanceAgentPlugin` - gets information about a specific plugin on an existing compute instance.

**Updating the Oracle Cloud Agent Software**

We recommend always running the latest version of the Oracle Cloud Agent software.

If the instance can access the internet, then no action is needed. Oracle Cloud Agent periodically checks for newer versions and installs the latest version when an update is available.

If the instance does not have access to the internet, then you must manually update the Oracle Cloud Agent software. For example, a compute instance cannot access the internet if it does not have a public IP address, internet gateway, or service gateway. In this situation, Oracle Cloud Agent cannot complete its checks for newer versions.

*To see which version of Oracle Cloud Agent is installed*

**Connect to the instance** and then do one of the following things:

• For Oracle Linux and CentOS, run the following command:

  ```
  sudo yum info oracle-cloud-agent
  ```

• For Ubuntu, run the following command:

  ```
  snap info oracle-cloud-agent
  ```

• For Windows, do one of the following things:
  • In Control Panel, select **Programs and Features** and then find the version number provided for "Oracle Cloud Agent."
  • In PowerShell, run the following command:

    ```
    Get-WmiObject -Class Win32_Product | Where-Object { $_.Name -eq "Oracle Cloud Agent" }
    ```

    Example output:

    ```
    IdentifyingNumber : {exampleuniqueidentifier}
    Name              : Oracle Cloud Agent
    Vendor            : Oracle Corporation
    Version           : 0.0.10.0
    Caption           : Oracle Cloud Agent
    ```

*To manually update Oracle Cloud Agent on a compute instance*

Do one of the following things:

• Temporarily allow the instance to access the internet so that Oracle Cloud Agent can update itself.
• Redo the installation steps, using the latest version.

**Oracle Cloud Agent Release Notes**

**Linux versions**
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
</table>
| 1.8.3    | January 13, 2021   | Ubuntu instances only:  
  • Adds support to enable or disable individual plugins.  
  • Adds two new metrics for monitoring.  
  • Fix for updater start in new images.  
  • Updater fix for signature verification on packages.  
  • Adds support for reattachable plugins so that Oracle Cloud Agent can be upgraded without stopping plugins. |
| 1.8.2    | January 13, 2021   | Compute Instance Monitoring:  
  • Improve filtering of UNIX disk devices. |
| 1.8.1    | January 13, 2021   | OS Management Service Agent:  
  • Disabled by default. |
| 1.8.0    | January 13, 2021   | Adds support to enable or disable individual plugins.  
  Adds two new metrics for monitoring.  
  OS Management Service Agent:  
  • Enabled by default. |
| 1.7.1    | December 17, 2020  | Fix for updater start in new images.  
  OS Management Service Agent disabled in US Government Cloud. |
| 1.7.0    | December 7, 2020   | Updater fix for signature verification on packages.  
  Custom Logs Monitoring:  
  • Bug fix for signature verification.  
  • Add default bucket namespace for non-commercial realms. |
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
</table>
| 1.6.0   | November 6, 2020   | Adds support for reattachable plugins so that Oracle Cloud Agent can be upgraded without stopping plugins.  
Compute Instance Run Command:  
• Includes support for the run command feature in all regions in the Oracle Cloud Infrastructure commercial realm.  
Custom Logs Monitoring:  
• Enables package signature verification in CentOS.  
OS Management Service Agent:  
• Fixes the plugin to stop its process when it is requested to stop rather than staying up idle.  
• Fixes an upgrade kill cycle bug where OS Management upgrades Oracle Cloud Agent using yum, which then stops Oracle Cloud Agent, which stops the plugin. |
| 1.5.1   | October 27, 2020   | Includes support for the run command feature.                           |
| 1.4.1   | October 21, 2020   | Hotfix for agent termination of orphaned processes.                     |
| 1.4.0   | October 2, 2020    | Fixes in updater daemon and plugins to make them more resilient.        |
| 1.3.2   | September 9, 2020  | Fix auto update download directory permissions.                         
Minor enhancements to the Compute Instance Monitoring plugin. Enable additional plugins.  
Create grpc sockets in /var/lib/oracle-cloud-agent/tmp. |
| 1.2.0   | August 3, 2020     | Upgrade the agent to support plugins                                    |
| 0.0.19  | May 28, 2020       | Fix updater failing to run on images that mount a filesystem with noexec flag set, to /tmp.  
Use instance metadata to generate client side URLs.  
Includes support for the instance metadata service (IMDS) v2. |
| 0.0.18  | May 11, 2020       | Miscellaneous updates.                                                  |
### Compute

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.15</td>
<td>January 15, 2020</td>
<td>Migrate from Python 2.7.15 to Python 3.6.9.</td>
</tr>
<tr>
<td>0.0.13</td>
<td>November 4, 2019</td>
<td>Fix a bug in handling monitoring service internal server errors.</td>
</tr>
<tr>
<td>0.0.11</td>
<td>September 13, 2019</td>
<td>Fix retry strategy for sending metrics and refresh security tokens.</td>
</tr>
<tr>
<td>0.0.10</td>
<td>July 15, 2019</td>
<td>Fix for correct handling of forced termination of the oracle-cloud-agent-updater.</td>
</tr>
</tbody>
</table>

### Windows versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.8.0</td>
<td>January 13, 2021</td>
<td>Adds support to enable or disable individual plugins.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adds two new metrics for monitoring.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OS Management Service Agent:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enabled by default.</td>
</tr>
<tr>
<td>1.7.1</td>
<td>December 17, 2020</td>
<td>All plugins disabled in US Government Cloud.</td>
</tr>
<tr>
<td>1.7.0</td>
<td>December 7, 2020</td>
<td>Updater fix for signature verification on packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compute Instance Run Command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enabled for Windows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Custom Logs Monitoring:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add default bucket namespace for non-commercial realms.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OS Management Service Agent:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Clean up leftover OS Management temporary directories due to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OS Management being terminated on system reboot.</td>
</tr>
<tr>
<td>1.5.0.0</td>
<td>November 6, 2020</td>
<td>Adds support for reattachable plugins so that Oracle Cloud Agent can be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>upgraded without stopping plugins.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Custom Logs Monitoring plugin enabled in US Government Cloud realms.</td>
</tr>
<tr>
<td>1.4.1.0</td>
<td>October 2, 2020</td>
<td>Fixes in updater daemon and plugins to make them more resilient.</td>
</tr>
</tbody>
</table>
### Generating a Diagnostic File for Oracle Cloud Agent

To make it easier for Oracle support to help you troubleshoot issues with the Oracle Cloud Agent software, you can install the Oracle Cloud Agent diagnostic tool on your compute instances. When you run the diagnostic tool, it generates a file that contains debugging information and logs for the plugins that are managed by Oracle Cloud Agent.

**To generate a diagnostic file on a Linux instance**

1. Connect to the instance.
2. Download the diagnostic tool by running the following command:

   ```bash
curl https://objectstorage.us-phoenix-1.oraclecloud.com/p/nBzj8SEG2UHheMQ7XDKFWjF0eCuqfnHHHe0UdifZC90DgmXihFvJ42xw81qV5Kh7/n/imagegen/b/agents/o/oca-diagnostic-util-linux-01-12-21 > oca-diag-01-12-21
   ```

3. Change the permissions on the diagnostic tool to make it an executable:

   ```bash
   chmod 744 ./oca-diag-01-12-21
   ```
4. Run the diagnostic tool:

```bash
./oca-diag-01-12-21
```

The tool generates a TAR file with a name in the format `oca-diag-<date>.<identifier>.tar.gz`. Provide the file when you open your support request.

**To generate a diagnostic file on a Windows instance**

1. Connect to the instance.
2. Open PowerShell as an administrator. Then, download the diagnostic tool by running the following command:

```powershell
$url = "https://objectstorage.us-phoenix-1.oraclecloud.com/p/P57bTyJBYq0U2zSfW6jChEd70nUY0q0P7tEN9fv_2nXP40asMoAFaEEpEftEh_B/n/imagegen/b/agents/o/oca-diagnostic-util-win-11-01-20.ps1"
$output_file = "C:\Users\opc\oca-diag-11-01-20.ps1"
$wc.DownloadFile($url, $output_file)
```

**Note:**

If you get an error when you try to download the diagnostic tool, it might be due to the Transport Layer Security (TLS) version. Run the following command, and then try downloading the diagnostic tool again.

```powershell
```

3. Change directories to the folder where the diagnostic tool is saved:

```bash
cd C:\Users\opc
```

4. Run the diagnostic tool:

```bash
./oca-diag-11-01-20.ps1
```

The tool generates a ZIP file and saves it to `C:\Users\opc\Desktop\`. Provide the file when you open your support request.

**Running Commands on an Instance**

You can remotely configure, manage, and troubleshoot compute instances by running scripts within the instance using the run command feature.

For example, the run command feature can help you automate tasks such as configuring secondary virtual network interface cards (VNICs), joining instances to an identity provider, troubleshooting SSH connectivity, or responding to cross-region disaster recovery scenarios.

You can run commands on an instance even when the instance does not have SSH access or open inbound ports.

The run command feature uses the Compute Instance Run Command plugin that is managed by the Oracle Cloud Agent software.

**Caution:**

Do not use the run command feature to provide or retrieve passwords, secrets, or other confidential information in plain text. To securely provide and retrieve confidential information, use an Object Storage location to store the script file and response. Use Oracle Cloud Infrastructure Vault to manage keys and secret credentials.
Supported Images
The run command feature is supported on compute instances that use the following Oracle-provided images:

- Oracle Autonomous Linux
- Oracle Linux
- CentOS
- Windows Server

Custom images that are based on a supported Oracle-provided image also support the run command feature.

Supported Regions
The run command feature is supported in all regions in the Oracle Cloud Infrastructure commercial realm.

Limitations and Considerations

- The maximum size for a script file that you upload directly to an instance in plain text is 4 KB. To provide a larger file, save the file in an Object Storage location.
- The output of a script when returned as plain text is limited to the last 1 KB. To save a larger response, save the output to an Object Storage location.
- When you use an Object Storage location to save the script file or response, the instance must have outbound connectivity such as a Network Access Translation (NAT) gateway, service gateway, or internet gateway. The instance must also allow egress traffic on port 443 for the Oracle Cloud Agent software, Object Storage, and IAM.
- Two scripts can run at a time by default. To change the default, update the run command configuration file:

```bash
cat /etc/oracle-cloud-agent/plugins/runcommand/config.yml
```

Set the following parameters:

```
logDir: /var/log/oracle-cloud-agent/plugins/runcommand
commandExecutionMaxWorkers: <number-of-parallel-scripts>
```

- A maximum of five scripts can be in flight at a time. A script is considered to be in flight if it has been received by the Compute Instance Run Command plugin, but not yet deleted from the queue.
- To perform long-running tasks, you should use the run command feature to schedule a cron job on the instance. Command orchestration is not supported.
- Each script runs once. If you want a script to run multiple times, use cron to configure a schedule for the script.
- Scripts that prompt for information are not supported. However, you can use the instance metadata service (IMDS) to programatically retrieve information about the instance that the script runs on.
- The exit codes that are returned are standard Linux error codes. An exit code of 0 indicates success.
- If you apply an optional timeout for a script, the default is 1 hour. The maximum is 24 hours.
- The maximum time that a script can run is 1 day.
- To monitor the resources that scripts consume, such as CPU utilization, use metrics.
- Canceling a script is a best-effort attempt. Commands can't be canceled after they have finished running or if they have expired.
- Script files and responses that are saved in plain text are retained for one month. Script files and responses that are saved in an Object Storage location are retained until you delete them.
- Do not run a script that causes the Oracle Cloud Agent software or the Compute Instance Run Command plugin to stop.

Running Commands with Administrator Privileges
If a command requires sudo permissions, you must grant sudo permissions to the Compute Instance Run Command plugin to be able to run the command. The plugin runs as the ocarun user.
You can use cloud-init to configure permissions at instance launch, or connect to an instance after it has launched and configure permissions manually. Do the following:

1. On the instance, create a sudoers configuration file for the Compute Instance Run Command plugin:

   `vi ./101-oracle-cloud-agent-run-command`

2. Allow the `ocarun` user to run all commands as sudo by adding the following line to the configuration file:

   `ocarun ALL=(ALL) NOPASSWD:ALL`

   You can optionally list specific commands. See the Linux man page for `sudoers` for more information.

3. Validate that the syntax in the configuration file is correct:

   `visudo -cf ./101-oracle-cloud-agent-run-command`

   If the syntax is correct, the follow message is returned:

   `./101-oracle-cloud-agent-run-command: parsed OK`

4. Add the configuration file to `/etc/sudoers.d`:

   `sudo cp ./101-oracle-cloud-agent-run-command /etc/sudoers.d/`

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: To write policy for the run command feature, do the following:

1. **Create a group** that includes the users who you want to allow to issue commands, cancel commands, and view the command output for the instances in a compartment. Then, write the following policy to grant access for the group:

   `Allow group RunCommandUsers to manage instance-agent-command-family in compartment ABC`

2. **Create a dynamic group** that includes the instances that you want to allow commands to run on. For example, a rule inside the dynamic group can state:

   `any { instance.id = 'ocid1.instance.oc1.phx.<unique_ID_1>', 'ocid1.instance.oc1.phx.<unique_ID_2>' }`

3. Write the following policy to grant access for the dynamic group:

   ```
   Note:
   If you create an instance and then add it to a dynamic group, it takes up to 30 minutes for the instance to start to poll for commands. If you create the dynamic group first and then create the instance, the instance starts to poll for commands as soon as the instance is created.
   ```

   `Allow dynamic-group RunCommandDynamicGroup to use instance-agent-command-execution-family in compartment ABC where request.instance.id=target.instance.id`
4. To allow the dynamic group to access the script file from an Object Storage bucket and save the response to an Object Storage bucket, write the following policies:

```plaintext
Allow dynamic-group RunCommandDynamicGroup to read objects in compartment ABC where all {target.bucket.name = '<bucket_with_script_file>'}
Allow dynamic-group RunCommandDynamicGroup to manage objects in compartment ABC where all {target.bucket.name = '<bucket_for_command_output>'}
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Prerequisites**

- The Compute Instance Run Command plugin must be enabled on the instance, and plugins must be running. For more information about how to enable and run plugins, see Managing Plugins with Oracle Cloud Agent on page 740.
- For Oracle-provided images that were released before October 2020, the Oracle Cloud Agent software must be updated to a version that supports the Compute Instance Run Command plugin (version 1.5.1 or later).
- You have prepared the script that you want to run. On Linux instances, the script runs in a Bash shell. On Windows instances, the script runs in a batch shell. We recommend that you test the command in a non-production environment before deploying it on instances that run production workflows.
- To provide the script file from an Object Storage location, upload the file to an Object Storage bucket in the same region as the target instance. Note the bucket and file name, or the Object Storage URL for the file. To use the same command across tenancies, create a pre-authenticated request that points to the file.
- To save the command output to an Object Storage location, create a bucket to save it in, in the same region as the target instance. Note the bucket name or the Object Storage URL for the bucket. You can optionally save the command output using a pre-authenticated request that points to an Object Storage location.

**Using the Console**

**To create a command to run on an instance**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
4. Click Create Command.
5. Enter a name for the command. Avoid entering confidential information.
6. In the Timeout in seconds box, enter the amount of time to give the Compute Instance Run Command plugin to run the command on the instance before timing out. The timer starts when the plugin starts the command. For no timeout, enter 0.
7. In the Add script section, upload the script that you want the Compute Instance Run Command plugin to run on the instance. Select one of the following options:
   - **Paste script**: Paste the command in the box.
   - **Select a file**: Upload the script as a text (.txt) file. Either browse to the file that you want to upload, or drag and drop the file into the box.
   - **Import from an Object Storage bucket**: Select the bucket that contains the script file. In the Object name box, enter the file name.
   - **Import from an Object Storage URL**: Enter the Object Storage URL for the script file.
8. In the **Output type** section, select the location to save the output of the command:
   - **Output as text**: The output is saved as plain text. You can review the output on the Instance Details page.
   - **Output to an Object Storage bucket**: The output is saved to an Object Storage bucket. Select a bucket. In the **Object name** box, enter a name for the output file. Avoid entering confidential information.
   - **Output to an Object Storage URL**: The output is saved to an Object Storage URL. Enter the URL.

9. Click **Create Command**.

**To view the output of a command**

If the command output was saved to an Object Storage location, either download the response object from the bucket where it was saved or navigate to the Object Storage pre-authenticated request URL.

If the command output was saved as a plain text file, do the following:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Under **Resources**, click **Run Command**.
4. Find the command in the list, click the Actions icon (three dots), and then click **View Command Details**.

**To cancel a command**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Under **Resources**, click **Run Command**.
4. Find the command in the list, click the Actions icon (three dots), and then click **Cancel Command**. Confirm when prompted.

**Using the API**

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use these API operations to work with the run command feature:

- CreateInstanceAgentCommand
- GetInstanceAgentCommand
- GetInstanceAgentCommandExecution
- ListInstanceAgentCommands
- ListInstanceAgentCommandExecutions
- CancelInstanceAgentCommand

**Troubleshooting the Compute Instance Run Command Plugin**

To troubleshoot the Compute Instance Run Command plugin, you can view the logs that the plugin generates. Connect to the instance and then use the following:

```
tail -f /var/log/oracle-cloud-agent/plugins/runcommand/runcommand.log
```

For easier visibility into the plugin's operations without having to connect to the instance, you can create custom logs using the Oracle Cloud Infrastructure Logging service.

**Log Errors**

This section describes how to resolve errors that appear in the log file.

**Failure to Poll**

If the Compute Instance Run Command plugin is failing to poll for commands, you might see the following error in the log file:

This error can occur when the dynamic group policy for the run command feature is not enabled or if the instance was recently added to the dynamic group. Instances don't belong to tenancy administrator groups by default, so you need to explicitly set dynamic group permissions for the instance. For instructions explaining how to enable the dynamic group policy, see Required IAM Policy on page 754.

When you create an instance and then add it to a dynamic group, it takes up to 30 minutes for the instance to start to poll for commands. If you create the dynamic group first and then create the instance, the instance starts to poll for commands as soon as the instance is created.

To test the dynamic group policy as soon as you add the instance to a dynamic group, restart the service manually using one of the following commands:

**Oracle Linux 6.x**

```
sudo initctl restart oracle-cloud-agent
```

**Oracle Linux 7.x and Oracle Linux 8.x**

```
sudo systemctl restart oracle-cloud-agent
```

**Windows Server**

```
net restart ocarun
```

### Getting Instance Metadata

The instance metadata service (IMDS) provides information about a running instance, including a variety of details about the instance, its attached virtual network interface cards (VNICs), and any custom metadata that you define. IMDS also provides information to cloud-init that you can use for various system initialization tasks.

You can find some of this information in the Console on the **Instance Details** page, or you can get all of it by logging in to the instance and using the metadata service. The service runs on every instance and is an HTTP endpoint listening on 169.254.169.254. If an instance has multiple VNICs, you must send the request using the primary VNIC.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To increase the security of metadata requests, we strongly recommend that you update all applications to use the IMDS version 2 endpoint, if supported by the image. Then, disable requests to IMDS version 1.</td>
</tr>
</tbody>
</table>

### Upgrading to the Instance Metadata Service v2

The instance metadata service is available in two versions, version 1 and version 2. IMDSv2 offers increased security compared to v1.

When you disable IMDSv1 and allow requests only to IMDSv2, the following things change:

- All requests must be made to the v2 endpoints (/opc/v2). Requests to the v1 endpoints (/opc/v1 and /openstack) are rejected with a 404 not found error.
- All requests to the v2 endpoints must include an authorization header. Requests that do not include the authorization header are rejected.
- Requests that are forwarded using the HTTP headers Forwarded, X-Forwarded-For, or X-Forwarded-Host are rejected.

To upgrade the instance metadata service on a compute instance, use the following high-level steps:

1. Verify that the instance uses an image that supports IMDSv2.
2. Identify requests to the legacy v1 endpoints.
3. Migrate all applications to support the v2 endpoints.
4. Disable all requests to the legacy v1 endpoints.

**Supported Images for IMDSv2**

IMDSv2 is supported on the following Oracle-provided platform images:

- Oracle Autonomous Linux 7.x images released in June 2020 or later
- Oracle Linux 8.x, Oracle Linux 7.x, and Oracle Linux 6.x images released in July 2020 or later

Other Oracle-provided platform images, most custom images, and most Marketplace images images do not support IMDSv2. Custom Linux images might support IMDSv2 if cloud-init is updated to version 20.03 or later and Oracle Cloud Agent is updated to version 0.0.19 or later. Custom Windows images might support IMDSv2 if Oracle Cloud Agent is updated to version 1.0.0.0 or later; cloudbase-init does not support IMDSv2.

**Identifying Requests to the Legacy IMDSv1 Endpoints**

To identify the specific IMDS endpoints that requests are being made to, and the agents that are making the requests, use the InstanceMetadataRequests metric.

To identify which versions of IMDS are enabled for an instance, do either of the following things:

- **Using the Console:**
  1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
  2. Click the instance that you're interested in.
  3. In the Instance Details section, next to Instance Metadata Service, note the version numbers.

- **Using the API:** Use the GetInstance operation or the ListInstances operation. In the response, the areLegacyImdsEndpointsDisabled attribute in the InstanceOptions object returns false if both IMDSv1 and IMDSv2 are enabled for the instance. It returns true if IMDSv1 is disabled.

**Disabling Requests to the Legacy IMDSv1 Endpoints**

After you migrate all applications so that they make requests only to the IMDSv2 endpoints, you should disable all requests to the legacy IMDSv1 endpoints.

**Important:**

Verify that the instance does not use the IMDSv1 endpoints before you disable requests to IMDSv1. If the instance still relies on IMDSv1 when you disable requests to it, you might lose some functionality.

Do either of the following things:

- **Using the Console:**
  1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
  2. Click the instance that you're interested in.
  3. In the Instance Details section, next to Instance Metadata Service, click Edit.
  4. For Allowed IMDS version, select the Version 2 only option.
  5. Click Save Changes.

- **Using the API:** Use the UpdateInstance operation. In the request body, in the InstanceOptions object, pass the value true for the areLegacyImdsEndpointsDisabled attribute.

**Note:**

If you disable IMDSv1 on an instance that does not support IMDSv2, you might not be able to connect to the instance when you launch it. To reenable IMDSv1: using the Console, on the Instance Details page, next to Instance Metadata Service, click Edit. Select the Version 1 and version 2 option,
Required IAM Policy

No IAM policy is required if you're logged in to the instance and using cURL to get the metadata.

For administrators: Users can also get instance metadata through the Compute API (for example, with GetInstance). The policy in Let users launch compute instances on page 2143 covers that ability. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

To require that legacy IMDSv1 endpoints are disabled on any new instances that are created, use the following policy:

```
Allow group InstanceLaunchers to manage instances in compartment ABC
where request.instanceOptions.areLegacyEndpointsDisabled = 'true'
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Getting Instance Metadata on Oracle-Provided Images

You can get instance metadata for Oracle-provided images by using cURL on Linux instances. On Windows instances, you can use cURL (if supported by the Windows version) or an internet browser.

All requests to the instance metadata service v2 must include the following header:

```
Authorization: Bearer Oracle
```

Instance metadata accessed using IMDSv2 is available at the following root URLs:

- All of the instance information:
  

- Information about the VNICs that are attached to the instance:
  

Instance metadata accessed using IMDSv1 is available at the following root URLs. No header is necessary.

- All of the instance information:
  

- Information about the VNICs that are attached to the instance:
  

The values for specific metadata keys are available as sub-paths below the root URL.

To get instance metadata for Linux instances

1. Connect to a Linux instance using SSH.
2. Use cURL to issue a GET request to the instance metadata URL that you're interested in. For example:

   ```
```
To get instance metadata for Windows instances

The steps to get metadata on a Windows instance depend on which version of the instance metadata service you're requesting metadata from.

To get Windows instance metadata using IMDSv2:
1. Connect to a Windows instance by using a Remote Desktop connection.
2. Depending on whether your Windows version includes cURL, do either of the following:
   - If your Windows version includes cURL, use cURL to issue a GET request to the instance metadata URL that you're interested in. For example:
     
     ```bash
     ```
   - If your Windows version does not include cURL, you can get instance metadata in your internet browser. Navigate to the instance metadata URL that you're interested in, and pass a request that includes the authorization header. See the instructions for your browser for more information about including headers in a request. You might need to install a third-party browser extension that lets you include request headers.

To get Windows instance metadata using IMDSv1:
1. Connect to a Windows instance by using a Remote Desktop connection.
2. Open an internet browser and then navigate to the instance metadata URL that you're interested in.

Metadata Keys

The instance metadata includes default metadata keys that are defined by Compute and cannot be edited, as well as custom metadata keys that you create.

Some metadata entries are directories that contain additional metadata keys. In the following tables, entries with a trailing slash indicate a directory. For example, `regionInfo/` is a directory that contains other metadata keys.

Metadata Keys for an Instance

The following metadata is available about an instance. The paths are relative to `http://169.254.169.254/opc/v2/instance/`.

<table>
<thead>
<tr>
<th>Metadata Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availabilityDomain</td>
<td>The availability domain the instance is running in. This name includes the tenancy-specific prefix for the availability domain name. Example: Uocm:PHX-AD-1</td>
</tr>
<tr>
<td>faultDomain</td>
<td>The name of the fault domain the instance is running in. Example: FAULT-DOMAIN-1</td>
</tr>
<tr>
<td>compartmentId</td>
<td>The OCID of the compartment that contains the instance.</td>
</tr>
<tr>
<td>displayName</td>
<td>The user-friendly name of the instance.</td>
</tr>
<tr>
<td>hostname</td>
<td>The hostname of the instance.</td>
</tr>
<tr>
<td>id</td>
<td>The OCID of the instance.</td>
</tr>
<tr>
<td>image</td>
<td>The OCID of the image used to boot the instance.</td>
</tr>
<tr>
<td>Metadata Entry</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>metadata/</td>
<td>A directory containing any custom metadata that you provide for the instance.</td>
</tr>
<tr>
<td></td>
<td>To query the metadata for a specific custom metadata key, use <code>metadata/&lt;key-name&gt;</code>, where <code>&lt;key-name&gt;</code> is the name of the key that you defined when creating the instance.</td>
</tr>
<tr>
<td>metadata/sshAuthorizedKeys</td>
<td>For Linux instances, the public SSH key that was provided when creating the instance.</td>
</tr>
<tr>
<td>metadata/user_data</td>
<td>User data to be used by cloud-init or cloudbase-init to run custom scripts or provide custom configuration.</td>
</tr>
<tr>
<td>region</td>
<td>The <code>region</code> that contains the availability domain the instance is running in.</td>
</tr>
<tr>
<td></td>
<td>For the us-phoenix-1 and us-ashburn-1 regions, <code>phx</code> and <code>iad</code> are returned, respectively. For all other regions, the full region identifier is returned.</td>
</tr>
<tr>
<td></td>
<td>Examples: <code>phx</code>, <code>eu-frankfurt-1</code></td>
</tr>
<tr>
<td>canonicalRegionName</td>
<td>The region identifier for the <code>region</code> that contains the availability domain the instance is running in.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>us-phoenix-1</code></td>
</tr>
<tr>
<td>ociAdName</td>
<td>The availability domain the instance is running in. This name is used internally and corresponds to the data center label.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>phx-ad-1</code></td>
</tr>
<tr>
<td>regionInfo/</td>
<td>A directory containing information about the <code>region</code> that contains the availability domain the instance is running in.</td>
</tr>
<tr>
<td>regionInfo/realmKey</td>
<td>The key for the <code>realm</code> that the region is in.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>ocl</code></td>
</tr>
<tr>
<td>regionInfo/realmDomainComponent</td>
<td>The domain for the realm.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>oraclecloud.com</code></td>
</tr>
<tr>
<td>regionInfo/regionKey</td>
<td>The 3-letter key for the <code>region</code>.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>PHX</code></td>
</tr>
<tr>
<td>regionInfo/regionIdentifier</td>
<td>The region identifier.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>us-phoenix-1</code></td>
</tr>
<tr>
<td>shape</td>
<td>The <code>shape</code> of the instance. The shape determines the number of CPUs and the amount of memory allocated to the instance. You can enumerate all available shapes by calling the <code>ListShapes</code> operation.</td>
</tr>
<tr>
<td>Metadata Entry</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>state</td>
<td>The current lifecycle state of the instance. For a list of allowed values, see Instance. Example: Running</td>
</tr>
<tr>
<td>timeCreated</td>
<td>The date and time the instance was created, in the format defined by RFC3339.</td>
</tr>
<tr>
<td>agentConfig/</td>
<td>A directory containing information about the Oracle Cloud Agent software running on the instance.</td>
</tr>
<tr>
<td>agentConfig/monitoringDisabled</td>
<td>A Boolean value indicating whether the Oracle Cloud Agent software can gather performance metrics and monitor the instance.</td>
</tr>
<tr>
<td>agentConfig/managementDisabled</td>
<td>A Boolean value indicating whether the Oracle Cloud Agent software can run all the available management plugins.</td>
</tr>
<tr>
<td>freeformTags/</td>
<td>A directory containing any free-form tags that are added to the instance.</td>
</tr>
<tr>
<td>definedTags/</td>
<td>A directory containing any defined tags that are added to the instance.</td>
</tr>
</tbody>
</table>

Here's an example response that shows all of the information for an instance:

```json
{
  "availabilityDomain" : "EMIr:PHX-AD-1",
  "faultDomain" : "FAULT-DOMAIN-3",
  "compartmentId" : "ocid1.tenancy.oc1..exampleuniqueID",
  "displayName" : "my-example-instance",
  "hostname" : "my-hostname",
  "id" : "ocid1.instance.oc1.phx.exampleuniqueID",
  "image" : "ocid1.image.oc1.phx.exampleuniqueID",
  "metadata" : {
    "ssh_authorized_keys" : "example-ssh-key"
  },
  "region" : "phx",
  "canonicalRegionName" : "us-phoenix-1",
  "ociAdName" : "phx-ad-1",
  "regionInfo" : {
    "realmKey" : "ocl",
    "realmDomainComponent" : "oraclecloud.com",
    "regionKey" : "PHX",
    "regionIdentifier" : "us-phoenix-1"
  },
  "shape" : "VM.Standard.E3.Flex",
  "state" : "Running",
  "timeCreated" : 1600381928581,
  "agentConfig" : {
    "monitoringDisabled" : false,
    "managementDisabled" : false
  },
  "freeformTags" : {
    "Department" : "Finance"
  },
  "definedTags" : {
    "Operations" : {
      "CostCenter" : "42"
    }
  }
}
```
Metadata Keys for Attached VNICs

The following metadata is available about the VNICs that are attached to the instance. The paths are relative to http://169.254.169.254/opc/v2/vnics/.

<table>
<thead>
<tr>
<th>Metadata Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vnicId</td>
<td>The OCID of the VNIC.</td>
</tr>
<tr>
<td>privateIp</td>
<td>The private IP address of the primary privateIp object on the VNIC. The address is within the CIDR of the VNIC’s subnet.</td>
</tr>
<tr>
<td>vlanTag</td>
<td>The Oracle-assigned VLAN tag of the attached VNIC. If the VNIC belongs to a VLAN as part of the Oracle Cloud VMware Solution, the vlanTag value is instead the value of the vlanTag attribute for the VLAN. See Vlan.</td>
</tr>
<tr>
<td>macAddr</td>
<td>The MAC address of the VNIC. If the VNIC belongs to a VLAN as part of the Oracle Cloud VMware Solution, the MAC address is learned. If the VNIC belongs to a subnet, the MAC address is a static, Oracle-provided value.</td>
</tr>
<tr>
<td>virtualRouterIp</td>
<td>The IP address of the virtual router.</td>
</tr>
<tr>
<td>subnetCidrBlock</td>
<td>The subnet’s CIDR block.</td>
</tr>
<tr>
<td>nicIndex</td>
<td>Which physical network interface card (NIC) the VNIC uses. Certain bare metal instance shapes have two active physical NICs (0 and 1). If you add a secondary VNIC to one of these instances, you can specify which NIC the VNIC will use. For more information, see Virtual Network Interface Cards (VNICs) on page 2855.</td>
</tr>
</tbody>
</table>

Here’s an example response that shows the VNICs that are attached to an instance:

```json
[ {
  "vnicId" : "ocid1.vnic.oc1.phx.exampleuniqueID",
  "privateIp" : "10.0.3.6",
  "vlanTag" : 11,
  "macAddr" : "00:00:00:00:00:01",
  "virtualRouterIp" : "10.0.3.1",
  "subnetCidrBlock" : "10.0.3.0/24",
  "nicIndex" : 0
}, {
  "vnicId" : "ocid1.vnic.oc1.phx.exampleuniqueID",
  "privateIp" : "10.0.4.3",
  "vlanTag" : 12,
  "macAddr" : "00:00:00:00:00:02",
  "virtualRouterIp" : "10.0.4.1",
  "subnetCidrBlock" : "10.0.4.0/24",
  "nicIndex" : 0
}
]```
Updating Instance Metadata

You can add and update custom metadata for a compute instance using the Command Line Interface (CLI) on page 4192 or REST APIs on page 4368.

When you create an instance using the LaunchInstance operation, you can specify custom metadata for the instance in the LaunchInstanceDetails datatype's metadata or extendedMetadata attributes.

To update an instance's metadata, use the UpdateInstance operation, specifying the custom metadata in the UpdateInstanceDetails datatype's metadata or extendedMetadata attributes.

The metadata attribute supports key/value string pairs. The extendedMetadata attribute supports nested JSON objects. The combined size of these two attributes can be a maximum of 32,000 bytes.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to update instance metadata. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Using the API

When you use the UpdateInstance operation, the instance's metadata will be the combination of the values specified in the UpdateInstanceDetails datatype's metadata or extendedMetadata attributes. Any set of key/value pairs specified for these attributes in the UpdateInstance operation will replace the existing values for these attributes, so you need to include all the metadata values for the instance in each call, not just the ones you want to add. If you leave the attribute empty when calling UpdateInstance, the existing metadata values in that attribute will be used. You cannot specify a value for the same metadata key twice, as this will cause the UpdateInstance operation to fail due to there being duplicate keys.

To understand this, consider the example scenario where you created an instance using the LaunchInstance operation and specified the following key/value pair for the metadata attribute:

"myCustomMetadataKey" : "myCustomMetadataValue"

If you then call the UpdateInstance operation, and add new metadata by specifying additional key/value pairs in the extendedMetadata attribute, but you leave the metadata attribute empty, do not include the myCustomMetadataKey key/value in the extendedMetadata attribute, as this will cause the operation to fail since that key already exists. If you do specify values for the metadata attribute, you need to include the myCustomMetadataKey key/value to maintain it in the instance's metadata. In this case, you can specify it in either of the attributes.

There are two reserved keys, user_data and ssh_authorized_keys, that can only be set for an instance at launch time, they cannot be updated later. If you use the metadata attribute to add or update metadata for an instance, you need to ensure that you include the values specified at launch time for both these keys, otherwise the UpdateInstance operation will fail.

Best Practices for Updating an Instance's Metadata

When using the UpdateInstance operation, we recommend the following:
• Use the GetInstance operation to retrieve the existing custom metadata for the instance to ensure that you include the values you want to maintain in the appropriate attributes when you call UpdateInstance. The metadata values are returned in the metadata and extendedMetadata attributes for the Instance. For a code example demonstrating this, see the UpdateInstanceExample in the SDK for Java on page 4225.
• Unless you are updating custom metadata that was added using the metadata attribute, use the extendedMetadata attribute to add custom metadata. Otherwise you need to include the launch time values for the user_data and ssh Authorized_keys reserved keys. If you use the metadata attribute to add values and you leave out the values for these reserved keys or specify different values for them, the UpdateInstance call will fail.

Editing an Instance

You can edit the properties of a compute instance without having to rebuild the instance or redeploy your applications.

On supported instances, you can edit the following properties:
• Name. See Renaming an Instance on page 765.
• The shape that's used for the instance. Changing the shape affects the processor, number of OCPUs, memory, and other resources that are allocated to the instance. This lets you scale up your Compute resources for increased performance, or scale down to reduce cost. See Changing the Shape of an Instance on page 766.
• The fault domain where the instance is placed. You can distribute your instances across fault domain to protect against unexpected hardware failures or maintenance outages. See Editing the Fault Domain for an Instance on page 768.
• The launch options for the instance, which include the following properties:
  • The networking type for the virtual network interface card (VNIC). The networking interface handles functions such as disk input/output and network communication. Choose between paravirtualized and hardware-assisted (SR-IOV) networking. Paravirtualized networking provides more management flexibility. SR-IOV networking offers better performance.
  • The boot volume attachment type. Choose between paravirtualized and iSCSI attachment types.

  See Editing the Launch Options for an Instance on page 769.
• Whether in-transit encryption is used for the boot volume or block volume. See Enabling In-Transit Encryption Between an Instance and Boot Volumes or Block Volumes on page 773.
• Whether a running instance is recovered to the same lifecycle state or stopped after a maintenance event affects the underlying infrastructure. See Setting Instance Availability During Maintenance Events on page 774.

When you edit an instance, the instance's OCID remains the same.

Renaming an Instance

You can rename an instance without changing its Oracle Cloud Identifier (OCID).

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to rename an instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.
Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click Edit.
4. Enter a new name. Avoid entering confidential information.
5. Click Save Changes.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to rename an instance:

- UpdateInstance

Changing the Shape of an Instance

You can change the shape of a virtual machine (VM) instance without having to rebuild your instances or redeploy your applications. This lets you scale up your Compute resources for increased performance, or scale down to reduce cost.

When you change the shape of an instance, it affects the number of OCPUs, amount of memory, network bandwidth, and maximum number of VNICs for the instance. Optionally, you can select a shape that uses a different processor. The instance's public and private IP addresses, volume attachments, and VNIC attachments remain the same.

Supported Shapes

The shape series and image of the original shape determine which shapes you can select as a target for the new shape. You can resize instances that use these shapes:

- **VM.Standard.E2, VM.Standard2, VM.Standard.B1, and VM.Standard1 series:**
  - For Linux images, the shape can be changed to any fixed shape in the VM.Standard.E2, VM.Standard2, VM.Standard.B1, or VM.Standard1 series. The shape can also be changed to the VM.Standard.E3 series flexible shape.
  - For Windows images, the shape can be changed to a new shape only within the same series. For example, you can change a VM.Standard2.1 shape to a VM.Standard2.2 shape, but you can't change a VM.Standard2.1 shape to a VM.Standard1.1 shape.

- **VM.Standard.E3 series:** You can change the number of OCPUs and the amount of memory allocated to a VM.Standard.E3 series flexible shape. For Linux images, a flexible shape can also be changed to any fixed shape in the VM.Standard.E2, VM.Standard2, VM.Standard.B1, or VM.Standard1 series.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Windows Server 2019 instances, resize a VM.Standard.E3 shape to a maximum of 32 OCPUs. See this known issue for more information.</td>
</tr>
</tbody>
</table>

- **VM.GPU3 series:** Can be changed to any shape in the VM.GPU3 series.

These shapes cannot be changed:

- VM.Standard.E2.1.Micro series
- VM.GPU2 series
- VM instances that run on dedicated virtual machine hosts
- Bare metal shapes
Limitations and Considerations

Be aware of the following information:

• The image that's used to launch the instance must be compatible with the new shape. To see which shapes are compatible, do either of the following things:
  
  • In the Console, on the Instance Details page, click the name of the image. Then, refer to the list of compatible shapes.
  
  • Using the API, call the ListShapes operation and pass the image OCID as a parameter.
  
  • Some Marketplace images cannot be resized because of licensing constraints. If you want to resize a Microsoft SQL Server image, contact support.
  
  • You must have sufficient service limits for the new shape. If you don't have service limits, the instance will remain with the original shape.
  
  • Different shapes are billed at different rates. When you change the shape of an instance, you are billed to the nearest second of usage for each shape that you use. For more information, see Compute Pricing and Resource Billing for Stopped Instances on page 780.
  
  • If the instance has secondary VNICs configured, you might need to reconfigure them after the instance is rebooted. For more information, see Virtual Network Interface Cards (VNICs) on page 2855.
  
  • If the instance is running when you change the shape, it is rebooted as part of the change shape operation. If the applications that run on the instance take a long time to shut down, they could be improperly stopped, resulting in data corruption. To avoid this, shut down the instance using the commands available in the OS before you change the shape.
  
  • When you change the shape from one hardware series to a different series, some hardware details such as the network interface name might change. This might cause problems for some guest OSs, particularly if the OS has been customized. If the OS fails to boot after you change the shape, then you should change the instance back to the original shape.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to change the shape of an instance. If the specified group doesn’t need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Prerequisites

• If you want to change the instance to a smaller shape that supports fewer VNICs, detach the extra VNICs.

Using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click Edit.
4. Click **Edit Shape**. Then, select the shape that you want to scale to. The following options are available:

- **AMD Rome**: The flexible shapes, which uses the current generation AMD processor and has a customizable number of OCPUs and amount of memory.
  
  - For **Number of OCPUs**, choose the number of OCPUs that you want to allocate to this instance by dragging the slider. You can select from 1 to 64 OCPUs.
  
  - For **Amount of memory (GB)**, choose the amount of memory that you want to allocate to this instance by dragging the slider. The amount of memory allowed is based on the number of OCPUs selected. For each OCPU, you can select up to 64 GB of memory, with a maximum of 1024 GB total. The minimum amount of memory allowed is either 1 GB or a value matching the number of OCPUs, whichever is greater. For example, if you select 25 OCPUs, the minimum amount of memory allowed is 25 GB.

  The other resources scale proportionately.

- **Intel Skylake**: Standard shapes that use the current generation Intel processor and have a fixed number of OCPUs.

- **Specialty and Legacy**: Standard shapes with previous generation Intel and AMD processors.

5. Click **Change Shape**. If the instance is running, it is rebooted.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to change the shape of an instance:

- **UpdateInstance**

**Editing the Fault Domain for an Instance**

You can change the fault domain where a virtual machine (VM) instance is placed.

A fault domain is a grouping of hardware and infrastructure that is distinct from other fault domains in the same availability domain. By properly leveraging fault domains you can increase the availability of applications running on Oracle Cloud Infrastructure. For more information and best practices, see Fault Domains on page 595.

**Supported Shapes**

You can change the fault domain for instances that use these shapes:

- VM.Standard.E3 series
- VM.Standard.E2 series
- VM.Standard2 series
- VM.Standard.B1 series
- VM.Standard1 series
- VM.DenseIO1 series
- VM.DenseIO2 series
- VM.GPU3 series

These shapes cannot be edited:

- VM.Standard.E2.1.Micro series
- VM.GPU2 series
- VM instances that run on dedicated virtual machine hosts
- Bare metal shapes

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message
that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and
which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to change
the fault domain for an instance. If the specified group doesn’t need to launch instances or attach volumes, you could
simplify that policy to include only manage instance-family, and remove the statements involving volume-
family and virtual-network-family.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For
reference material about writing policies for instances, cloud networks, or other Core Services API resources, see
Details for the Core Services on page 2181.

**Using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click Edit.
4. Click Edit Fault Domain. Then, select a new fault domain.
5. Click Save Changes.

   If the instance is running, it is rebooted.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on
page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to change the fault domain for an instance:

- UpdateInstance

**Editing the Launch Options for an Instance**

You can tune the compatibility and performance of virtual machine (VM) instances by changing the networking type
or the boot volume attachment type.

**Networking Launch Types**

The networking interface handles functions such as disk input/output and network communication. The following
networking types are available:

- **Paravirtualized networking**: For general purpose workloads such as enterprise applications, microservices,
  and small databases. Paravirtualized networking also provides increased flexibility to use the same image across
different hardware platforms. Linux images with paravirtualized networking support live migration during
infrastructure maintenance.

- **Hardware-assisted (SR-IOV) networking**: Single root input/output virtualization. For low-latency workloads
  such as video streaming, real-time applications, and large or clustered databases. Hardware-assisted (SR-IOV)
  networking uses the VFIO driver framework.

  **Note:**

  On Windows Server 2012 R2 images, SR-IOV networking is only supported
  on the VM.Standard2 and VM.DenseIO2 shapes.

The following table lists the default and supported networking types for VM shapes.

<table>
<thead>
<tr>
<th>Shape series</th>
<th>Default Networking Type</th>
<th>Supported Networking Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard1</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.Standard2</td>
<td>Paravirtualized</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>Shape series</td>
<td>Default Networking Type</td>
<td>Supported Networking Types</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>VM.Standard.E2</td>
<td>Paravirtualized</td>
<td>Paravirtualized only</td>
</tr>
<tr>
<td>VM.Standard.E3</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
</tbody>
</table>

**Note:** Due to driver support, the Windows Server 2012 platform image supports paravirtualized networking only.

<table>
<thead>
<tr>
<th>Shape series</th>
<th>Default Networking Type</th>
<th>Supported Networking Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.DenseIO1</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.DenseIO2</td>
<td>Paravirtualized</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.GPU2</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
<tr>
<td>VM.GPU3</td>
<td>SR-IOV</td>
<td>Paravirtualized, SR-IOV</td>
</tr>
</tbody>
</table>

To use paravirtualized networking, you must also use an image that supports paravirtualized networking. Paravirtualized networking is supported on these Oracle-provided images:

- **Oracle Linux 8:** All images.
- **Oracle Linux 7, Oracle Linux 6:** Images published in March 2019 or later.
- **CentOS 8:** All images.
- **CentOS 7:** Images published in July 2019 or later.
- **Ubuntu 18.04, Ubuntu 16.04:** Images published in March 2019 or later.
- **Windows Server 2019:** All images.
- **Windows Server 2016:** Images published in August 2019 or later.

SR-IOV networking is supported on all Oracle-provided images, except for Windows Server 2019 when launched using a VM.Standard2 shape. On Windows Server 2012 R2, SR-IOV networking is only supported on the VM.Standard2 and VM.DenseIO2 shapes.

### Boot Volume Attachment Types

The following boot volume attachment types are available:

- **iSCSI:** A TCP/IP-based standard used for communication between a volume and attached instance.
- **Paravirtualized:** A virtualized attachment available for VMs. This is the default for boot volumes and remote block storage volumes on Oracle-provided platform images.

### Supported Shapes

You can edit the launch options for instances that use these shapes:

- VM.Standard.E3 series
- VM.Standard.E2 series
- VM.Standard2 series
- VM.Standard.B1 series
- VM.Standard1 series
- VM.DenseIO1 series
- VM.DenseIO2 series
- VM.GPU3 series

These shapes cannot be edited:

- VM.Standard.E2.1.Micro series
- VM.GPU2 series
- VM instances that run on dedicated virtual machine hosts
Limitations and Considerations

**Caution:**

Some instances might not function properly if you change the networking type or the boot volume attachment type. This happens due to shape and image compatibility and driver support. After the instance reboots and is running, connect to it. If the connection fails or the OS doesn't behave as expected, the changes are not supported. Revert the instance to the original settings.

Before you change the networking type or the boot volume attachment type, you must ensure that paravirtualized drivers are installed on the image. The steps depend on the image:

**Oracle Linux 7.x, CentOS 8.x, CentOS 7.x, Ubuntu 20, Ubuntu 18, Ubuntu 16**

Paravirtualized drivers are installed on Oracle-provided platform images.


The Oracle VirtIO Drivers for Microsoft Windows release 1.1.5 must be installed on Oracle-provided platform images.

1. To determine whether the VirtIO drivers are installed, connect to the instance using a Remote Desktop connection. Then, do either of the following things:

   - Open `Control Panel > Program and Features`. If `Oracle Windows VirtIO Drivers` is installed, note the version number.
   - In Registry Editor, go to `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Oracle Corporation\Oracle Windows VirtIO Drivers`. If the VirtIO drivers are installed, note the version number.

2. If the drivers are not installed or a version that is not 1.1.5 is installed, download Oracle VirtIO Drivers release 1.1.5:

   - Sign in to the [Oracle Software Delivery Cloud site](https://www.oracle.com/software-delivery-cloud/).
   - In the [All Categories](https://www.oracle.com/software-delivery-cloud/software.html) list, select [Release](https://www.oracle.com/software-delivery-cloud/released.html).
   - Type `Oracle Linux 7.7` in the search box and click [Search](https://www.oracle.com/software-delivery-cloud/search.html).
   - Add [REL: Oracle Linux 7.7.x](https://www.oracle.com/software-delivery-cloud/category/oracle-linux-x86-64.html) to your cart, and then click [Continue](https://www.oracle.com/software-delivery-cloud/continue.html).
   - In the [Platforms/Languages](https://www.oracle.com/software-delivery-cloud/platforms-languages.html) list, select [x86 64 bit](https://www.oracle.com/software-delivery-cloud/platforms-languages.html). Click [Continue](https://www.oracle.com/software-delivery-cloud/continue.html).
   - Accept the license agreement and then click [Continue](https://www.oracle.com/software-delivery-cloud/continue.html).
   - Select the check box next to [Oracle VirtIO Drivers Version for Microsoft Windows 1.1.5](https://www.oracle.com/software-delivery-cloud/checkout.html). Clear the other check boxes.
   - Click [Download](https://www.oracle.com/software-delivery-cloud/download.html) and then follow the prompts.

3. Install the drivers and then restart the instance. For steps, see [Installing the Oracle VirtIO Drivers for Microsoft Windows on Existing Microsoft Windows Guests](https:// docs.oracle.com/en/database/oracle-cloud-infrastructure/user-guide/compute.html#GUID-16E6C470-13BB-452B-A77F-D9203B9435C1).

**Oracle Linux 6.x**

For Oracle-provided platform images, connect to the instance using a Secure Shell (SSH) connection. Then, run the following commands:

```
sudo bash
cd /boot/efi
echo "fs0:\EFI\redhat\grub.efi"> startup.nsh
chmod 500 startup.nsh
sync
```

**Images that are not Oracle-provided platform images**
To verify that your system has paravirtualized drivers installed, run the following command:

```
lsinitrd | grep virtio
```

- If paravirtualized drivers are installed, you will see multiple files listed with paths similar to `lib/modules/4.4.21-69-default/kernel/drivers/block/virtio_blk.ko`.
- If no files are listed, your system either does not support paravirtualized drivers, or does not have paravirtualized drivers installed. Refer to the documentation for your operating system for more information.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a `policy` by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which `compartment` you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to edit the launch options for an instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage `instance-family`, and remove the statements involving `volume-family` and `virtual-network-family`.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Prerequisites**

- Detach (delete) all secondary VNICs and detach all block volumes. The primary VNIC and boot volume should remain attached.

**Using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click Edit.
4. Click Show Advanced Options.
5. To change the networking type, in the Networking type section, select from the following options:
   - **Hardware-assisted (SR-IOV) networking**: Single root input/output virtualization. For low-latency workloads such as video streaming, real-time applications, and large or clustered databases.
   - **Paravirtualized networking**: For general purpose workloads such as enterprise applications, microservices, and small databases. The image must have paravirtualized drivers, as described in Limitations and Considerations on page 771.

   For more information, see Recommended Networking Launch Types on page 696.

6. To change the boot volume attachment type, in the Boot volume attachment type section, select from the following options:
   - **iSCSI**: A TCP/IP-based standard used for communication between a volume and attached instance.
   - **Paravirtualized**: A virtualized attachment available for VMs. This is the default for boot volumes and remote block storage volumes on Oracle-provided platform images.

7. Click Save Changes.

   If the instance is running, it is rebooted.

8. Connect to the instance after it reboots and is running. If the connection fails or the OS doesn't behave as expected, the changes are not supported. Revert the instance to the original settings.

9. If necessary, reattach any secondary VNICs and block volumes.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use this API operation to edit the launch options for an instance:

- **UpdateInstance**

## Enabling In-Transit Encryption Between an Instance and Boot Volumes or Block Volumes

After you create a virtual machine (VM) instance, you can enable or disable in-transit encryption between the instance and its paravirtualized boot volume and block volume attachments.

All boot volume and block volume data at rest is always encrypted by the Oracle Cloud Infrastructure Block Volume service using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. For more information, see [Block Volume Encryption](#) on page 504.

**Important:** See this [known issue](#) for more information about editing the in-transit encryption settings.

### Supported Shapes and Images

You can enable or disable in-transit encryption for existing instances that use these shapes:

- VM.Standard.E3 series
- VM.Standard.E2 series
- VM.Standard2 series
- VM.Standard.B1 series
- VM.Standard1 series
- VM.DenseIO1 series
- VM.DenseIO2 series
- VM.GPU3 series

In-transit encryption for boot volumes and block volumes is available for [Oracle-provided images](#). It is not supported in most cases for instances launched from custom images imported for "bring your own image" (BYOI) scenarios. To confirm support for certain Linux-based custom images, contact support.

These shapes cannot be edited:

- VM.Standard.E2.1.Micro series
- VM.GPU2 series
- VM instances that run on dedicated virtual machine hosts
- Bare metal shapes

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a [policy](#) by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which [compartment](#) you should work in.

For administrators: The policy in [Let users launch compute instances](#) on page 2143 includes the ability to change the shape of an instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only `manage instance-family`, and remove the statements involving `volume-family` and `virtual-network-family`.

If you're new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see [Details for the Core Services](#) on page 2181.

### Using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click Edit.
4. Click Show Advanced Options.
5. Select the Use in-transit encryption check box.
6. Click Save Changes.

   If the instance is running, it is rebooted.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to enable or disable in-transit encryption between an instance and its paravirtualized boot volume attachments:

- UpdateInstance

**Setting Instance Availability During Maintenance Events**

When the underlying infrastructure for a virtual machine (VM) instance needs to undergo planned maintenance or recover from an unexpected failure, Oracle Cloud Infrastructure automatically attempts to recover the instance by migrating it to healthy hardware. By default, the instance is recovered to the same lifecycle state as before the maintenance event. If you have an alternate process to recover the instance after a reboot migration, you can optionally configure the instance to remain stopped after it is migrated to healthy hardware. You can then restart the instance on your own schedule.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to edit the maintenance recovery action for an instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click Edit.
4. Click Show Advanced Options.
5. For the Restore instance lifecycle state after infrastructure maintenance check box, select an option:
   - To reboot a running instance after it is recovered, select the check box.
   - To recover the instance in the stopped state, clear the check box.
6. Click Save Changes.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to edit the maintenance recovery action for an instance:

- UpdateInstance
Moving a Compute Instance to a New Host

This topic covers how to relocate a virtual machine or a bare metal instance by using reboot migration or a manual process.

**Note:**

- **Dedicated virtual machine hosts:** Dedicated virtual machine hosts do not support reboot migration. To relocate these instances, use the process described in Moving an Instance with Manual Migration on page 775.
- **Oracle Platform Services:**
  For instances that were created with Oracle Platform Services and located in the compartment ManagedCompartmentForPaaS, you must use the interface for the specific Platform Service to reboot the instances.

**Live Migration**

During an infrastructure maintenance event, where applicable, Oracle Cloud Infrastructure live migrates Standard VM instances from the physical VM host that needs maintenance to a healthy VM host without disrupting running instances. If a VM cannot be live migrated, there might be a short downtime while the instance is reboot migrated. You can avoid this downtime by proactively reboot migrating the instance.

**Reboot Migration**

For instances with a date in the **Reboot Maintenance** field (available in the Console, CLI, and SDKs), you can reboot your instance to move it to new infrastructure. After you reboot the instance, the **Reboot Maintenance** field is cleared. This change indicates that the instance was moved successfully.

**Prerequisites for Reboot Migration**

1. Prepare the instance for reboot migration:
   - Ensure that any remote block volumes defined in /etc/fstab use the recommended options.
   - Ensure that any File Storage service (NFS) mounts use the nofail option.
   - If you use the Oracle-provided script to configure secondary VNICs, ensure it runs automatically at startup.

**Moving an Instance with Reboot Migration**

After you complete the prerequisites:

1. Stop any running applications.
2. Reboot the instance.
3. Confirm that the **Reboot Maintenance** field no longer has a date.

**Limitations and Warnings for Manual Migration**

Be aware of the following limitations and warnings when performing a manual migration:

- Any public IP addresses assigned to your instance from a reserved public pool are retained. Any that were not assigned from a reserved public IP address pool will change. Private IP addresses do not change.
• MAC addresses, CPUIDs, and other unique hardware identifiers do change during the move. If any applications running on the instance use these identifiers for licensing or other purposes, be sure to take note of this information before moving the instance to help you manage the change.

Prerequisites for Manual Migration

1. Before moving the instance, document all critical details:
   • The instance's region, availability domain, and fault domain.
   • The instance's display name.
   • All private IP addresses, names, and subnets. Note that the instance can have multiple VNICs, and each VNIC can have multiple secondary IP addresses.
   • All private DNS names. The instance can have multiple VNICs, and each VNIC can have multiple secondary IP addresses. Each private IP address can have a DNS name.
   • Any public IP addresses assigned from a reserved public pool. Note that the instance can have multiple VNICs, and each VNIC can have multiple secondary private IP addresses. Each VNIC and secondary private IP address can have an attached public IP address.
   • Any remote block volumes attached to the instance.
   • Any tags on the instance or attached resources.

2. Prepare the instance for manual migration:
   • Ensure that any remote block volumes defined in /etc/fstab use the recommended options.
   • Ensure that any File Storage service (NFS) mounts use the nofail option.
   • If you have statically defined any network interfaces belonging to secondary VNICs using their MAC addresses, such as those defined in /etc/sysconfig/network-scripts/ifcfg*, those interfaces will not start due to the change in the MAC address. Remove the static mapping.
   • If you use the Oracle-provided script to configure secondary VNICs, ensure it runs automatically at startup.

Moving an Instance Manually

After you complete the prerequisites:

1. Stop any running applications.
2. Ensure that those applications will not start automatically.

Caution:

When the relocated instance starts for the first time, remote block volumes, secondary VNICs, or any resource that relies on them, will not be attached. The absence of these resources can cause application issues.

3. If your instance has local NVMe storage (dense instances), you must back up this data:
   a. Create and attach one or more remote block volumes to the instance.
   b. Copy the data from the NVMe devices to the remote block volumes.
4. Unmount any remote block volumes or File Storage service (NFS) mounts.
5. Back up all remote block volumes. See Overview of Block Volume Backups on page 540 for more information.
6. Create a backup of the root volume.

Important:

Do not generalize or specialize Windows instances.
7. Terminate the instance:
   
   **Using the Console**
   
   To terminate the instance, follow the steps in Terminating an Instance on page 783, ensuring that the **Permanently delete the attached boot volume** check box is cleared. This preserves the boot volume that is associated with the instance.
   
   **Using the API**
   
   To terminate the instance, use the TerminateInstance operation and pass the preserveBootVolume parameter set to true in the request.
   
   **Using the CLI**
   
   To terminate the instance, use the terminate operation and set the preserve-boot-volume option to true.

8. Create a new instance using the boot volume from the terminated instance.

9. In the launch instance flow, specify the private IP address that was attached to the primary VNIC. If the public IP address was assigned from a reserved IP address pool, be sure to assign the same IP address.

10. When the instance state changes to **RUNNING**, stop the instance.

11. Recreate any secondary VNICs and secondary IP addresses.

12. Attach any remote block volumes.

   **Note:**
   
   This step includes any volumes used to back up local NVMe devices. Copy the data onto the NVMe storage on the new instance, and then detach the volumes.

13. Start the instance.


15. Configure the applications to start automatically, as required.

16. Recreate the required tags.

17. (Optional) After you confirm that the instance and applications are healthy, you can delete the volume backups.

### Moving Compute Resources to a Different Compartment

You can move Compute resources such as instances, instance pools, and custom images from one compartment to another.

When you move a Compute resource to a new compartment, associated resources such as boot volumes and VNICs are not moved.

After you move the resource to the new compartment, inherent policies apply immediately and affect access to the resource through the Console. For more information, see Managing Compartments on page 2431.

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators: The following policies allow users to move Compute resources to a different compartment:

- Allow group ComputeCompartmentMovers to manage instance-family in tenancy
- Allow group ComputeCompartmentMovers to manage compute-management-family in tenancy
- Allow group ComputeCompartmentMovers to manage auto-scaling-configurations in tenancy
If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Security Zones

Security Zones ensure that your cloud resources comply with Oracle security principles. If any operation on a resource in a security zone compartment violates a policy for that security zone, then the operation is denied.

The following security zone policies affect your ability to move Compute resources from one compartment to another:

• You can't move a compute instance from a security zone to a standard compartment.
• You can't move a compute instance from a standard compartment to a compartment that is in a security zone.

Using the Console

To move an instance to a different compartment

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. In the List Scope section, select a compartment.
3. Click the instance that you're interested in.
4. Click More Actions, and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To track the progress of the operation, you can monitor the associated work request. For more information, see Using the Console to View Work Requests on page 260.

7. If there are alarms monitoring the instance, update the alarms to reference the new compartment. See To update an alarm after moving a resource on page 2737 for more information.
8. Optionally, move the resources that are attached to the instance to the new compartment.

To move an instance configuration to a different compartment

Note:

Most of the properties for an existing instance configuration, including the compartment, cannot be modified after you create the instance configuration. Although you can move an instance configuration to a different compartment, you will not be able to use the instance configuration to manage instance pools in the new compartment. If you want to update an instance configuration to point to a different compartment, you should instead create a new instance configuration in the target compartment. For steps, see Creating an Instance Configuration on page 710.

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Configurations.
2. In the List Scope section, select a compartment.
3. Click the instance configuration that you're interested in.
4. Click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To move an instance pool to a different compartment

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. In the List Scope section, select a compartment.
3. Click the instance pool that you're interested in.
4. Click More Actions, and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.
7. Optionally, update the instance pool with an instance configuration that points to the new compartment. Do the following:
   a. Create a new instance configuration in the new compartment. You can do this using the Console or the API. For steps, see Creating an Instance Configuration on page 710.
   b. Update the instance pool with the new instance configuration. You can do this using the API. For steps, see Updating an Instance Pool on page 713.
8. Optionally, move the instances and other resources that are associated with the instance pool to the new compartment.

To move an autoscaling configuration to a different compartment
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Autoscaling Configurations.
2. In the List Scope section, select a compartment.
3. Click the autoscaling configuration that you're interested in.
4. Click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To move a custom image to a different compartment
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images.
2. In the List Scope section, select a compartment.
3. Click the custom image that you're interested in.
4. Click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To move a cluster network to a different compartment
1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Cluster Networks.
2. In the List Scope section, select a compartment.
3. Click the cluster network that you're interested in.
4. Click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.
7. Optionally, move the instances and other resources that are associated with the cluster network to the new compartment.

Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to move Compute resources to different compartments:
- ChangeInstanceCompartment
- ChangeInstanceConfigurationCompartment
- ChangeInstancePoolCompartment
- ChangeAutoScalingConfigurationCompartment
- ChangeImageCompartment
- ChangeClusterNetworkCompartment

Stopping and Starting an Instance
You can stop and start an instance as needed to update software or resolve error conditions.

For steps to manage the lifecycle state of instances in an instance pool, see Stopping and Starting the Instances in an Instance Pool on page 716.
Stopping or Restarting an Instance Using the Instance's OS

In addition to using the API and Console, you can stop and restart instances using the commands available in the operating system when you are logged in to the instance. Stopping an instance using the instance's OS does not stop billing for that instance. If you stop an instance this way, be sure to also stop it from the Console or API.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to stop or start an existing instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

Resource Billing for Stopped Instances

For both VM and bare metal instances, billing depends on the shape that you use to create the instance:

- **Standard shapes**: Stopping an instance pauses billing. However, stopped instances continue to count toward your service limits.
- **Dense I/O shapes**: Billing continues for stopped instances because the NVMe storage resources are preserved. Related resources continue to count toward your service limits. To halt billing and remove related resources from your service limits, you must terminate the instance.
- **GPU shapes**: Billing continues for stopped instances because GPU resources are preserved. Related resources continue to count toward your service limits. To halt billing and remove related resources from your service limits, you must terminate the instance.
- **HPC shapes**: Billing continues for stopped instances because the NVMe storage resources are preserved. Related resources continue to count toward your service limits. To halt billing and remove related resources from your service limits, you must terminate the instance.

Stopping an instance using the instance's OS does not stop billing for that instance. If you stop an instance this way, be sure to also stop it from the Console or API.

For more information about Compute pricing, see Compute Pricing. For more information about how instances running Microsoft Windows Server are billed when they are stopped, see How am I charged for Windows Server on Oracle Cloud Infrastructure? on page 805.

Recovering a Virtual Machine (VM) During Planned Maintenance

Oracle Cloud Infrastructure performs routine data center maintenance on the physical infrastructure for VM instances. This maintenance includes tasks such as upgrading and replacing hardware or performing maintenance that halts power to the host. When an underlying infrastructure component needs to undergo maintenance, you are notified in advance before the impact to your instances.

During an infrastructure maintenance event, where applicable, Oracle Cloud Infrastructure live migrates Standard VM instances to a healthy physical VM host without disrupting running instances. If a VM instance cannot be live migrated, then the instance is stopped on the physical VM host that needs maintenance, reboot migrated to a healthy VM host, and then restarted. If you have an alternate process to recover the instances, you can optionally configure the instances to remain stopped after they are reboot migrated to healthy hardware.

If VM instances are scheduled for a maintenance reboot, you can proactively reboot (or stop and start) the instances at any time before the scheduled reboot. Proactively rebooting lets you control how and when your applications
experience downtime. Customer-managed VM maintenance is supported on Standard and GPU instance shapes, including Oracle-provided platform images and custom images that were imported from outside of Oracle Cloud Infrastructure.

To identify the VM instances that you can proactively reboot, do any of the following things:

**Using the Console: To see which instances in the current compartment are scheduled for a maintenance reboot**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.

   If the instance has a maintenance reboot scheduled and can be proactively rebooted, a warning icon appears next to the instance name.

2. Click the instance that you're interested in, and then check the **Maintenance Reboot** field for the instance. This field displays the date and start time for the maintenance reboot.

**Using the API: To see which instances in a compartment are scheduled for a maintenance reboot**

Use the ListInstances operation. The `timeMaintenanceRebootDue` field for the Instance returns the date and start time for the maintenance reboot.

**Using Search: To find all instances that are scheduled for a maintenance reboot**

1. In the top navigation bar, click **Search for resources, services, and documentation**, and then click **Advanced Resource Query**.

2. Click **Select Sample Query**, and then click **Query for all instances which have an upcoming scheduled maintenance reboot**.

3. Click **Search**.

If you choose not to reboot before the scheduled time, then Oracle Cloud Infrastructure will migrate your instances within a 24-hour period after the scheduled time.

An instance is no longer impacted by a maintenance event when the **Maintenance Reboot** field for the instance is blank.

**VM Recovery Due to Infrastructure Failure**

When the underlying infrastructure of a VM instance fails due to software or hardware issues, Oracle Cloud Infrastructure automatically attempts to recover the instance.

Standard and GPU VM instances are recovered to another physical VM host using **reboot migration**. During the reboot, instance properties such as private and ephemeral public IP addresses, attached block volumes, and VNICs are preserved.

Dense I/O VM instances are recovered by rebooting the instance on the same physical host. If recovering a Dense I/O instance on the same physical host isn't possible, Oracle Cloud Infrastructure notifies you to terminate the instance within 14 days. If you don't terminate the instance before the deadline, Oracle Cloud Infrastructure will terminate it. The boot volume and remote attached data volume are preserved.

Oracle Cloud Infrastructure notifies you by email or **announcements** of any VM infrastructure failure events, with the status of the recovery action that was taken. You can also monitor the **instance status metric** to stay aware of any unexpected reboots.

Optionally, you can **configure your instances to remain stopped** after they are recovered.

**Hardware Reclamation for Stopped Bare Metal Instances**

When a bare metal instance remains in the stopped state for longer than 48 hours, the instance is taken offline and the physical hardware is reclaimed. The next time that you restart the instance, it starts on different physical hardware. There are no changes to the block volumes, boot volumes, and instance metadata, including the ephemeral and public IP addresses.

However, the following properties do change when a bare metal instance restarts on different physical hardware: the MAC addresses and the host serial number. You might also notice changes in the BIOS firmware version, BIOS settings, and CPU microcode. If you want to keep the same physical hardware, do not stop the instance using the
Console or the API, SDKs, or CLI. Instead, shut down the instance using the instance's OS. When you want to restart the instance, use the Console or the API, SDKs, or CLI.

This behavior applies to Linux instances that use the following shapes:

- BM.Standard1.36
- BM.Standard.B1.44
- BM.Standard2.52
- BM.Standard.E2.64

### Using the Console

#### To start an instance

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click **Start**.

#### To stop an instance

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click **Stop**.
4. By default, the Console gracefully stops the instance by sending a shutdown command to the operating system. After waiting 15 minutes for the OS to shut down, the instance is powered off.

   **Note:**
   
   If the applications that run on the instance take more than 15 minutes to shut down, they could be improperly stopped, resulting in data corruption. To avoid this, shut down the instance using the commands available in the OS before you stop the instance using the Console.

   If you want to stop the instance immediately, without waiting for the OS to respond, select the **Force stop the instance by immediately powering off** check box.
5. Click **Stop Instance**.

#### To reboot an instance

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Click **Reboot**.
4. By default, the Console gracefully restarts the instance by sending a shutdown command to the operating system. After waiting 15 minutes for the OS to shut down, the instance is powered off and then powered back on.

   **Note:**
   
   If the applications that run on the instance take more than 15 minutes to shut down, they could be improperly stopped, resulting in data corruption. To avoid this, shut down the instance using the commands available in the OS before you restart the instance using the Console.

   If you want to reboot the instance immediately, without waiting for the OS to respond, select the **Force reboot the instance by immediately powering off, then powering back on** check box.
5. Click **Reboot Instance**.
**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the InstanceAction operation to stop, start, or reboot an instance.

**Terminating an Instance**

You can permanently terminate (delete) instances that you no longer need. Any attached VNICs and volumes are automatically detached when the instance terminates. Eventually, the instance's public and private IP addresses are released and become available for other instances.

By default, the instance's boot volume is preserved when you terminate the instance. You can attach the boot volume to a different instance as a data volume, or use it to launch a new instance. If you no longer need the boot volume, you can permanently delete it at the same time that you terminate the instance.

**Caution:**

If your instance has NVMe storage, terminating the instance securely erases the NVMe drives. Any data that was on the NVMe drives becomes unrecoverable. Ensure that you back up any important data before you terminate an instance. For more information, see Protecting Data on NVMe Devices.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to terminate an instance (with or without an attached block volume).

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click More Actions, and then click Terminate.
4. If you want to delete the boot volume that is associated with the instance, select the Permanently delete the attached boot volume check box.
5. Click Terminate Instance.

Terminated instances temporarily remain in the list of instances with the state Terminated.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the TerminateInstance operation to terminate an instance.

**Enabling Monitoring for Compute Instances**

This topic describes how to enable monitoring, specifically for the compute instance metrics, on compute instances.
The compute instance metrics provide data about the activity level and throughput of the instance. These metrics are required to use features such as autoscaling, metrics, alarms, and notifications with compute instances. A compute instance emits these metrics only when the Compute Instance Monitoring plugin is enabled and running on the instance.

The Compute Instance Monitoring plugin is managed by the Oracle Cloud Agent software.

**Supported Images**

Compute instance metrics are supported on current Oracle-provided images and on custom images that are based on current Oracle-provided images.

If you use an older Oracle-provided image, you must manually install the Oracle Cloud Agent software before you can use the Compute Instance Monitoring plugin. Select an image dated after November 15, 2018 (except Ubuntu, which must be dated after February 28, 2019).

You might have success enabling compute instance metrics on other images that support the Oracle Cloud Agent software, though the Compute Instance Monitoring plugin has not been tested on other operating systems and there is no guarantee that it will work. Compute instance metrics are not supported on Windows Server 2008 R2 custom images.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For more information about the IAM policies that are needed to create and update a compute instance, see Creating an Instance on page 695.

**Prerequisites**

- Service gateways or public IP addresses: The compute instance must have either a public IP address or a service gateway to be able to send compute instance metrics to the Monitoring service.

  If the instance does not have a public IP address, set up a service gateway on the virtual cloud network (VCN). The service gateway lets the instance send compute instance metrics to the Monitoring service without the traffic going over the internet. Here are special notes for setting up the service gateway to access the Monitoring service:

  - When creating the service gateway, enable the service label called All <region> Services in Oracle Services Network. It includes the Monitoring service.
  
  - When setting up routing for the subnet that contains the instance, set up a route rule with Target Type set to Service Gateway, and the Destination Service set to All <region> Services in Oracle Services Network.

  For detailed instructions, see Access to Oracle Services: Service Gateway on page 3256.

- Oracle Cloud Agent: The Oracle Cloud Agent software must be installed on the instance. Oracle Cloud Agent is installed by default on current Oracle-provided images. For steps to manually install Oracle Cloud Agent on older images, see Installing the Oracle Cloud Agent Software on page 741.

- Compute Instance Monitoring plugin: For the instance to emit the compute instance metrics, the Compute Instance Monitoring plugin must be enabled on the instance and plugins must be running. For more information about how to enable and run plugins, see Managing Plugins with Oracle Cloud Agent on page 740.

**Enabling Monitoring for a New Compute Instance**

To configure a new compute instance to emit the compute instance metrics, use the following steps.

**Creating a Monitoring-Enabled Instance Using the Console**

1. Follow the steps to create an instance, until the advanced options. Ensure that the instance has either a public IP address or a service gateway, as described in the prerequisites.
2. Click **Show Advanced Options**.
3. On the **Oracle Cloud Agent** tab, select the **Compute Instance Monitoring** check box.

   **Note:**
   If you’re using an older Oracle-provided image or a custom image that is not based on a recent Oracle-provided image, you must manually install the Oracle Cloud Agent software. You can do this by providing a cloud-init script. For more information, see Installing the Oracle Cloud Agent Software on page 741. Compare the date of the image to the date listed in Supported Images.

4. Click **Create**.

   The newly created, monitoring-enabled instance emits compute instance metrics to the Monitoring service.

**Creating a Monitoring-Enabled Instance Using the API**

Use the **LaunchInstance** operation. Include the following parameters:

```json
{
   "agentConfig": {
      "isMonitoringDisabled": false,
      "areAllPluginsDisabled": false,
      "pluginsConfig": [
         {
            "name": "Compute Instance Monitoring",
            "desiredState": "ENABLED"
         }
      ]
   }
}
```

Ensure that the instance has either a public IP address or a service gateway, as described in the prerequisites.

**Note:**
If you’re using an older Oracle-provided image or a custom image that is not based on a recent Oracle-provided image, you must manually install the Oracle Cloud Agent software. You can do this by providing a cloud-init script. For more information, see Installing the Oracle Cloud Agent Software on page 741. Compare the date of the image to the date listed in Supported Images.

**Enabling Monitoring for an Existing Compute Instance**

To configure an existing Compute instance to emit the compute instance metrics, use the following steps.

**To enable monitoring on an existing compute instance using the Console**

1. Install the Oracle Cloud Agent software, if it is not already installed.
2. Enable the Compute Instance Monitoring plugin.
3. Confirm that plugins are running on the instance.
4. Ensure that the instance has either a public IP address or a service gateway, as described in the prerequisites.
5. To confirm that monitoring is enabled:
   a. Go to the Metrics page for the instance:
      1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
      2. Click the instance that you're interested in.
      3. Under **Resources**, click **Metrics**.
      4. In the **Metric Namespace** list, select **oci_computeagent**.
   b. If you see metric charts with data, then the Monitoring service is receiving compute instance metrics from this instance. For more information about these metrics, see **Compute Instance Metrics** on page 788.

   If monitoring is not enabled (and the instance uses a supported image), then a button is available to enable monitoring. Click **Enable monitoring**.

**To enable monitoring on an existing compute instance using the API**

1. Install the Oracle Cloud Agent software, if it is not already installed.
2. Use the **UpdateInstance** operation. Include the following parameters:

   ```json
   {  
     "agentConfig": {  
       "isMonitoringDisabled": false,  
       "areAllPluginsDisabled": false,  
       "pluginsConfig": [  
         {  
           "name": "Compute Instance Monitoring",  
           "desiredState": "ENABLED"  
         }  
       ]  
     }  
   }
   ```

3. Ensure that the instance has either a public IP address or a service gateway, as described in the **prerequisites**.

**Managing the Compute Instance Monitoring Plugin**

For an instance to emit the compute instance metrics, the Compute Instance Monitoring plugin must be enabled on the instance and plugins must be running.

If you want to temporarily prevent the instance from emitting compute instance metrics, you can disable the Compute Instance Monitoring plugin. You can also stop all of the plugins that run on the instance, including the Compute Instance Monitoring plugin.

**Caution:**

Functionality that depends on the plugin, such as monitoring and autoscaling, does not work when the plugin is disabled or stopped.

For more information about how to enable and run plugins, see **Managing Plugins with Oracle Cloud Agent** on page 740.

**Finding Out if Monitoring Has Your Metrics**

To determine whether Monitoring is receiving the compute instance metrics, you can either query the instance metrics, or view the instance properties to confirm that the Compute Instance Monitoring plugin is enabled and running.

**Using the Console: To find out whether Monitoring is receiving metrics by querying instance metrics**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Under **Resources**, click **Metrics**.
4. In the Metric Namespace list, select **oci_computeagent**.

If you see metric charts with data, then the Monitoring service is receiving metrics from this instance. For more information about these metrics, see Compute Instance Metrics on page 788.

If you see a message that monitoring is not enabled, or that the Oracle Cloud Agent software needs to be installed, then complete those tasks.

**Using the Console:** To find out whether the Compute Instance Monitoring plugin is enabled and running

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Click the Oracle Cloud Agent tab.
4. Confirm that the Compute Instance Monitoring plugin is enabled, and all plugins are running.

**Using the API:** To find out whether Monitoring is receiving metrics by querying instance metrics

Use the SummarizeMetricsData API operation. If metrics are returned, it indicates that the Monitoring service is receiving metrics from the instance.

**Using the API:** To find out whether the Compute Instance Monitoring plugin is enabled and running

Use the GetInstance operation (or ListInstances operation, for multiple instances).

In the response, if the `agentConfig` object returns the following values, it indicates that the Compute Instance Monitoring plugin is enabled and all plugins are running.

```
{
  "agentConfig": {
    "isMonitoringDisabled": false,
    "areAllPluginsDisabled": false,
    "pluginsConfig": [
      {
        "name": "Compute Instance Monitoring",
        "desiredState": "ENABLED"
      }
    ]
  }
}
```

**Not seeing metrics for your instance?**

If you don't see any metric charts, the instance might not be emitting metrics. See the following possible causes and resolutions.

<table>
<thead>
<tr>
<th>Possible cause</th>
<th>How to check</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Compute Instance Monitoring plugin is disabled on the instance or plugins are stopped.</td>
<td>Review the instance properties.</td>
<td>Enable the Compute Instance Monitoring plugin and start all plugins.</td>
</tr>
<tr>
<td>The instance cannot access the Monitoring service because its VCN does not use the internet.</td>
<td>Review the instance's IP address. If it's not public, then a service gateway is needed.</td>
<td>Set up a service gateway.</td>
</tr>
<tr>
<td>The instance does not use a supported image.</td>
<td>Review the supported images.</td>
<td>Create an instance with a supported image.</td>
</tr>
<tr>
<td>Older images and custom images: No Oracle Cloud Agent software exists on the instance.</td>
<td>Connect to the instance and look for the software.</td>
<td>Install the Oracle Cloud Agent software.</td>
</tr>
</tbody>
</table>
Possible cause | How to check | Resolution
--- | --- | ---
New instance in a new compartment: The IAM policies required for the instance to publish metrics to Monitoring are not yet initialized. | (not applicable) | Check back after 10 or 20 minutes.
More information: IAM policies are automatically created for new instances and are immediately available, unless the instances are in a new compartment. For a new instance in a new compartment, the policies can take up to 20 minutes to initialize, which delays the emission of metrics.

Compute Metrics

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

There are multiple Monitoring service metric namespaces related to Compute resources:

- **oci_computeagent**: Metrics related to the activity level and throughput of compute instances, as emitted by the Compute Instance Monitoring plugin. See Compute Instance Metrics on page 788.
- **oci_instancepools**: Metrics related to the lifecycle state of instances in instance pools. See Instance Pool Metrics on page 793.
- **oci_compute_infrastructure_health**: Metrics related to the up/down status, health, and maintenance status of compute instances. See Infrastructure Health Metrics on page 795.
- **oci_compute**: Metrics related to the instance metadata service (IMDS) that provides information about running compute instances. See Compute Management Metrics on page 798.

Compute Instance Metrics

You can monitor the health, capacity, and performance of your Compute instances by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace **oci_computeagent** (the Compute Instance Monitoring plugin on Compute instances).

You can view these metrics for individual Compute instances, and for all the instances in an instance pool.

Resources: Monitoring-enabled Compute instances.

**Overview of Metrics for an Instance and Related Resources**

This section gives an overall picture of the different types of metrics available for an instance and its storage and network devices. See the following diagram and table for a summary.
<table>
<thead>
<tr>
<th>Metric Namespace</th>
<th>Resource ID</th>
<th>Where Measured</th>
<th>Available Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>oci_computeagent</td>
<td>Instance OCID</td>
<td>On the instance. The metrics in this namespace are aggregated across all the related resources on the instance. For example, DiskBytesRead is aggregated across all the instance's attached storage volumes, and NetworkBytesIn is aggregated across all the instance's attached VNICs.</td>
<td>See Available Metrics: oci_computeagent on page 790.</td>
</tr>
<tr>
<td>oci_blockstore</td>
<td>Boot or block volume OCID</td>
<td>By the Block Volume service. The metrics are for an individual volume (either boot volume or block volume).</td>
<td>See Block Volume Metrics on page 585.</td>
</tr>
<tr>
<td>oci_vcn</td>
<td>VNIC OCID</td>
<td>By the Networking service. The metrics are for an individual VNIC.</td>
<td>See VNIC Metrics on page 3321.</td>
</tr>
</tbody>
</table>

**Prerequisites**

- IAM policies: To monitor resources, you must be given the required type of access in a *policy* written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which *compartment* you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.
- Metrics exist in Monitoring: The resources that you want to monitor must emit metrics to the Monitoring service.
- Compute instances: To emit metrics, the Compute Instance Monitoring plugin must be enabled on the instance, and plugins must be running. The instance must also have either a service gateway or a public IP address to send...
metrics to the Monitoring service. For more information, see Enabling Monitoring for Compute Instances on page 783.

Available Metrics: oci_computeagent

The compute instance metrics help you measure activity level and throughput of compute instances. The metrics listed in the following table are available for any monitoring-enabled compute instance. You must enable monitoring on the instance to get these metrics.

The metrics in this namespace are aggregated across all the related resources on the instance. For example, DiskBytesRead is aggregated across all the instance's attached storage volumes, and NetworkBytesIn is aggregated across all the instance's attached VNICs.

You also can use the Monitoring service to create custom queries.

Each metric includes the following dimensions

<table>
<thead>
<tr>
<th>availabilityDomain</th>
<th>The availability domain where the instance resides.</th>
</tr>
</thead>
<tbody>
<tr>
<td>faultDomain</td>
<td>The fault domain where the instance resides.</td>
</tr>
<tr>
<td>imageId</td>
<td>The OCID of the image for the instance.</td>
</tr>
<tr>
<td>instancePoolId</td>
<td>The instance pool that the instance belongs to.</td>
</tr>
<tr>
<td>region</td>
<td>The region where the instance resides.</td>
</tr>
<tr>
<td>resourceDisplayName</td>
<td>The friendly name of the instance.</td>
</tr>
<tr>
<td>resourceId</td>
<td>The OCID of the instance.</td>
</tr>
<tr>
<td>shape</td>
<td>The shape of the instance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CpuUtilization</td>
<td>CPU Utilization</td>
<td>percent</td>
<td>Activity level from CPU. Expressed as a percentage of total time.</td>
<td>availabilityDomain</td>
</tr>
<tr>
<td>DiskBytesRead[1,3]</td>
<td>Disk Read Bytes</td>
<td>bytes</td>
<td>Read throughput. Expressed as bytes read per interval.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>DiskBytesWritten</td>
<td>Disk Write Bytes</td>
<td>bytes</td>
<td>Write throughput. Expressed as bytes written per interval.</td>
<td></td>
</tr>
<tr>
<td>DiskIopsRead(^1,(^3)</td>
<td>Disk Read I/O</td>
<td>operations</td>
<td>Activity level from I/O reads. Expressed as reads per interval.</td>
<td></td>
</tr>
<tr>
<td>DiskIopsWritten(^1)</td>
<td>Disk Write I/O</td>
<td>operations</td>
<td>Activity level from I/O writes. Expressed as writes per interval.</td>
<td></td>
</tr>
<tr>
<td>LoadAverage</td>
<td>Load Average</td>
<td>number of processes</td>
<td>Average system load calculated over a 1 minute period.</td>
<td></td>
</tr>
<tr>
<td>MemoryAllocationStalls</td>
<td>Memory Allocation Stalls</td>
<td>number of stalls</td>
<td>Number of times page reclaim was called directly.</td>
<td></td>
</tr>
<tr>
<td>MemoryUtilization</td>
<td>Memory Utilization</td>
<td>percent</td>
<td>Space currently in use. Measured by pages. Expressed as a percentage of used pages. For instance pools, the value is averaged across all instances in the pool.</td>
<td></td>
</tr>
<tr>
<td>NetworksBytesIn(^2)</td>
<td>Network Receive Bytes</td>
<td>bytes</td>
<td>Network receipt throughput. Expressed as bytes received.</td>
<td></td>
</tr>
<tr>
<td>NetworksBytesOut(^2)</td>
<td>Network Transmit Bytes</td>
<td>bytes</td>
<td>Network transmission throughput. Expressed as bytes transmitted.</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\)This metric is a cumulative counter that shows monotonically increasing behavior for each session of the Oracle Cloud Agent software, resetting when the operating system is restarted.

\(^2\)The Networking service provides additional metrics (in the `oci_vcn` metric namespace) for each VNIC on the instance. For more information, see Networking Metrics on page 3320.

\(^3\)The Block Volume service provides additional metrics (in the `oci_blockstore` metric namespace) for each volume attached to the instance. For more information, see Block Volume Metrics on page 585.

**Using the Console**

*To view default metric charts for a single Compute instance*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Under **Resources**, click **Metrics**.
4. In the **Metric Namespace** list, select **oci_computeagent**.

The Metrics page displays a default set of charts for the current instance.

**Not seeing any metric charts for the instance?**

If you don't see any metric charts, the instance might not be emitting metrics. See the following possible causes and resolutions.

<table>
<thead>
<tr>
<th>Possible cause</th>
<th>How to check</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Compute Instance Monitoring plugin is disabled on the instance or plugins are stopped.</td>
<td>Review the instance properties.</td>
<td>Enable the Compute Instance Monitoring plugin and start all plugins.</td>
</tr>
<tr>
<td>The instance cannot access the Monitoring service because its VCN does not use the internet.</td>
<td>Review the instance's IP address. If it's not public, then a service gateway is needed.</td>
<td>Set up a service gateway.</td>
</tr>
<tr>
<td>The instance does not use a supported image.</td>
<td>Review the supported images.</td>
<td>Create an instance with a supported image.</td>
</tr>
<tr>
<td>Older images and custom images: No Oracle Cloud Agent software exists on the instance.</td>
<td>Connect to the instance and look for the software.</td>
<td>Install the Oracle Cloud Agent software.</td>
</tr>
<tr>
<td>New instance in a new <strong>compartment</strong>: The IAM <strong>policies</strong> required for the instance to publish metrics to Monitoring are not yet initialized. More information: IAM policies are automatically created for new instances and are immediately available, unless the instances are in a new compartment. For a new instance in a new compartment, the policies can take up to 20 minutes to initialize, which delays the emission of metrics.</td>
<td>(not applicable)</td>
<td>Check back after 10 or 20 minutes.</td>
</tr>
</tbody>
</table>

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**To view default metric charts for resources related to a Compute instance**

- **For an attached block volume**:
  
  While viewing the instance's details, under **Resources**, click **Attached Block Volumes**, and then click the volume that you're interested in. Click **Metrics** to see the volume's charts. For more information about the emitted metrics, see **Block Volume Metrics** on page 585.

- **For the attached boot volume**:
  
  While viewing the instance's details, under **Resources**, click **Boot Volume**, and then click the volume that you're interested in. Click **Metrics** to see the volume's charts. For more information about the emitted metrics, see **Block Volume Metrics** on page 585.

- **For an attached VNIC**:
  
  While viewing the instance's details, under **Resources**, click **Attached VNICs**, and then click the VNIC that you're interested in. Click **Metrics** to see the charts for the VNIC. For more information about the emitted metrics, see **Networking Metrics** on page 3320.

**To view default metric charts for all Compute instances in a compartment**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Select a compartment.
3. For Metric Namespace, select `oci_computeagent`.

   The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for the instances in an instance pool

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the instance pool that you're interested in.
4. In the Metric Namespace list, select `oci_computeagent`.

   The Metrics page displays a default set of charts for the current instance pool.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Instance Pool Metrics

You can monitor the health, capacity, and performance of your Compute instance pools by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace `oci_instancepools`.

Resources: Compute instance pools.

Overview of Metrics: `oci_instancepools`

The instance pool metrics help you monitor the lifecycle state of instances in your instance pools.

Required IAM Policy

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: `oci_instancepools`

The metrics listed in the following table are automatically available for each instance pool that you create. You do not need to enable monitoring on the instances in the pool to get these metrics.

You also can use the Monitoring service to create custom queries.

Depending on the metric, the following dimensions are available:

**AvailabilityDomain**

The availability domain where the instance pool resides.
Compute

DisplayName
The friendly name of the instance pool.

FaultDomain
The fault domain where the instance pool resides.

region
The region where the instance pool resides.

resourceId
The OCID of the instance pool.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstancePoolSize</td>
<td>Instance Pool Size</td>
<td>instances</td>
<td>Number of instances in the pool.</td>
<td>DisplayName, region, resourceId</td>
</tr>
<tr>
<td>ProvisioningInstances</td>
<td>Provisioning</td>
<td>instances</td>
<td>Number of instances in the pool that are provisioning.</td>
<td>AvailabilityDomain, DisplayName, FaultDomain, region, resourceId</td>
</tr>
<tr>
<td>RunningInstances</td>
<td>Instances Running</td>
<td>instances</td>
<td>Number of running instances in the pool.</td>
<td>AvailabilityDomain, DisplayName, FaultDomain, region, resourceId</td>
</tr>
<tr>
<td>TerminatedInstances</td>
<td>Instances Terminated</td>
<td>instances</td>
<td>Number of instances in the pool that are terminating or terminated.</td>
<td>AvailabilityDomain, DisplayName, FaultDomain, region, resourceId</td>
</tr>
</tbody>
</table>

Using the Console
To view default metric charts for a single instance pool

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instance Pools.
2. Click the instance pool that you're interested in.
4. In the Metric Namespace list, select oci_instancepools.

The Metrics page displays a default set of charts for the current instance pool.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.
To view default metric charts for all instance pools in a compartment

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. Select a compartment.
3. For **Metric Namespace**, select `oci_instancepools`.

   The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

**Infrastructure Health Metrics**

You can monitor the health, capacity, and performance of the infrastructure for your Compute virtual machine (VM) and bare metal instances by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace `oci_compute_infrastructure_health`.

Resources: Compute instances.

**Overview of Metrics: oci_compute_infrastructure_health**

The Compute infrastructure health metrics help you monitor the status and health of Compute instances.

- **Instance health (up/down) status**: The `instance_status` metric lets you check whether a VM or bare metal instance is available (up) or unavailable (down) when in the running state.
- **Instance maintenance status**: The `maintenance_status` metric lets you monitor whether a VM instance is scheduled for planned infrastructure maintenance.
- **Bare metal infrastructure health status**: The `health_status` metric helps you monitor the health of the infrastructure for bare metal instances, including hardware components such as the CPU and memory.

Based on the value of the metrics, you can proactively move affected instances to healthy hardware and thereby minimize the impact on your applications.

**Required IAM Policy**

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

**Available Metrics: oci_compute_infrastructure_health**

The metrics listed in the following table are automatically available for your instances. The `instance_status` metric is available for both VM and bare metal instances, the `maintenance_status` metric is available only for VM instances, and the `health_status` metric is available only for bare metal instances. You do not need to enable monitoring on the instance to get these metrics.

You also can use the Monitoring service to create custom queries.

The metric includes the following **dimensions**: 

---

**Oracle Cloud Infrastructure User Guide** 795
The type of hardware issue:

- **CPU**: A fault has been detected in one or more CPUs.
- **MEM–BOOT**: A fault in the memory subsystem was detected during instance launch or a recent reboot.
- **MEM–RUNTIME**: A fault in the memory subsystem was detected.
- **MGMT–CONTROLLER**: A fault in the instance management controller has been detected.
- **PCI**: A fault in the PCI subsystem has been detected.
- **PCI–NIC**: A fault in the instance network interface card (NIC) has been detected.
- **SDN–INTERFACE**: A fault in the instance software defined network interface has been detected.

For troubleshooting suggestions and more information about these hardware issues, see Compute Health Monitoring for Bare Metal Instances on page 801.

**resourceDisplayName**

The friendly name of the instance.

**resourceId**

The OCID of the instance.

**maintenanceDueTime**

The scheduled start time of the 24-hour maintenance window, in the format defined by RFC3339.

**computeMaintenanceAction**

The action that Oracle Cloud Infrastructure will perform on an instance during a scheduled maintenance event:

- **REBOOT**: The instance is migrated from the physical VM host that needs maintenance to a healthy VM host. If live migration is not possible, then the instance is reboot migrated.

**recommendedAction**

The action that you can take before the scheduled maintenance event, so that you can control how and when your applications experience downtime.

- **REBOOT**: You can proactively reboot the instance before the scheduled maintenance time. When you reboot an instance for maintenance, the instance is stopped on the physical VM host that needs maintenance, and then restarted on a healthy VM host. For more information, see Moving a Compute Instance to a New Host on page 775.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>health_status</td>
<td>Infrastructure Health Status</td>
<td>Issues</td>
<td>The number of health issues for a bare metal instance. Any non-zero value indicates a health defect.</td>
<td>faultClass, resourceDisplayName, resourceId</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>instance_status</td>
<td>Instance Status</td>
<td>Count</td>
<td>The status of a running VM or bare metal instance. A value of 0 indicates that the instance is available (up). A value of 1 indicates that the instance is not available (down) due to an infrastructure issue. If the instance is stopped, then the metric does not have a value.</td>
<td>resourceDisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceId</td>
</tr>
<tr>
<td>maintenance_status</td>
<td>Maintenance Status</td>
<td>Count</td>
<td>The maintenance status of a VM instance. A value of 0 indicates that the instance is not scheduled for an infrastructure maintenance event. A value of 1 indicates that the instance is scheduled for an infrastructure maintenance event.</td>
<td>maintenanceDueTime</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>computeMaintenanceAction</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>recommendedAction</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceDisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceId</td>
</tr>
</tbody>
</table>

**Using the Console**

*To view infrastructure health metrics for a single Compute instance*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you're interested in.
3. Under **Resources**, click **Metrics**.
4. In the **Metric Namespace** list, select **oci_compute_infrastructure_health**.

The Metrics page displays a default set of charts for the current instance.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

*To view infrastructure health metrics for all Compute instances in a compartment*

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Select a compartment.
3. For **Metric Namespace**, select **oci_compute_infrastructure_health**.

The Service Metrics page dynamically updates to show charts for each metric that is emitted by the selected metric namespace.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Compute Management Metrics

You can monitor requests to the instance metadata service on compute virtual machine (VM) and bare metal instances by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace oci_compute.

Resources: compute instances.

Overview of Metrics: oci_compute

The instance metadata service (IMDS) provides metadata about an instance, its attached VNICS, and custom metadata that you supply. IMDS is available in two versions, version 1 and version 2. IMDSv2 offers increased security compared to the legacy v1.

Use the Compute management metric to identify requests to the legacy v1 endpoints. After you migrate any applications to support the v2 endpoints, you can disable all requests to the legacy v1 endpoints.

Required IAM Policy

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_compute

The metric listed in the following table is automatically available for your instances. You do not need to enable monitoring on the instance to get this metric.

You also can use the Monitoring service to create custom queries.

The metric includes the following dimensions:

- metadataVersion
  - The version of the instance metadata service that requests were made to.

- path
  - The URL path that instance metadata requests were made to.

- resourceId
  - The OCID of the instance.

- userAgent
  - The source of the instance metadata request.

- status
  - The HTTP response code for requests to instance metadata service.
## Compute NVMe Performance

The content in the sections below apply to **Category 7** and **Section 3.a** of the Oracle PaaS and IaaS Public Cloud Services Pillar documentation.

Oracle Cloud Infrastructure provides a variety of instance configurations in both bare metal and virtual machine (VM) shapes. Each shape varies on multiple dimensions including memory, CPU cores, network bandwidth, and the option of local NVMe SSD storage found in DenseIO and HPC shapes.

Oracle Cloud Infrastructure provides a service-level agreement (SLA) for NVMe performance. Measuring performance is complex and open to variability.

An NVMe drive also has non-uniform drive performance over the period of drive usage. An NVMe drive performs differently when tested brand new compared to when tested in a steady state after some duration of usage. New drives have not incurred many write/erase cycles and the inline garbage collection has not had a significant impact on IOPS.

### Using the Console

**To view management metrics for a single compute instance**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance that you’re interested in.
3. Under **Resources**, click **Metrics**.
4. In the **Metric Namespace** list, select **oci_compute**.

   The Metrics page displays a default set of charts for the current instance.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**To view management metrics for all compute instances in a compartment**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Select a compartment.
3. For **Metric Namespace**, select **oci_compute**.

   The **Service Metrics** page dynamically updates to show charts for each metric that is emitted by the selected metric namespace.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

### Using the API

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the following APIs for monitoring:

- **Monitoring API** for metrics and alarms
- **Notifications API** for notifications (used with alarms)

### Oracle Cloud Infrastructure User Guide

<table>
<thead>
<tr>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceMetadataRequests V1 Versus V2</td>
<td>Sum</td>
<td>The number of requests to the instance metadata service, comparing the version 1 and version 2 endpoints.</td>
<td>metadataVersion path resourceId userAgent status</td>
</tr>
</tbody>
</table>
performance. To achieve the goal of reproducibility and reduced variability, our testing focuses on the steady state duration of the NVMe drive’s operation.

**Testing Methodology**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before running any tests, protect your data by making a backup of your data and operating system environment to prevent any data loss. The tests described in this document will overwrite the data on the disk, and cause data corruption.</td>
</tr>
</tbody>
</table>

**Summary:** To capture the IOPS measure, first provision a shape such as the BM.DenseIO2.52 shape, and then use the Gartner Cloud Harmony test suite to run tests on an instance running the latest supported Oracle Linux 7 image for each NVMe drive target.

**Instructions:**

1. Launch an instance based on the latest supported Oracle Linux 7 image and select a shape such as the BM.DenseIO2.52 shape. For instructions, see Creating an Instance on page 695.
2. Run the Gartner Cloud Harmony test suite tests on the instance for each NVMe drive target. The following is an example of a command that will work for all shapes and drives on the shape:

   ```
   sudo ./run.sh `ls /dev/nvme[0-9]n1 | sed -e 's/\//\--target=\//'` --nopurge --noprecondition --fio_direct=1 --fio_size=10g --test=iops --skip_blocksize=512b --skip_blocksize=8k --skip_blocksize=16k --skip_blocksize=32k --skip_blocksize=64k --skip_blocksize=128k --skip_blocksize=1m
   ```

The SLA for NVMe drive performance is measured against 4k block sizes with 100% random write workload on DenseIO shapes where the drive is in a steady state of operation.

**Performance Benchmarks**

The following table lists the minimum IOPS for the specified shape to meet the SLA, given the testing methodology with 4k block sizes for 100% random write tests using the tests described in the previous section.

<table>
<thead>
<tr>
<th>Shape</th>
<th>Minimum Supported IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.DenseIO1.4</td>
<td>200k</td>
</tr>
<tr>
<td>VM.DenseIO1.8</td>
<td>250k</td>
</tr>
<tr>
<td>VM.DenseIO1.16</td>
<td>400k</td>
</tr>
<tr>
<td>BM.DenseIO1.36</td>
<td>2.5MM</td>
</tr>
<tr>
<td>VM.DenseIO2.8</td>
<td>250k</td>
</tr>
<tr>
<td>VM.DenseIO2.16</td>
<td>400k</td>
</tr>
<tr>
<td>VM.DenseIO2.24</td>
<td>800k</td>
</tr>
<tr>
<td>BM.DenseIO2.52</td>
<td>3.0MM</td>
</tr>
<tr>
<td>BM.HPC2.36</td>
<td>250k</td>
</tr>
</tbody>
</table>

Although the NVMe drives are capable of higher IOPS, Oracle Cloud Infrastructure currently guarantees this minimum level of IOPS performance.
Frequently Asked Questions

Q: I suspect a slowdown in my NVMe drive performance. Is there a SLA violation?
A: We test hosts on a regular basis to ensure that are our low-level software updates do not regress performance. If you have reproduced the testing methodology and your drive’s performance does not meet the terms in the SLA, please contact your Oracle sales team.

Q: Why does the testing methodology not represent a diversity of IO workloads such as random reads and writes to reflect real world IO?
A: We focused on reproducibility and we believe the tests provide a significant indicator of overall drive performance.

Q: Will Oracle Cloud Infrastructure change the tests in this document?
A: We will make changes to provide greater customer value through better guarantees and improved reproducibility.

Compute Health Monitoring for Bare Metal Instances

Compute health monitoring for bare metal instances is a feature that provides notifications about hardware issues with your bare metal instances. With the health monitoring feature, you can monitor the health of the hardware for your bare metal instances, including components such as the CPU, motherboard, DIMM, and NVMe drives. You can use the notifications to identify problems, letting you proactively redeploy your instances to improve availability.

Health monitoring notifications are emailed to the tenant administrator within one business day of the error occurring. This warning helps you to take action before any potential hardware failure and redeploy your instances to healthy hardware to minimize the impact on your applications.

You can also use the infrastructure health metrics available in the Monitoring service to create alarms and notifications based on hardware issues.

Error Messages and Troubleshooting

This section contains information about the most common health monitoring error messages and provides troubleshooting suggestions for you to try for your bare metal instance.

A fault has been detected in one or more CPUs

Fault class: CPU

Details: This error indicates that a processor or one or more cores have failed in your instance. Your instance might be inaccessible or there might be fewer available cores than expected.

Troubleshooting steps:
• If the instance is inaccessible, you must replace it using the steps in Moving a Compute Instance to a New Host on page 775.
• If your instance is available, check for the expected number of cores:
  • On Linux-based systems, run the following command:
    nproc --all
  • On Windows-based systems, open Resource Monitor.

  Compare the core count to the expected values documented in Compute Shapes on page 655. If the number of cores is less than expected and this reduction impacts your application, we recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

A fault in the memory subsystem was detected during instance launch or a recent reboot

Fault class: MEM-BOOT

Details: This error indicates that one or more failed DIMMs were detected in your instance while the instance was being launched or rebooted. Any failed DIMMs have been disabled.
Troubleshooting steps: The total amount of memory in the instance will be lower than expected. If this impacts your application, we recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

To check for the amount of memory in the instance:

- On Linux-based systems, run the following command:

  ```bash
  awk '$3=="kB"{${2=2/1024**2;${3="GB"}} 1}' /proc/meminfo | column -t | grep MemTotal
  ```

- On Windows-based systems, open Resource Monitor.

The expected values are documented in Compute Shapes on page 655.

A fault in the memory subsystem was detected

**Fault class:** MEM-RUNTIME

**Details:** This error indicates that one or more non-critical errors were detected on a DIMM in your instance. The instance might have unexpectedly rebooted in the last 72 hours.

**Troubleshooting steps:**

- If the instance has unexpectedly rebooted in the last 72 hours, one or more DIMMs might have been disabled. To check for the total amount of memory in the instance:

  ```bash
  awk '$3=="kB"{${2=2/1024**2;${3="GB"}} 1}' /proc/meminfo | column -t | grep MemTotal
  ```

- On Windows-based systems, open Resource Monitor.

  If the total memory in the instance is lower than expected, then one or more DIMMs have failed. If this impacts your application, we recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

- If the instance has not unexpectedly rebooted, it is at increased risk of doing so. During the next reboot, one or more DIMMs might be disabled. We recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

A fault in the instance management controller has been detected

**Fault class:** MGMT-CONTROLLER

**Details:** This error indicates that a device used to manage your instance might have failed. You might not be able to use the Console, CLI, SDKs, or APIs to stop, start, or reboot your instance. This functionality will still be available from within the instance using the standard operating system commands. You also might not be able to create a console connection to your instance. You will still be able to terminate your instance.

**Troubleshooting steps:** If this loss of control impacts your application, we recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

A fault in the PCI subsystem has been detected

**Fault class:** PCI

**Details:** This error indicates that one or more of the PCI devices in your instance have failed or are not operating at peak performance.

**Important:**

The PCI fault class will be deprecated in the future. You should migrate to the PCI-NIC fault class for similar functionality.

**Troubleshooting steps:**
• If you cannot connect to the instance over the network, the NIC might have failed. Use the Console or CLI to stop the instance and then start the instance. For steps, see Stopping and Starting an Instance on page 779.

If you're still unable to connect to the instance over the network, you might be able to connect to it using a console connection. Follow the steps in Connecting to the Serial Console on page 817 or Connecting to the VNC Console on page 822 to establish a console connection and then reboot the instance. If the instance remains inaccessible, you must replace it using the steps in Moving a Compute Instance to a New Host on page 775.

• An NVMe device may have failed.

  On Linux-based systems, run the command `sudo lsblk` to get a list of the attached NVMe devices.

  On Windows-based systems, open Disk Manager. Check the count of NVMe devices against the expected number of devices in Compute Shapes on page 655.

  If you determine that an NVMe device is missing from the list of devices for your instance, we recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

A fault in the instance network interface card (NIC) has been detected

**Fault class:** PCI-NIC

**Details:** This error indicates that one or more of the instance network interface card (NIC) devices in your instance have failed or are not operating at peak performance.

**Troubleshooting steps:** If you cannot connect to the instance over the network, the NIC might have failed. Use the Console or CLI to stop the instance and then start the instance. For steps, see Stopping and Starting an Instance on page 779.

If you're still unable to connect to the instance over the network, you might be able to connect to it using a console connection. Follow the steps in Connecting to the Serial Console on page 817 or Connecting to the VNC Console on page 822 to establish a console connection and then reboot the instance. If the instance remains inaccessible, you must replace it using the steps in Moving a Compute Instance to a New Host on page 775.

A fault in the instance software defined network interface has been detected

**Fault class:** SDN-INTERFACE

**Details:** If you cannot connect to the instance or if you're experiencing networking issues, the software-defined network interface device might have a fault.

**Troubleshooting steps:** Although restarting the instance might temporarily resolve the issue, we recommend that you replace the instance using the steps in Moving a Compute Instance to a New Host on page 775.

**Microsoft Licensing on Oracle Cloud Infrastructure**

This topic provides information about the licensing requirements to use Microsoft products on Oracle Cloud Infrastructure.

For more information about how to bring your own Microsoft licenses to Oracle Cloud Infrastructure, see Licensing Options for Microsoft Windows on page 809.

For information about how to move eligible Microsoft server application licenses to Oracle Cloud Infrastructure by enrolling in the License Mobility through Microsoft Software Assurance benefit, see Moving Microsoft Licenses to Oracle Cloud Infrastructure: Microsoft License Mobility on page 811.

**Using Microsoft Windows on Oracle Cloud Infrastructure: FAQ**

Oracle Cloud Infrastructure is licensed to provide Microsoft software offerings. Oracle is a member of the Microsoft Partner Network, licensed to sell Microsoft software under the Service Provider License Agreement (SPLA). Oracle is also an authorized Microsoft Authorized Mobility Partner with an active Premier Support for Partners agreement with Microsoft.

For the latest Microsoft licensing requirements, refer to the Microsoft Product Terms.
Compute

If you can't find the answer to your question here, or you need more assistance running Microsoft products on Oracle Cloud Infrastructure, contact Oracle Support.

**General Questions**

**What OS editions of Microsoft Windows Server are supported?**

**Oracle-provided images**

These Windows versions are available for Oracle-provided images:

- Windows Server 2012 R2 Standard, Datacenter
- Windows Server 2016 Standard, Datacenter
- Windows Server 2019 Standard, Datacenter

**Bring Your Own Image (BYOI)**

These Windows versions support custom image import:

- Windows Server 2008 R2 Standard, Enterprise, Datacenter
- Windows Server 2012 Standard, Datacenter
- Windows Server 2012 R2 Standard, Datacenter
- Windows Server 2016 Standard, Datacenter
- Windows Server 2019 Standard, Datacenter

If you don't need to migrate your Windows OS licenses, you can use the Bring Your Own Image process to migrate your Windows image to Oracle Cloud Infrastructure.

**Is Windows Server 2019 available as an Oracle-provided image?**

Yes, Windows Server 2019 is available as an Oracle-provided image.

**Is Windows Server 2019 available as a Bring Your Own Image (BYOI) image?**

Yes, you can import your own Windows Server 2019 image for virtual machines only. For source image requirements and steps to import an image, see Importing Custom Windows Images on page 677.

**What VM and bare metal options are available for Windows Server operating systems?**

The following table shows support for Microsoft Windows Server operating systems on Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Bare Metal Machines</th>
<th>Virtual Machines (VMs)</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an Oracle-provided Windows Server operating system image for Windows Server 2012 R2 and later versions.</td>
<td>Supported</td>
<td>Supported</td>
<td>SPLA volume license issued by Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Bring your own virtual machine image. You can import your own custom virtual machine Windows Server OS image.</td>
<td>Not supported</td>
<td>Supported</td>
<td>SPLA volume license issued by Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Bring your own Windows Server ISO image.</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Customer-owned license</td>
</tr>
</tbody>
</table>
Does Oracle Cloud Infrastructure support Bring Your Own Image (BYOI) for Windows Server?

Yes, you are permitted to import your own generalized custom image of Windows Server.

When you create an instance with an imported image on a VM or a shared bare metal machine, Oracle Cloud Infrastructure licenses the instance. For more information about imported images, see Creating Windows Custom Images on page 668.

If you want to use your own license, BYOI is supported only for bare metal machines on a dedicated host.

How am I charged for Windows Server on Oracle Cloud Infrastructure?

The cost of a Microsoft Windows Server license is an additional cost, on top of the underlying Compute instance price. You pay separately for the Compute instance and the Windows Server license. For more information about Microsoft Windows Server pricing, see Compute Pricing.

Billing for the Windows Server license is based on per-OCPU, per-second usage. Billing starts when an instance is in the “running” state and ends when you terminate (delete) the instance.

When an instance is stopped, billing for the Windows Server license depends on the shape that was used to create the instance. Billing pauses for instances that use a Standard shape. Billing continues for instances that use a Dense I/O shape, GPU shape, or HPC shape. Depending on the shape, you might also be billed for the underlying Compute instance when the instance is stopped.

How does Windows Server get updated with the latest patches?

You must update your VCN’s security list to enable egress traffic for port 80 (HTTP) and port 443 (HTTPS) to install patches from Microsoft. Oracle Cloud Infrastructure enables automatic updates for Microsoft Windows Server and uses the default settings for applying Windows Server patches.

Can I take a snapshot image after customizing a running Window Server instance?

Yes, there are several options available on both bare metal and virtual machines:

- **Create a custom image:** Creates a custom image that you can use to launch other instances. Instances that you launch from your image include the customizations, configuration, and software installed when you created the image.
- **Clone a boot volume:** Makes a copy of an existing boot volume without needing to go through the backup and restore process. A boot volume clone is a point-in-time direct disk-to-disk deep copy of the source boot volume, so all the data that is in the source boot volume when the clone is created is copied to the boot volume clone.
- **Back up a block volume:** Makes a point-in-time backup of data on a block volume. You can restore a backup to a new volume either immediately after a backup or at a later time that you choose.
- **Back up a boot volume:** Makes a backup of a boot volume. Boot volume backup capabilities are the same as block volume backup capabilities and are in-region only. Windows boot volume backups cannot be copied across regions.

Can I export a custom Windows Server image?

Yes, exporting custom Windows Server operating system images is supported.
When exporting Windows-based images, you are responsible for complying with the Microsoft Product Terms and all product use conditions, as well as verifying your compliance with Microsoft.

For steps to export an image, see Image Import/Export on page 670.

**What support is available for Microsoft Windows Server on Oracle Cloud Infrastructure?**

Oracle Support provides limited assistance for Oracle-provided Microsoft Windows Server images if the Windows Server version has not reached end of support with Microsoft. All other Microsoft software is supported directly by Microsoft Support.

Oracle Support can help verify that the operating system boots, that the operating system connects to the network, and that attached storage connects and performs as expected. If you encounter other issues with Microsoft Windows Server, work directly with Microsoft Support to resolve the issue. For more information, see Support Options for Microsoft Windows on page 812.

**How do I upgrade to a newer version of Windows Server?**

To upgrade to a newer version of Windows Server, you can do either of the following things:

- Obtain the installation media from Microsoft or your Microsoft reseller, and then upgrade the existing Compute instance. The license issued by Oracle Cloud Infrastructure remains in effect.
- Create a new Compute instance using the desired version of the Windows Server platform image, and then migrate your applications and data to the new instance.

**Licensing - Windows Server**

**What is BYOL?**

BYOL stands for "bring your own license." BYOL lets you use software licenses that you already own to deploy software on Oracle Cloud Infrastructure, without any additional licensing fees. This process uses the License Mobility through Microsoft Software Assurance benefit provided by Microsoft. You must have active Software Assurance with Microsoft to bring your licenses to Oracle Cloud Infrastructure.

**What is Microsoft License Mobility?**

License Mobility through Software Assurance is a Microsoft benefit that permits you to move your eligible Microsoft licenses to cloud services providers such as Oracle Cloud Infrastructure. Oracle is an Authorized Mobility Partner for License Mobility.

With License Mobility through Software Assurance, you can deploy eligible application servers on bare metal hosts or virtual shared hardware in Oracle Cloud Infrastructure. An example of an application eligible for License Mobility through Software Assurance is Microsoft SQL. Windows Server operating systems are not eligible.

You may move Microsoft licenses from on-premises or another Authorized Mobility Partner only after more than 90 days have passed since the last license move.

For more information about this Microsoft benefit, see License Mobility through Microsoft Software Assurance. For steps to move your Microsoft licenses to Oracle Cloud Infrastructure, see Moving Microsoft Licenses to Oracle Cloud Infrastructure: Microsoft License Mobility on page 811.

**Is Oracle a Microsoft Authorized Mobility Partner?**

Yes, Oracle is an Authorized Mobility Partner for the Microsoft License Mobility through Software Assurance benefit.

**Can I bring my own license for Microsoft Windows Server to Oracle Cloud Infrastructure?**

Yes. You can bring your own license (BYOL) for Microsoft Windows Server on a dedicated bare metal or dedicated virtual machine host, subject to the Microsoft Product Terms. You are responsible for managing your own licenses to maintain compliance with Microsoft licensing terms. For more information, see Licensing Options for Microsoft Windows on page 809.

The following table shows the BYOL requirements for Microsoft licenses on Oracle Cloud Infrastructure.
<table>
<thead>
<tr>
<th>Microsoft License</th>
<th>Bare Metal Machines and Dedicated Virtual Machine Hosts</th>
<th>Virtual Machines (Multi-Tenant Shared Host)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Server</strong></td>
<td>BYOL on a bare metal dedicated host is only eligible when using a KVM hypervisor. BYOL is not eligible for Microsoft Windows Server using Oracle-provided images or when importing your own Microsoft Windows Server image.</td>
<td>Not eligible. Shared hosts must use Oracle-provided images that include the Microsoft license.</td>
</tr>
<tr>
<td><strong>SQL Server</strong></td>
<td>Eligible. You must have License Mobility through Software Assurance.</td>
<td>Eligible. You must have License Mobility through Software Assurance.</td>
</tr>
<tr>
<td><em>Subject to the Microsoft Product Terms</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft 365 Apps for enterprise (Office 365 ProPlus) and Office Professional Plus</strong></td>
<td>Eligible. You must have an Enterprise Agreement license with Software Assurance or a Windows Virtual Desktop Access (VDA) license.</td>
<td>Not eligible.</td>
</tr>
<tr>
<td><strong>Windows 7, Windows 8, and Windows 10</strong></td>
<td>Eligible. You must have an Enterprise Agreement license with Software Assurance or a Windows Virtual Desktop Access (VDA) license.</td>
<td>Not eligible.</td>
</tr>
<tr>
<td><strong>Other Microsoft applications</strong></td>
<td>Eligible. Subject to the Microsoft Product Terms.</td>
<td>Eligible. You must have License Mobility through Software Assurance.</td>
</tr>
</tbody>
</table>

Application licenses such as SQL Server or System Center require License Mobility through Software Assurance when running on Oracle Cloud Infrastructure VM instances. License Mobility is not used for Microsoft Office, Windows clients, or Windows Server BYOL. Review the Microsoft Product Terms to validate which applications support License Mobility.

Direct questions about your licensing rights to Microsoft or your Microsoft reseller.

**Can I use virtual machines and bring my own license for Microsoft Windows Server to Oracle Cloud Infrastructure?**

You cannot migrate your Windows Server OS licenses when using Oracle Cloud Infrastructure virtual machines. However, you can `bring your own hypervisor` (KVM) to run a Windows Server VM with your own Windows Server OS license.

The following restrictions apply:

- You can use VMs with their own license only if you use bring your own hypervisor on a dedicated bare metal host.
- BYOL of Microsoft Windows Server is not supported for VMs running on a shared host. Oracle Cloud Infrastructure-provided VMs offer Windows Server.
  - You can use a bare metal instance under bring your own hypervisor.
  - You must install and manage a hypervisor (KVM or Hyper-V) and launch your own VMs. This will ensure isolation, because all Oracle VMs are running on a dedicated bare metal server.
• BYOL on a dedicated host (KVM hypervisor only) is permitted for Microsoft Windows Server.
• VMs can run Windows Server with a Visual Studio (MSDN) subscription license when used for development use only.

Licensing - Other Microsoft Software

What other Microsoft applications can I bring to Oracle Cloud Infrastructure?

Any Microsoft Server licenses permitted on Oracle Cloud Infrastructure must be eligible according to the latest Microsoft Product Terms. It is your responsibility to verify that the licensing agreements with Microsoft permit you to bring on-premises perpetual Microsoft licenses to Oracle Cloud Infrastructure and are eligible licensed products according to the latest Microsoft Product Terms. Microsoft application products that are currently eligible for License Mobility require an active Software Assurance benefit to move your license. For more information, see Moving Microsoft Licenses to Oracle Cloud Infrastructure: Microsoft License Mobility on page 811.

Can I bring my own SQL Server license to Oracle Cloud Infrastructure?

Yes, you can bring your own SQL Server license using License Mobility through Active Software Assurance. The following restrictions apply:

• When you move your Microsoft SQL license using the license mobility process, the Microsoft Windows Server license is not included. Microsoft Windows Server licenses are not permitted to be moved under License Mobility. Windows Server operating systems must use the license issued by Oracle Cloud Infrastructure.
• Perpetual licenses can be moved from on-premises or other cloud providers only after more than 90 days have passed since the last license move.
• End-of-support versions are not supported on shared host virtual machines on Oracle Cloud Infrastructure.

Follow the license mobility process to move your SQL Server license to Oracle Cloud Infrastructure.

Can I use my Visual Studio (MSDN) license on Microsoft Windows Server on Oracle Cloud Infrastructure?

Yes, you can use your Visual Studio (MSDN) subscription license for non-production purposes on Oracle Cloud Infrastructure on either bare metal or virtual machine instances. You are responsible for complying with the Visual Studio subscription terms.

Can I buy a Visual Studio (MSDN) subscription from Oracle Cloud Infrastructure?

No, Oracle does not sell Visual Studio (MSDN) subscriptions. Contact Microsoft or your Microsoft reseller.

Can I use a Visual Studio (MSDN) license for a production environment?

No, Visual Studio (MSDN) subscription licenses are for development, testing, or demonstration purposes only.

How can I remote access to a Windows Server instance on Oracle Cloud Infrastructure?

Follow the steps to connect to a Windows instance. Windows operating systems permit remote access for a maximum of two users using Remote Desktop Services (RDS) for Administration purposes.

RDS Client Access Licenses (CALs) are required for each user or device using Remote Desktop.

Does Oracle Cloud Infrastructure offer additional Remote Desktop Services licenses for applications running on Windows VMs?

No, Oracle Cloud Infrastructure does not offer Microsoft RDS (Remote Desktop Server) Subscriber Access Licenses (SALs). You can bring your own license (BYOL) and use your RDS Client Access Licenses (CALs) on Oracle Cloud Infrastructure bare metal or virtual machines only if you have active Software Assurance coverage and move those licenses using the license mobility process.

Can I bring my own RDS CALs if I want more than two users to access my Windows Server instance?

Yes, you can use your Remote Desktop Services (RDS) Client Access Licenses (CALs) on Oracle Cloud Infrastructure if you use the Oracle Cloud Infrastructure bare metal offering. In addition, you can use virtual machines with their own Visual Studio (MSDN) subscription license if you bring your own hypervisor (KVM).
You can use your RDS CAL licenses on Oracle Cloud Infrastructure virtual machines only if you have active Software Assurance coverage and move your CALs using the license mobility process.

**Can I bring my own System Center Management Licenses to Oracle Cloud Infrastructure?**

You can bring Microsoft System Center server Management Licenses (server MLs) using the license mobility process. There are minimums to take into consideration with System Center Management License 2-core licenses and 16-core licenses. A virtual machine requires a minimum of 16 core licenses to be assigned to it, and more if the VM has more than 16 virtual cores.

System Center client Management Licenses (client MLs) are not eligible for license mobility and cannot be moved to Oracle Cloud Infrastructure.

**Other Windows Server Questions**

**Are there user data capabilities when launching Windows Server images?**

Yes, Oracle-provided Windows images include cloudbase-init installed by default. You can use cloudbase-init to run PowerShell scripts, batch scripts, or other user data content on instance launch. Cloudbase-init is the equivalent of cloud-init on Linux-based images.

**Can I use Windows Remote Management on Oracle Cloud Infrastructure?**

Yes, Microsoft Windows Remote Management (WinRM) is enabled by default on Oracle-provided Windows images. WinRM enables you to remotely manage the operating system.

**What is Microsoft end of support?**

Microsoft establishes the support lifecycle policy for its products. When a product reaches the end of its support lifecycle, Microsoft no longer provides security updates for the product. You should upgrade to the latest version to remain secure.

**Can I use Windows Server 2008 R2 even though it's past the end-of-support date?**

Windows Server 2008 R2 reached the end of its support lifecycle on January 14, 2020. Although you can continue to import your own Windows 2008 R2 images and run your existing instances, you are at a higher risk of security issues, incompatibility, or failures. Oracle does not provide any operating system support for end-of-support operating systems.

Oracle Cloud Infrastructure does not provide platform images after the end-of-support date. However, you can import your own image and launch it on a shared host VM.

There are no restrictions to running end-of-support operating systems on bare metal machines on a dedicated host. You may bring your own image (BYOI) of a Windows Server 2008 R2 image, but you must import a custom OS image and run the image on a dedicated host.

**Can I purchase Microsoft Extended Security Updates for end-of-support Windows OSs?**

Yes, you can purchase Extended Security Updates (ESUs) from Microsoft for use on Oracle Cloud Infrastructure. For VMs on shared infrastructure, you must have an enterprise agreement in place with Microsoft. With that agreement in place, you can purchase ESUs per virtual core matching the number of OCPUs per VM instance, with a minimum requirement of 16 virtual core licenses per VM instance.

For bare metal machines, you must have an enterprise agreement in place with Microsoft. With that agreement in place, you can purchase ESUs per physical core of the dedicated bare metal host.

Oracle Cloud Infrastructure cannot purchase ESUs on your behalf.

You are fully responsible for purchasing the correct number of ESUs for your instances. Oracle Cloud Infrastructure does not keep track of whether you have enough ESUs.

**Licensing Options for Microsoft Windows**

You can choose to bring your own license (BYOL) for Microsoft applications that you want to run on Oracle Cloud Infrastructure, or use a license that is issued by Oracle.
The following table describes the licensing models that are available for using Microsoft Windows images on Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>Image</th>
<th>License</th>
<th>Additional Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle-provided image</td>
<td>Issued by Oracle</td>
<td>VM instances on a shared host, bare metal instances, and VM instances launched on a dedicated host are all permitted. BYOL for Oracle-provided images is not available.</td>
</tr>
<tr>
<td>Bring your own image (BYOI)</td>
<td>Issued by Oracle</td>
<td>VM instances on a shared host, bare metal instances, and VM instances launched on a dedicated host are all permitted. Import the image. Oracle will issue a license when an instance is created using the imported image.</td>
</tr>
<tr>
<td>Bring your own image (BYOI)</td>
<td>BYOL</td>
<td>Instances must be launched on a dedicated host. Create a bare metal instance using the KVM image from Marketplace. Then, copy your Windows guest OS to the hypervisor.</td>
</tr>
<tr>
<td>Bring your own Hyper-V</td>
<td>Issued by Oracle</td>
<td>Instances must be launched on a dedicated host. Create a bare metal instance using the Oracle-provided Windows Server Datacenter platform image. Then, copy your on-premises guest OS to Hyper-V on the bare metal instance.</td>
</tr>
</tbody>
</table>

**Bringing Your Own Microsoft License**

You can BYOL for Microsoft application licenses that are eligible for License Mobility with active Software Assurance onto virtual machines and dedicated hosts. According to the Microsoft Product Terms, some of the applications that are permitted for BYOL include the following:

- Microsoft SQL Server
- Microsoft Exchange Server
- Microsoft SharePoint Server
- Microsoft System Center
- Microsoft Dynamics products

Any Microsoft Server licenses permitted on Oracle Cloud Infrastructure must be eligible according to the latest Microsoft Product Terms. It is your responsibility to verify that the licensing agreements with Microsoft permit you to bring on-premises perpetual Microsoft licenses to Oracle Cloud Infrastructure and are eligible licensed products according to the latest Microsoft Product Terms. Microsoft application products that are currently eligible for License Mobility require an active Software Assurance benefit to move your license. For more information, see Moving Microsoft Licenses to Oracle Cloud Infrastructure: Microsoft License Mobility on page 811.
For Microsoft Windows Server OS, there are restrictions. BYOL is only permitted for eligible Windows OS licenses with active Software Assurance running on a dedicated bare metal host or a dedicated VM host using a KVM hypervisor.

For Windows clients (Windows 8 and Windows 10), BYOL is permitted for Enterprise Agreement licenses with an active Software Assurance benefit or with Windows Virtual Desktop Access (VDA) licenses.

Activating licenses can either be scripted on startup using the slmgr.vbs command line tool or by using your own Microsoft Key Management Service (KMS) server.

**Activating Licenses on a Dedicated Host**

When you bring your own Microsoft licenses, you are responsible for validating that your licensing agreements with Microsoft permit you to move your own licenses to Oracle Cloud Infrastructure. It is your responsibility to ensure that you comply with all Microsoft product terms and product use conditions.

**Moving Microsoft Licenses to Oracle Cloud Infrastructure: Microsoft License Mobility**

Microsoft Volume Licensing customers can move eligible Microsoft server application licenses purchased under a Volume Licensing agreement to Oracle Cloud Infrastructure. To do this, you must enroll in the License Mobility through Microsoft Software Assurance benefit. This benefit is included with an active Software Assurance contract. You don't need to purchase additional Microsoft software licenses, and there are no associated mobility fees.

For more information about this Microsoft benefit, see [License Mobility through Microsoft Software Assurance](https://www.microsoft.com).

**Eligibility Requirements**

To enroll in Microsoft License Mobility through Software Assurance, you must be a Microsoft Volume License customer with eligible server application products. The following are key requirements:

- Windows Server operating systems, desktop client operating systems, and desktop applications such as Microsoft Office are not eligible under License Mobility through Software Assurance. You can bring your own license (BYOL) outside of License Mobility onto a dedicated host. For more information, see [Can I bring my own license for Microsoft Windows Server to Oracle Cloud Infrastructure?](https://www.oracle.com) on page 806.
- Active Software Assurance coverage is required on eligible licenses migrated to Oracle Cloud Infrastructure.
- All licenses that are used to run and access your licensed software require active Software Assurance coverage. This includes server licenses, processor licenses, Client Access Licenses (CALs), External Connector (EC) licenses, and server management licenses. Your rights to run licensed software and manage instances on Oracle Cloud Infrastructure expire with the expiration of the Software Assurance coverage on those licenses.
- Eligible Volume Licensing programs include the Microsoft Enterprise Agreement, Microsoft Enterprise Subscription Agreement, and Microsoft Open Value agreement, where Software Assurance is included, and other Volume Licensing programs where Software Assurance is an option, such as the Microsoft Open License agreement and the Microsoft Select Plus agreement.
- You may move Microsoft licenses from on-premises or another cloud services provider only after more than 90 days have passed since the last license move.
- Eligible Microsoft licenses on Oracle Cloud Infrastructure must be maintained for a minimum period of 90 days in a specific Oracle Cloud Infrastructure region. After the 90-day period, you may move the licensed software to a shared host in another Oracle Cloud Infrastructure region.
- Any Microsoft Server licenses permitted on Oracle Cloud Infrastructure must be eligible according to the latest Microsoft Product Terms. It is your responsibility to verify that the licenses you bring to Oracle Cloud Infrastructure are eligible according to the latest Microsoft Product Terms.

**Enrolling in License Mobility through Software Assurance**

All customers using License Mobility through Software Assurance must complete a license verification process. Microsoft verifies that you have eligible licenses with active Software Assurance and sends confirmation when the verification process is complete.

You can deploy your application server software before completing the verification process, but you must submit the license verification form within 10 days of deployment.
You are responsible for managing true ups and renewals as required under your Volume Licensing agreement. You must submit a new form each time that you deploy additional licenses, when you renew your agreement, and when you deploy any previously unverified products.

To enroll in License Mobility through Software Assurance:

1. Verify that you are a Microsoft Volume Licensing customer with eligible application server licenses that are covered by active Software Assurance.
2. Download the license verification form:
   a. Go to the Microsoft Product Licensing search page.
   b. In the Document Type area, select License Verification.
   c. Filter the results by language, region, and business sector. Note that the verification form is not available in the WW (World Wide) region.
   d. Download the LicenseMobilityVerif document.
3. Complete the license verification form. To specify Oracle as the Authorized Mobility Partner, provide the following information:
   • Authorized Mobility Partner Name: Oracle America, Inc.
   • Authorized Mobility Partner Website URL: http://www.oracle.com/
   • Authorized Mobility Partner Email Address: microsoftlm_us_grp@oracle.com
   For instructions to complete the form, see the Microsoft License Mobility Verification Guide (PDF).
4. Submit the completed verification form to both Microsoft and Oracle:
   • Microsoft: Submit the form through your Microsoft reseller or directly to the email address in the form.
   • Oracle: Send the form to microsoftlm_us_grp@oracle.com.

Microsoft and Oracle verify that the product licenses for the workloads you deploy to Oracle Cloud Infrastructure are eligible according to the terms of your License Mobility through Software Assurance benefit. Microsoft will communicate your verification status to you and to Oracle as an Authorized Mobility Partner.

Support Options for Microsoft Windows

Oracle Support provides limited assistance for Microsoft Windows Server operating systems running on Oracle Cloud Infrastructure and for SQL Server images provided by Oracle Cloud Marketplace. For product issues, work directly with Microsoft Support.

**Microsoft Windows Server**

Oracle Support provides limited assistance for Microsoft Windows Server operating systems running on Oracle Cloud Infrastructure as long as the Windows Server version has not reached end of support with Microsoft. For details about Microsoft Windows lifecycles, see Lifecycle FAQ - Windows.

In order for Oracle to provide support for Bring Your Own Image (BYOI) images, the images must follow the guidelines outlined in Importing Custom Windows Images on page 677 and must meet all Microsoft licensing requirements.

Under these conditions, Oracle Support can help verify that:

- the operating system boots
- the operating system connects to the network
- attached storage connects and performs as expected

If you encounter other issues with Microsoft Windows Server, work directly with Microsoft Support to resolve the issue. Microsoft Support provides assistance when you have an existing Premier Support agreement or when you pay for professional support.

**SQL Server**

Oracle Support provides limited assistance with SQL Server images provided by Oracle Cloud Marketplace. For product issues, work directly with Microsoft Support.
For SQL Server images provided by Oracle Cloud Marketplace, Oracle Support can help verify that the services start and that they allow local connections.

The following tasks fall outside the scope of Oracle Support and should be addressed directly with Microsoft Support. Microsoft Support provides assistance when you have an existing Premier Support agreement or when you pay for professional support.

- Query optimization
- Failover clustering
- Issues with third-party applications and with Microsoft applications that are not included in the Oracle Cloud Marketplace image. For example, software fails to install errors.
- Image configurations that diverge from Oracle’s standard configurations. For example, requests such as Roaming Profiles are going into read-only mode when our users log in via terminal server/RDS are out of scope.
- Activities that breach the Microsoft license terms of use

Troubleshooting Compute Instances

For information about how to troubleshoot issues with compute instances, see the following topics:

- Troubleshooting Instances Using Instance Console Connections on page 813. To debug issues that happen during instance launch or during the OS boot sequence, use a serial console connection or a VNC console connection.
- Sending a Diagnostic Interrupt on page 825. To debug a running virtual machine (VM) instance that becomes unresponsive, you can generate a copy of the system memory (also called a crash dump) by sending a diagnostic interrupt to the instance.

Troubleshooting Instances Using Instance Console Connections

The Oracle Cloud Infrastructure Compute service provides console connections that enable you to remotely troubleshoot malfunctioning instances, such as:

- An imported or customized image that does not complete a successful boot
- A previously working instance that stops responding

Two types of instance console connections exist: serial console connections and VNC console connections. Instance console connections are for troubleshooting purposes only. To connect to a running instance for administration and general use with Secure Shell (SSH) or Remote Desktop connection, see Connecting to an Instance on page 733.

To configure your console connection, follow these steps:

1. Make sure you have the correct permissions.
2. Complete the prerequisites, including creating your SSH key pair.
3. Create the instance console connection.
4. Connect to the serial console or connect to the VCN console.
5. If you're trying to connect to the serial console and you think the connection isn't working, test your connection to the serial console using Cloud Shell.

Required IAM Policies

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

To create instance console connections, an administrator needs to grant user access to manage instance console connections and to read instances through an IAM policy. The resource name for instance console connections is instance-console-connection. The resource name for instances is instance. The following policies grant users the ability to create instance console connections:

Allow group <group_name> to manage instance-console-connection in tenancy
Allow group <group_name> to read instance in tenancy

Instance console connections also support network sources. The following policies grant users the ability to create instance console connections with a network source:

Allow group <group_name> to manage instance-console-connection in tenancy
where request.networkSource.name='example-network-source'
Allow group <group_name> to read instance in tenancy where
request.networkSource.name='example-network-source'

If you're new to policies, see Getting Started with Policies and Common Policies.

Prerequisites

Complete these prerequisites before creating the instance console connection.

Installing an SSH Client and a Command-line Shell (Windows)

Windows does not include an SSH client by default. If you are connecting from a Windows client, you need to install an SSH client. You can use PuTTY plink.exe with Windows PowerShell or software that includes a version of OpenSSH such as:

- Git for Windows
- Windows Subsystem for Linux

The instructions in this topic frequently use PuTTY and Windows PowerShell.

If you want to make the console connection from Windows with Windows PowerShell, PowerShell might already be installed on your Windows operating system. If not, follow the steps at the link. If you are connecting to the instance from a Windows client using PowerShell, plink.exe is required. plink.exe is the command link connection tool included with PuTTY. You can install PuTTY or install plink.exe separately. For installation information, see http://www.putty.org.

Creating SSH Key Pairs

To create the secure console connection, you need an SSH key pair. The method to use for creating key pairs depends on your operating system. When connecting to the serial console, you must use an RSA key. The instructions in this section show how to create an RSA SSH key pair.

Creating the SSH key pair for Linux

For detailed instructions about creating an SSH key pair to use on Linux, see Managing Key Pairs on Linux Instances on page 693.

To create an SSH key pair on the command line

If you're using a UNIX-style system, you probably already have the ssh-keygen utility installed. To determine whether the utility is installed, type ssh-keygen on the command line. If the utility isn't installed, you can download OpenSSH for UNIX from http://www.openssh.com/portable.html and install it.

1. Open a shell or terminal for entering the commands.
2. At the prompt, enter ssh-keygen and provide a name for the key when prompted. Optionally, include a passphrase.

   The keys will be created with the default values: RSA keys of 2048 bits.

Alternatively, you can type a complete ssh-keygen command, for example:

```
ssh-keygen -t rsa -N "" -b 2048 -C "<key_name>" -f <path/root_name>
```

The command arguments are shown in the following table:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t rsa</td>
<td>Use the RSA algorithm.</td>
</tr>
</tbody>
</table>
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-N &quot;&lt;passphrase&gt;&quot;</td>
<td>A passphrase to protect the use of the key (like a password). If you don't want to set a passphrase, don't enter anything between the quotes. A passphrase is not required. You can specify one as a security measure to protect the private key from unauthorized use. If you specify a passphrase, when you connect to the instance you must provide the passphrase, which typically makes it harder to automate connecting to an instance.</td>
</tr>
<tr>
<td>-b 2048</td>
<td>Generate a 2048-bit key. You don't have to set this if 2048 is acceptable, as 2048 is the default. A minimum of 2048 bits is recommended for SSH-2 RSA.</td>
</tr>
<tr>
<td>-C &quot;&lt;key_name&gt;&quot;</td>
<td>A name to identify the key.</td>
</tr>
<tr>
<td>-f &lt;path/root_name&gt;</td>
<td>The location where the key pair will be saved and the root name for the files.</td>
</tr>
</tbody>
</table>

---

### Creating the SSH key pair for Windows using PuTTY

If you are using a Windows client to connect to the instance console connection, use an SSH key pair generated by PuTTY.

**To create the SSH key pair using PuTTY**

1. Find `puttygen.exe` in the PuTTY folder on your computer, for example, `C:\Program Files (x86)\PuTTY`. Double-click `puttygen.exe` to open it.

2. Specify a key type of SSH-2 RSA and a key size of 2048 bits:
   - In the **Key** menu, confirm that the default value of **SSH-2 RSA key** is selected.
   - For the **Type of key to generate**, accept the default key type of **RSA**.
   - Set the **Number of bits in a generated key** to 2048 if not already set.

3. Click **Generate**.

4. To generate random data in the key, move your mouse around the blank area in the PuTTY window.

5. When the key is generated, it appears under **Public key for pasting into OpenSSH authorized_keys file**.

6. A **Key comment** is generated for you, including the date and timestamp. You can keep the default comment or replace it with your own more descriptive comment.

7. Leave the **Key passphrase** field blank.
7. Click **Save private key**, and then click **Yes** in the prompt about saving the key without a passphrase.

The key pair is saved in the PuTTY Private Key (PPK) format, which is a proprietary format that works only with the PuTTY tool set.

You can name the key anything you want, but use the .ppk file extension. For example, *mykey.ppk*.

8. Select **all** of the generated key that appears under **Public key for pasting into OpenSSH authorized_keys file**, copy it using **Ctrl + C**, paste it into a text file, and then save the file in the same location as the private key.

(Do not use **Save public key** because it does not save the key in the OpenSSH format.)

You can name the key anything you want, but for consistency, use the same name as the private key and a file extension of pub. For example, *mykey.pub*.

9. Write down the names and location of your public and private key files. You need the public key when creating an instance console connection. You need the private key to connect to the instance console connection using PuTTY.

**Signing in to an instance from the serial console (optional)**

To troubleshoot instances and see serial output using the serial console, you don't need to sign in. To connect to a running instance for administration and general use with Secure Shell (SSH) or Remote Desktop connection, see **Connecting to an Instance** on page 733.

If you want to sign in to an instance using an instance console connection, you can use Secure Shell (SSH) or Remote Desktop connection to sign in. If you want to sign in with a username and password, you need a user account with a password. Oracle Cloud Infrastructure does not set a default password for the **opc** user. Therefore, if you want to sign in as the opc user, you need to create a password for the opc user. Otherwise, add a different user with a password and sign in as that user.

**Connecting Through Firewalls**

If your system is behind a firewall, the system must be able to reach the console servers. The client system connecting to the serial console must be able to reach the serial or VCN console server (for example, *instance-console.us-ashburn-1.oraclecloud.com*) over SSH using port 443, directly or through a proxy.

**Supported Instance Types**

Serial console connections are supported on the following types of instances:

- Virtual machine (VM) instances launched in September 2017 or later
- Bare metal instances launched in November 2017 or later

VNC console connections are supported on the following types of instances:

- VM instances launched on October 13, 2017 or later
- Bare metal instances that use one of the following shapes:
  - BM.Standard2.52 - launched on February 21, 2019 or later
  - BM.Standard.E2.64 - launched after September 17, 2020 in the Oracle Cloud Infrastructure commercial realm
  - BM.Standard.E3.128 - launched on February 21, 2019 or later
  - BM.DenseIO2.52 - launched on February 21, 2019 or later
  - BM.GPU2.2 - launched on February 21, 2019 or later
  - BM.GPU3.8 - launched on February 21, 2019 or later
  - BM.GPU.4.8 - launched on February 21, 2019 or later
  - BM.HPC2.36 - launched on February 21, 2019 or later

**Creating the Instance Console Connection**

Before you can connect to the serial console or VNC console, you need to create the instance console connection.

**Note:**

Instance console connections are limited to one client at a time. If the client fails, the connection remains active for approximately five minutes. During this time, no other client can connect. After five minutes, the connection is
closed, and a new client can connect. During the five-minute timeout, any attempt to connect a new client fails with the following message:

```
channel 0: open failed: administratively prohibited: console access is limited to one connection at a time
Connection to <instance and OCID information> closed.
```

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you're interested in.
3. Under Resources, click Console Connection.
4. Click Create Console Connection.
5. Upload the public key portion for the SSH key. You have three options for adding the SSH key.
   - **Generate SSH key pair**: You can have Oracle Cloud Infrastructure generate an SSH key pair to use. If you are using PowerShell or PuTTY to connect to the instance from a Windows client, you cannot use the generated SSH key pair without first converting it to a .ppk file.
     - To convert a generated .key private key file
       a. Open PuTTYgen.
       b. Click Load, and select the private key generated when you created the instance. The extension for the key file is .key.
       c. Click Save private key.
       d. Specify a name for the key. The extension for new private key is .ppk.
       e. Click Save.
   - **Choose public key file**: Browse to a public key file on your computer. If you followed the steps in Creating SSH Key Pairs on page 814 in the Prerequisites section to create a key pair, use this option to navigate to the .pub file.
   - **Paste public key**: Paste the content of your public key file into the text box.
6. Click Create Console Connection.

When the console connection has been created and is available, the state changes to Active.

Connecting to the Serial Console

After you create the console connection for the instance, you can connect to the serial console using a Secure Shell (SSH) connection. When connecting to the serial console, you must use an RSA key. You can use the same SSH key for the serial console that was used when you launched the instance, or you can use a different SSH key.

When you are finished with the serial console and have terminated the SSH connection, you should delete the serial console connection. If you do not disconnect from the session, Oracle Cloud Infrastructure terminates the serial console session after 24 hours and you must reauthenticate to connect again.

Connecting from Mac OS X and Linux Operating Systems

Use an SSH client to connect to the serial console. Mac OS X and most Linux distributions include the SSH client OpenSSH by default.

**To connect to the serial console for an instance using OpenSSH on Mac OS X or Linux**

1. On the instance details page in the Oracle Cloud Infrastructure Console, under Resources, click Console Connection.
2. Click the Actions icon (three dots), and then click Copy Serial Console Connection for Linux/Mac.
3. Paste the connection string into a terminal window on a Mac OS X or Linux system, and then press Enter to connect to the console.

If you are not using the default SSH key or ssh-agent, modify the serial console connection string to include the identity file flag, -i, to specify the private key portion for the SSH key to use, for example id_rsa. Specify this flag for both the SSH connection and the SSH ProxyCommand, as shown in the following line:

   `ssh -i /path/<ssh_key> -o ProxyCommand='ssh -i /path/<ssh_key> -W %h:%p -p 443...`

4. Press Enter again to activate the console. If the connection is active, a message appears in the console:

   **IMPORTANT:** Use a console connection to troubleshoot a malfunctioning instance.

5. In the Oracle Cloud Infrastructure Console, reboot your instance. If the instance is functional and the connection is active, the serial output appears in your console. If serial output does not appear in the console, the instance operating system is not booting.

Connecting from Windows Operating Systems

The steps to connect to the serial console from Windows Powershell are different from the steps for OpenSSH. The following steps do not work in the Windows terminal.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are connecting to the instance from a Windows client using PowerShell, plink.exe is required. plink.exe is the command link connection tool included with PuTTY. You can install PuTTY or install plink.exe separately. For more information, see Installing an SSH Client and a Command-line Shell (Windows) on page 814.</td>
</tr>
</tbody>
</table>

To connect to the serial console for an instance on Microsoft Windows

1. On the instance details page in the Oracle Cloud Infrastructure Console, under **Resources**, click **Console Connection**.
2. Click the Actions icon (three dots). Depending on which SSH client you are using, do one of the following:
   - If you are using Windows PowerShell, click **Copy Serial Console Connection for Windows**.
   - If you are using OpenSSH, click **Copy Serial Console Connection for Linux/Mac**.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The copied connection string for Windows contains the parameter -i specifying the location of the private key file. The default value for this parameter in the connection string references an environment variable which might not be configured on your Windows client, or it might not represent the location where the private key file is saved. Verify the value specified for the -i parameter and make any required changes before proceeding to the next step.</td>
</tr>
</tbody>
</table>

3. Paste the connection string copied from the previous step into a text file so that you can add the file path to the private key file.
4. In the text file, replace `$env:homedrive$env:homepath\oci\console.ppk` with the file path to the `.ppk` file on your computer. This file path appears twice in the string. Replace it in both locations.
5. Paste the modified connection string into the PowerShell window or your OpenSSH client, and then press Enter to connect to the console.
6. Press Enter again to activate the console.
7. In the Oracle Cloud Infrastructure Console, reboot your instance. If the instance is functional and the connection is active, the serial output appears in your client. If serial output does not appear in the client, the instance operating system is not booting.
Connecting from Cloud Shell

If you encounter issues when connecting to your instance's serial console using the steps for connection from Mac OS X, Linux, or Windows, test connecting to the serial console using Cloud Shell. Cloud Shell is a web browser-based terminal accessible from the Console, see Cloud Shell for more information. This procedure includes steps to access Cloud Shell. For an introductory walkthrough of using Cloud Shell, see Using Cloud Shell.

Note:

You cannot use Cloud Shell for VNC console connections. You can only use it for serial console connections.

To connect to the serial console for an instance using Cloud Shell

1. Sign in to the Console.
2. Click the Cloud Shell icon in the Console header as shown in the following screenshot:

This action displays the Cloud Shell in a "drawer" at the bottom of the console as shown in the following screenshot:
Welcome to Oracle Cloud Shell.

Your Cloud Shell machine comes with 5GB of storage for your home directory.

john_doe@cloudshell:~ (us-ashburn-1)$
3. Run the following command in Cloud Shell to generate an SSH key pair:

```
ssh-keygen -t rsa
```

4. At the prompt to enter the file in which to save the key, press **Enter** to use the default location.

5. At the passphrase prompt, press **Enter** for no passphrase, and then press **Enter** again to confirm.

6. Run the following command to display the public key, and then copy the output:

```
cat $HOME/.ssh/id_rsa.pub
```

7. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.

8. Click the instance that you're interested in.

9. Under **Resources**, click **Console Connection**.

10. Click **Create Console Connection**.

11. Select **Paste SSH Key** and paste the public key contents you copied in step 6.

12. Click **Create Console Connection**.

After the console connection state changes to **Active** proceed to the next step.

13. Click the Actions icon (three dots), and then click **Copy Serial Console Connection for Linux/Mac**.

14. Paste the connection string copied from the previous step to Cloud Shell, and then press **Enter** to connect to the console.

15. Press **Enter** again to activate the console.

### Connecting to the VNC Console

After you create the console connection for the instance, you need to set up a secure tunnel to the VNC server on the instance, and then you can connect with a VNC client.

**Caution:**

The VNC console connection uses SSH port forwarding to create a secure connection from your local system to the VNC server attached to your instance's console. Although this method is a secure way to use VNC over the internet, owners of multiuser systems should know that opening a port on the local system makes it available to all users on that system until a VNC client connects. For this reason, we don't recommend using this product on a multiuser system unless you take proper actions to secure the port or you isolate the VNC client by running it in a virtual environment, such as Oracle VM VirtualBox.

To set up a secure tunnel to the VNC server on the instance using OpenSSH on Mac OS X or Linux

1. On the instance details page in the Oracle Cloud Infrastructure Console, under **Resources**, click **Console Connection**.

2. Click the Actions icon (three dots), and then click **Copy VNC Connection for Linux/Mac**.

3. Paste the connection string copied from the previous step to a terminal window on a Mac OS X or Linux system, and then press **Enter** to set up the secure connection.

4. After the connection is established, open your VNC client and specify **localhost** as the host to connect to and **5900** as the port to use.

**Note:**

Mac OS X Screen Sharing.app Not Compatible with VNC Console Connections

The Mac OS X built-in VNC client, Screen Sharing.app does not work with VNC console connections in Oracle Cloud Infrastructure. Use another VNC client, such as Real VNC Viewer or Chicken.

To set up a secure tunnel to the VNC server on the instance using PowerShell on Windows
Important:

If you are connecting to the VNC server on the instance from a Windows
client using PowerShell, plink.exe is required. plink.exe is the command
link connection tool included with PuTTY. You can install PuTTY or install
plink.exe separately. For installation information, see http://www.putty.org.

1. On the instance details page in the Oracle Cloud Infrastructure Console, under Resources, click Console
Connection.
2. Click the Actions icon (three dots), and then click Copy VNC Connection for Windows.

Tip:

The copied connection string for Windows contains the parameter –i
specifying the location of the private key file. The default value for this
parameter in the connection string references an environment variable
which might not be configured on your Windows client, or it might not
represent the location where the private key file is saved. Verify the value
specified for the –i parameter and make any required changes before
proceeding to the next step.

3. Paste the connection string copied from the previous step to Windows Powershell, and then press Enter to set up
the secure connection.
4. After the connection is established, open your VNC client and specify localhost as the host to connect to and
5900 as the port to use.

Note:

Secure Connection Warning

When you connect, you might see a warning from the VNC client that the
connection is not encrypted. Because you are connecting through SSH, the
connection is secure, so this warning is not an issue.

Troubleshooting Instances from Instance Console Connections on Linux

The following tasks describe steps specific to instances running Oracle Autonomous Linux 7.x, Oracle Linux 8.x,
and Oracle Linux 7.x, connecting from OpenSSH. Other operating system versions and SSH clients might require
different steps.

After you are connected with an instance console connection, you can perform various tasks, such as:

• Edit system configuration files.
• Add or reset the SSH keys for the opc user.
• Reset the password for the opc user.

These tasks require you to boot into a bash shell in maintenance mode.

To boot into maintenance mode

1. Reboot the instance from the Console.
2. When the reboot process starts, switch back to the terminal window, and you see Console messages start to appear
in the window. As soon as the GRUB boot menu appears, use the up/down arrow key to stop the automatic boot
process, enabling you to use the boot menu.
3. In the boot menu, highlight the top item in the menu, and press e to edit the boot entry.
4. In edit mode, use the down arrow key to scroll down through the entries until you reach the line that starts with
linuxefi for instances running Oracle Autonomous Linux 7.x, Oracle Linux 8.x, and Oracle Linux 7.x.
5. At the end of that line, add the following:

```
init=/bin/bash
```
6. Reboot the instance from the terminal window by entering the keyboard shortcut CTRL+X.
When the instance has rebooted, you see the Bash shell command line prompt, and you can proceed with the following procedures.

**To edit the system configuration files**

1. From the Bash shell, run the following command to load the SELinux policies to preserve the context of the files you are modifying:

   ```bash
   /usr/sbin/load_policy -i
   ```

2. Run the following command to remount the root partition with read/write permissions:

   ```bash
   /bin/mount -o remount, rw /
   ```

3. Edit the configuration files as needed to try to recover the instance.

4. After you have finished editing the configuration files, to start the instance from the existing shell, run the following command:

   ```bash
   exec /usr/lib/systemd/systemd
   ```

   Alternatively, to reboot the instance, run the following command:

   ```bash
   /usr/sbin/reboot -f
   ```

**To add or reset the SSH key for the opc user**

1. From the Bash shell, run the following command to load the SELinux policies to preserve the context of the files you are modifying:

   ```bash
   /usr/sbin/load_policy -i
   ```

2. Run the following command to remount the root partition with read/write permissions:

   ```bash
   /bin/mount -o remount, rw /
   ```

3. From the Bash shell, run the following command to change to the SSH key directory for the opc user:

   ```bash
   cd ~opc/.ssh
   ```

4. Rename the existing authorized keys file with the following command:

   ```bash
   mv authorized_keys authorized_keys.old
   ```

5. Replace the contents of the public key file with the new public key file with the following command:

   ```bash
   echo '<contents of public key file>' >> authorized_keys
   ```

6. Restart the instance by running the following command:

   ```bash
   /usr/sbin/reboot -f
   ```

**To reset the password for the opc user**

1. From the Bash shell, run the following command to load the SELinux policies to preserve the context of the files you are modifying. This step is necessary to sign in to your instance using SSH and the Console.

   ```bash
   /usr/sbin/load_policy -i
   ```

2. Run the following command to remount the root partition with read/write permissions:

   ```bash
   /bin/mount -o remount, rw /
   ```
3. Run the following command to reset the password for the opc user:

```
sudo passwd opc
```

4. Restart the instance by running the following command:

```
sudo reboot -f
```

### Exiting the Instance Console Connection

#### To exit the serial console connection

When using SSH, the ~ character at the beginning of a new line is used as an escape character.

- To exit the serial console, enter:

```
~.
```

- To suspend the SSH session, enter:

```
~^z
```

The ^ character represents the CTRL key.

- To see all the SSH escape commands, enter:

```
~?
```

#### To exit the VNC console connection

1. Close the VNC client.
2. In the Terminal or PowerShell window, type `CTRL C`

When you are finished using the console connection, delete the connection for the instance.

#### To delete the console connection for an instance

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you’re interested in.
3. Under Resources, click Console Connection.
4. Click the Actions icon (three dots), and then click Delete. Confirm when prompted.

### Tagging Resources

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

#### To manage tags for an instance console connection

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance that you’re interested in.
3. Under Resources, click Console Connection.
4. For the console connection that you’re interested in, click the Actions icon (three dots) and then click Add Tags.
   To view existing tags, click View Tags.

### Sending a Diagnostic Interrupt

**Caution:**

This feature is for advanced users. Sending a diagnostic interrupt to a live system can cause data corruption or system failure.

You can send a diagnostic interrupt to debug an unresponsive or unreachable compute virtual machine (VM) instance.
A diagnostic interrupt causes the instance's OS to crash and reboot. Before you send a diagnostic interrupt, you must configure the OS to generate a crash dump (also called a memory dump file) when it crashes. The crash dump captures information about the state of the OS at the time of the crash. After the OS restarts, you can analyze the crash dump to identify and debug the issue.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users launch compute instances on page 2143 includes the ability to send a diagnostic interrupt to an instance. If the specified group doesn't need to launch instances or attach volumes, you could simplify that policy to include only manage instance-family, and remove the statements involving volume-family and virtual-network-family.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For reference material about writing policies for instances, cloud networks, or other Core Services API resources, see Details for the Core Services on page 2181.

**Prerequisites**

- The instance's OS must be configured to generate a crash dump file.
- The instance must be in the Running state. For more information, see Stopping and Starting an Instance on page 779.
- There are no in-progress actions affecting the instance, such as block volumes or secondary VNICs in the process of being attached or detached.

**Configuring the OS to Generate a Crash Dump**

Before you send a diagnostic interrupt to an instance, you must configure the OS to generate a crash dump when it crashes. The diagnostic interrupt is received as a non-maskable interrupt (NMI) on the target instance.

The steps depend on the OS.

**Linux**

**Note:**

On Oracle-provided images for Oracle Linux, the OS is either fully configured or partially configured to generate a crash dump, depending on the image release date.

**Oracle Linux 8**

- **Images released in August 2020 or later:** The image is fully configured to generate a crash dump.
- **Earlier images:** The dump-capture kernel is installed and configured, but you must perform the other configuration steps.

**Oracle Linux 7**

- **Images released in August 2020 or later:** The image is fully configured to generate a crash dump.
- **Earlier images:** The dump-capture kernel is installed and configured, but you must perform the other configuration steps.

**Oracle Linux 6**

- **Images released in September 2020 or later:** The image is fully configured to generate a crash dump.
Earlier images: The dump-capture kernel is installed and configured, but you must perform the other configuration steps.

1. Connect to the instance.
2. Install and configure the dump-capture kernel:
   a. Install kdump and kexec by running the following command:
      
      ```bash
      sudo yum install kexec-tools
      ```
   b. Reserve memory on the kernel to save the crash dump. Do the following:
      1. Open the `etc/default/grub` file in a text editor.
      2. In the line that starts with `GRUB_CMDLINE_LINUX_DEFAULT`, add the parameter `crashkernel=<memory-to-reserve>`. For example, to reserve 100 MB, add `crashkernel=100M`.
      3. Save the changes and close the file.
      4. Rebuild the GRUB file by running the following command:
         ```bash
         sudo grub2-mkconfig -o /boot/grub2/grub.cfg
         ```
   3. Configure the kernel to crash when it receives a diagnostic interrupt. To do this, open the `/etc/sysctl.conf` file in a text editor and add the following line:
      ```
      kernel.unknown_nmi_panic=1
      ```
   4. Apply the change to `/etc/sysctl.conf` by running the following command:
      ```bash
      sysctl -p
      ```

Windows Server - Oracle-Provided Image

If you use an Oracle-provided image for Windows Server that was released in April 2020 or later, the image is already configured to generate a crash dump.

If you use an image that was released before April 2020, do the following:

1. Connect to the instance.
2. Download the Oracle Windows VirtIO drivers:
   a. Sign in to the Oracle Software Delivery Cloud site.
   b. In the All Categories list, select Release.
   c. Type Oracle Linux 7.7 in the search box and click Search.
   d. Add REL: Oracle Linux 7.7.x to your cart, and then click Continue.
   e. In the Platforms/Languages list, select x86 64 bit. Click Continue.
   f. Accept the license agreement and then click Continue.
   g. Select the check box next to Oracle VirtIO Drivers Version for Microsoft Windows 1.1.5. Clear the other check boxes.
   h. Click Download and then follow the prompts.
3. Install the drivers and then restart the instance. For steps, see Installing the Oracle VirtIO Drivers for Microsoft Windows on Existing Microsoft Windows Guests.

Windows Server - Customer-Provided Image

Refer to the third-party documentation for your operating system for more information.

Sending a Diagnostic Interrupt

After you configure the instance's OS to generate a crash dump when it crashes, use the following procedures to send a diagnostic interrupt.
To send a diagnostic interrupt using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click More Actions, and then click Send Diagnostic Interrupt.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending a diagnostic interrupt to a live system can cause data corruption or system failure.</td>
</tr>
</tbody>
</table>

3. Review the confirmation message and then click Send Diagnostic Interrupt.

   The lifecycle state that appears in the Console remains Running while the instance's OS crashes and restarts. Do not send multiple diagnostic interrupts.

4. Wait several minutes for the instance's OS to restart, and then connect to the instance. You can now retrieve and analyze the crash dump.

To send a diagnostic interrupt using the API

Use the InstanceAction operation, passing the value SENDDIAGNOSTICINTERRUPT as the action to perform.

Analyzing a Crash Dump

The crash dump is saved locally on the instance's OS.

- **Linux instances**: The default location where the crash dump is saved depends on the Linux distribution.
  - Oracle Linux 8, Oracle Linux 7: saved in /var/oled/crash
  - Other Linux distributions: saved in /var/crash/

To change the location, modify the /etc/kdump.conf file.

- **Windows instances**: The crash dump is saved in %SystemRoot%memory.dmp. On most Windows systems, this is C:\Windows\memory.dmp.

To analyze the crash dump, use a third-party tool such as the crash utility on Linux instances or WinDbg on Windows instances.

Updating the Linux iSCSI Service to Restart Automatically

Oracle Cloud Infrastructure supports iSCSI attached remote boot and block volumes to Compute instances. These iSCSI attached volumes are managed by the Linux iSCSI initiator service, iscsid. In scenarios where this service is stopped for any reason, such as the service crashes or a system administrator inadvertently stops the service, it's important that this service is automatically restarted immediately.

The following platform images distributed by Oracle Cloud Infrastructure are configured so that the iscsid service restarts automatically:

- Oracle Autonomous Linux 7 images.
- Oracle Linux 8 images.
- Oracle Linux 7 images released February 26, 2019 and later. See the release notes for Oracle-Linux-7.6-Gen2-GPU-2019.02.20-0 and Oracle-Linux-7.6-2019.02.20-0.
- Oracle Linux 6 images released February 26, 2019 and later. See the release notes for Oracle-Linux-6.10-2019.02.22-0.
- CentOS 7 images released February 25, 2019 and later. See the release notes for CentOS-7-2019.02.23-0.

Instances created from earlier versions of CentOS 7.x and Oracle Linux platform images, or any versions of Ubuntu platform images, do not have this configuration. You should update these existing instances and custom images created from these images so that the iscsid service restarts automatically. You should also check this configuration on your imported paravirtualized custom images and any instances launched from these images and update the configuration as needed.

This topic describes how to update the iscsid service on an instance so that it will restart automatically.
**Note:**

Configuring an instance to automatically restart the `iscsid` service does not require a reboot and will increase the stability of your infrastructure.

**Oracle Linux 7**

Run the following command to update the `iscsid` service on your Oracle 7 Linux instances:

```
sudo yum update -y iscsi-initiator-utils
```

After running this command, the version of the `iscsid` service should be 6.2.0.874 or newer.

Run the following command to check the version:

```
yum info iscsi-initiator-utils
```

This update does not require a system reboot and will not make any changes to your instances beyond configuring `iscsid` to restart automatically.

**Oracle Linux 6**

Run the following command to update the `iscsid` service on your Oracle 6 Linux instances:

```
sudo yum update -y iscsi-initiator-utils
```

After running this command, the version of the `iscsid` service should be 6.2.0.873 or newer.

Run the following command to check the version:

```
yum info iscsi-initiator-utils
```

This update does not require a system reboot and will not make any changes to your instances beyond configuring `iscsid` to restart automatically.

**CentOS 7.x**

**Important:**

Do not directly edit the `systemd iscsid.service` file. You should instead create an override to ensure that the `restart` option isn't overwritten the next time the `iscsid` service is updated.

On your CentOS 7 instances run the following command to create an override file:

```
sudo systemctl edit iscsid.service
```

Paste and save the following into the file:

```
[Service]
Restart=always
```

Run the following commands to reload `systemd` and restart the `iscsid` service:

```
sudo systemctl daemon-reload
sudo systemctl restart iscsid
```
Ubuntu 18

Important:
Do not directly edit the systemctl iscsid.service file, instead create an override to ensure that the restart option isn't overwritten the next time the iscsid service is updated.

On your Ubuntu 18 instances run the following command to create an override file:

```
sudo systemctl edit iscsid.service
```

Paste and save the following into the file:

```
[Service]
Restart=
Restart=always
```

Run the following commands to reload systemd and restart the iscsid service:

```
sudo systemctl daemon-reload
sudo systemctl restart iscsid
```

Ubuntu 16

Important:
Do not directly edit the systemctl iscsid.service file, instead create an override to ensure that the restart option isn't overwritten the next time the iscsid service is updated.

On your Ubuntu 16 instances run the following command to create an override file:

```
sudo systemctl edit iscsid.service
```

Paste and save the following into the file:

```
[Service]
Restart=
Restart=always
```

Run the following commands to reload systemd and restart the iscsid service:

```
sudo systemctl daemon-reload
sudo systemctl restart iscsid
```

Ubuntu 14

On your Ubuntu 14 instances run the following command to install the monit package:

```
sudo apt-get install monit
```

Create the `/etc/monit/conf.d/iscsid.conf` file and include the following commands:

```
check process iscid with pidfile /run/iscsid.pid
start program = "/etc/init.d/open-iscsi start" with timeout 60 seconds
stop program = "/etc/init.d/open-iscsi stop"
```
Run the following command to start the `monit` service:

```
/etc/init.d/monit start
```

**Testing the iscsid Service Update**

Perform these steps to verify that the `iscsid` service has been updated successfully, and that it restarts automatically.

```
1. Run the following command to confirm that the `iscsid` service is running:
   `ps -ef | grep iscsid`

2. Run the following command to stop the `iscsid` service:
   `sudo pkill -9 iscsid`

3. Wait 60 seconds and then run the following command to verify that the `iscsid` service has restarted:
   `ps -ef | grep iscsid`
```

**Windows Generalized Image Support Files**

To generalize a Windows custom image, download the appropriate file for your instance based on the shape of the instance. Then, follow the instructions in Creating Windows Custom Images on page 668.

The files apply to the following Windows versions:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

**VM Instances**

Use this download for all VM instances.

Download: `oracle-cloud_windows-server_generalize_2019-02-06.SED.EXE`

**Bare Metal Instances - AMD Shapes**

Use this download for AMD-based bare metal instances.

Download: `oracle-cloud_windows-server-bm-gen2_generalize_2019-01-31.SED.EXE`

**Bare Metal Instances - X7 Shapes**

Use this download for X7-based bare metal instances.

Download: `oracle-cloud_windows-server-bm-gen2_generalize_2019-01-31.SED.EXE`

**Bare Metal Instances - X5 Shapes**

Use this download for X5-based bare metal instances.

Download: `oracle-cloud_windows-server_generalize_2019-02-06.SED.EXE`
Chapter 12

Container Engine for Kubernetes

This chapter explains how to define and create Kubernetes clusters to enable the deployment, scaling, and management of containerized applications.

Overview of Container Engine for Kubernetes

Oracle Cloud Infrastructure Container Engine for Kubernetes is a fully-managed, scalable, and highly available service that you can use to deploy your containerized applications to the cloud. Use Container Engine for Kubernetes (sometimes abbreviated to just OKE) when your development team wants to reliably build, deploy, and manage cloud-native applications. You specify the compute resources that your applications require, and Container Engine for Kubernetes provisions them on Oracle Cloud Infrastructure in an existing OCI tenancy.

Container Engine for Kubernetes uses Kubernetes - the open-source system for automating deployment, scaling, and management of containerized applications across clusters of hosts. Kubernetes groups the containers that make up an application into logical units (called pods) for easy management and discovery. Container Engine for Kubernetes uses versions of Kubernetes certified as conformant by the Cloud Native Computing Foundation (CNCF). Container Engine for Kubernetes is itself ISO-compliant (ISO-IEC 27001, 27017, 27018).

You can access Container Engine for Kubernetes to define and create Kubernetes clusters using the Console and the REST API. You can access the clusters you create using the Kubernetes command line (kubectl), the Kubernetes Dashboard, and the Kubernetes API.

Container Engine for Kubernetes is integrated with Oracle Cloud Infrastructure Identity and Access Management (IAM), which provides easy authentication with native Oracle Cloud Infrastructure identity functionality.

For an introductory tutorial, see Creating a Cluster with Oracle Cloud Infrastructure Container Engine for Kubernetes. A number of related Developer Tutorials are also available.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

Creating Automation with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.
Container Engine for Kubernetes

See Container Engine for Kubernetes on page 1842 for details about Container Engine for Kubernetes resources that emit events.

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you're a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Note that to perform certain operations on clusters created by Container Engine for Kubernetes, you might require additional permissions granted via a Kubernetes RBAC role or clusterrole. See About Access Control and Container Engine for Kubernetes on page 920.

Container Engine for Kubernetes Capabilities and Limits

In each region that is enabled for your tenancy, you can create three clusters (Monthly Universal Credits) or one cluster (Pay-as-You-Go or Promo) by default. Each cluster you create can have a maximum of 1000 nodes. A maximum of 110 pods can run on each node. See Service Limits on page 215.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies.

For more details about policies for Container Engine for Kubernetes, see:

• Policy Configuration for Cluster Creation and Deployment on page 868
• Details for Container Engine for Kubernetes on page 2177

Container Engine and Kubernetes Concepts

Clusters and Nodes

A Kubernetes cluster is a group of nodes. The nodes are the machines running applications. Each node can be a physical machine or a virtual machine. The node's capacity (its number of CPUs and amount of memory) is defined when the node is created. A cluster comprises:

• One or more control plane nodes (previously referred to as 'master nodes'). For high availability, typically there will be a number of control plane nodes.
• One or more worker nodes (sometimes known as 'minions').
A Kubernetes cluster can be organized into namespaces, to divide the cluster's resources between multiple users. Initially, a cluster has the following namespaces:

- **default**, for resources with no other namespace
- **kube-system**, for resources created by the Kubernetes system
- **kube-node-lease**, for one lease object per node to help determine node availability
- **kube-public**, usually used for resources that have to be accessible across the cluster

### Kubernetes Processes

The control plane nodes in a cluster run a number of processes:

- **kube-apiserver** to support API operations via the Kubernetes command line tool (kubectl) and the REST API, and includes admissions controllers required for advanced Kubernetes operations
- **kube-controller-manager** to manage different Kubernetes components (for example, replication controller, endpoints controller, namespace controller, and serviceaccounts controller)
- **kube-scheduler** to control where in the cluster to run jobs
- **etcd** to store the cluster's configuration data

Each worker node runs two Kubernetes processes:

- **kubelet** to communicate with the control plane nodes
- **kube-proxy** to handle networking

Each worker node also runs the Docker runtime.

The Kubernetes processes running on the control plane nodes are collectively referred to as the Kubernetes Control Plane. Together, the Control Plane processes monitor and record the state of the cluster and distribute requested operations between the nodes in the cluster.

### Pods

Where an application running on a worker node comprises multiple containers, Kubernetes groups the containers into a single logical unit called a pod for easy management and discovery. The containers in the pod share the same networking namespace and the same storage space, and can be managed as a single object by the Kubernetes Control Plane. A number of pods providing the same functionality can be grouped into a single logical set known as a service.

### Manifest Files (or Pod Specs)

A Kubernetes manifest file comprises instructions in a yaml or json file that specify how to deploy an application to the node or nodes in a Kubernetes cluster. The instructions include information about the Kubernetes deployment, the Kubernetes service, and other Kubernetes objects to be created on the cluster. The manifest is commonly also referred to as a pod spec, or as a deployment.yaml file (although other filenames are allowed). The parameters to include in a Kubernetes manifest file are described in the Kubernetes documentation.

### Node Pools

A node pool is a subset of machines within a cluster that all have the same configuration. Node pools enable you to create pools of machines within a cluster that have different configurations. For example, you might create one pool of nodes in a cluster as virtual machines, and another pool of nodes as bare metal machines. A cluster must have a minimum of one node pool, but a node pool need not contain any worker nodes.

### Admission Controllers

A Kubernetes admission controller intercepts authenticated and authorized requests to the Kubernetes API server before admitting an object (such as a pod) to the cluster. An admission controller can validate an object, or modify it, or both. Many advanced features in Kubernetes require an enabled admission controller. For more information, see the Kubernetes documentation.
Preparing for Container Engine for Kubernetes

Before you can use Container Engine for Kubernetes to create a Kubernetes cluster:

- You must have access to an Oracle Cloud Infrastructure tenancy. The tenancy must be subscribed to one or more of the regions in which Container Engine for Kubernetes is available (see Availability by Region on page 836).
- Your tenancy must have sufficient quota on different types of resource (see Service Limits on page 215). More specifically:
  - Compute instance quota: To create a Kubernetes cluster, at least one compute instance (node) must be available in the tenancy. However, you'll probably want more than this minimum. For example, to create a highly available cluster in a region with three availability domains (ADs), at least three compute instances must be available (one in each availability domain).
  - Block volume quota: If you intend to create Kubernetes persistent volumes, sufficient block volume quota must be available in each availability domain to meet the persistent volume claim. Persistent volume claims must request a minimum of 50 gigabytes. See Creating a Persistent Volume Claim on page 947.
  - Load balancer quota: If you intend to create a load balancer to distribute traffic between the nodes running a service in a Kubernetes cluster, sufficient load balancer quota must be available in the region. See Creating Load Balancers to Distribute Traffic Between Cluster Nodes on page 937.
- Within your tenancy, there must already be a compartment to contain the necessary network resources (such as a VCN, subnets, internet gateway, route table, security lists). If such a compartment does not exist already, you will have to create it. Note that the network resources can reside in the root compartment. However, if you expect multiple teams to create clusters, best practice is to create a separate compartment for each team.
- Within the compartment, network resources (such as a VCN, subnets, internet gateway, route table, security lists) must be appropriately configured in each region in which you want to create and deploy clusters. For example, to create a highly available cluster in a region with three availability domains, the VCN must include:
  - For worker nodes: a regional subnet (recommended), or three AD-specific subnets (one in each of the availability domains).
  - For load balancers: optionally (but usually) an additional regional subnet (recommended), or an additional two AD-specific subnets (each in a different availability domain).

Best practice is to use regional subnets to make failover across availability domains simpler to implement.

When creating a new cluster, you can have Container Engine for Kubernetes automatically create and configure new network resources for the new cluster, or you can specify existing network resources. If you specify existing network resources, you or somebody else must have already configured those resources appropriately. See Network Resource Configuration for Cluster Creation and Deployment on page 836.

- To create and/or manage clusters, you must belong to one of the following:
  - The tenancy's Administrators group
  - A group to which a policy grants the appropriate Container Engine for Kubernetes permissions. If you are creating or modifying clusters using the Console, or want Container Engine for Kubernetes to automatically
create and configure new network resources for a new cluster, policies must also grant the group the following permissions:

- VCN_READ and VCN_CREATE
- SUBNET_READ and SUBNET_CREATE
- COMPARTMENT_INSPECT
- INTERNET_GATEWAY_CREATE
- NAT_GATEWAY_CREATE
- ROUTE_TABLE_UPDATE
- SECURITY_LIST_CREATE

If you want to create a service gateway to enable applications deployed on a cluster to pull images from Oracle Cloud Infrastructure Registry (or to use other Oracle Cloud Infrastructure resources) without exposing data to the public internet, a policy must also grant the group the SERVICE_GATEWAY_CREATE permission.

See Create Required Policy for Groups on page 868.

- To perform operations on a cluster:
  - You must be able to run the Kubernetes command line tool kubectl. You can use the kubectl installation included in Cloud Shell, or you can use a local installation of kubectl (see Accessing a Cluster Using Kubectl on page 890).
  - You must have set up your own copy of the cluster's kubeconfig configuration file (see Setting Up Cluster Access on page 876). Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up.
  - You must have appropriate permissions to access the cluster (see About Access Control and Container Engine for Kubernetes on page 920).

**Availability by Region**

Container Engine for Kubernetes is available in all the Oracle Cloud Infrastructure regions listed at Regions and Availability Domains on page 180. Refer to that topic to see region identifiers, region keys, and availability domain names.

In some cases, you might have to use shortened versions of availability domain names. For example, when defining a persistent volume claim (PVC), to request storage in a particular availability domain by specifying the value of the failure-domain.beta.kubernetes.io/zone Kubernetes label. To find out how to construct shortened versions of availability domain names, see failure-domain.beta.kubernetes.io/zone on page 899.

**Network Resource Configuration for Cluster Creation and Deployment**

Before you can use Container Engine for Kubernetes to create and deploy clusters in the regions in a tenancy:

- Within the tenancy, there must already be a compartment to contain the necessary network resources (such as a VCN, subnets, internet gateway, route table, security lists). If such a compartment does not exist already, you will have to create it. Note that the network resources can reside in the root compartment. However, if you expect multiple teams to create clusters, best practice is to create a separate compartment for each team.
- Within the compartment, network resources (such as a VCN, subnets, internet gateway, route table, security lists) must be appropriately configured in each region in which you want to create and deploy clusters. When creating a new cluster, you can have Container Engine for Kubernetes automatically create and configure new network resources for a new ‘quick cluster’. Alternatively, you can explicitly specify the existing network resources to use for a ‘custom cluster’. If you specify existing network resources, you or somebody else must have already configured those resources appropriately, as described in this topic.

This topic describes the necessary configuration for each network resource. To see details of a typical configuration, see Example Network Resource Configurations on page 840.

For an introductory tutorial, see Creating a Cluster with Oracle Cloud Infrastructure Container Engine for Kubernetes. A number of related Developer Tutorials are also available.
**VCN Configuration**

The VCN in which you want to create and deploy clusters must be configured as follows:

- The VCN must have a CIDR block defined that is large enough for the number of subnets you specify for the clusters you create. For example, to create a highly available cluster in a region with three availability domains will typically require two regional subnets (recommended) or five AD-specific subnets to support the necessary number of worker nodes and load balancers. However, you can create clusters with fewer subnets. A /16 CIDR block would be large enough for almost all use cases (10.0.0.0/16 for example). The CIDR block you specify for the VCN must not overlap with the CIDR block you specify for pods and for the Kubernetes services (see **CIDR Blocks and Container Engine for Kubernetes** on page 867).

- The VCN must have an appropriate number of subnets defined. For example, to create a highly available cluster in a region with three availability domains, the VCN must include:
  - For worker nodes: a regional subnet (recommended), or three AD-specific subnets (one in each of the availability domains).
  - For load balancers: optionally (but usually) an additional regional subnet (recommended), or an additional two AD-specific subnets (each in a different availability domain).

However, you can create clusters with fewer worker nodes, and fewer or no load balancers, and therefore require fewer subnets. Best practice is to use regional subnets to make failover across availability domains simpler to implement. See **Subnet Configuration** on page 839.

- The VCN must have security lists defined for worker node subnets and load balancer subnets (if specified). See **Security List Configuration** on page 838.

In addition:

- Oracle recommends DNS Resolution is selected for the VCN.

- If you expect applications deployed on a cluster to require worker nodes to initiate connections to the internet, the VCN must have an internet gateway (if the worker nodes are in public subnets) or a NAT gateway (if the worker nodes are in private subnets). See **Internet Gateway Configuration** on page 837 and **NAT Gateway Configuration** on page 837.

- If you expect applications deployed on a cluster to pull images from Oracle Cloud Infrastructure Registry (or to use other Oracle Cloud Infrastructure resources) and you don't want to expose the data to the public internet, you can define a service gateway in the VCN. See **Service Gateway Configuration** on page 837.

- If the VCN has a NAT gateway, an internet gateway, or a service gateway, it must have a route table with appropriate rules defined. See **Route Table Configuration** on page 838.

See **VCNs and Subnets** on page 2821 and **Example Network Resource Configurations** on page 840.

**Internet Gateway Configuration**

If you intend to deploy worker nodes in public subnets, and you expect deployed applications to require the worker nodes to initiate connections to the internet, the VCN must have an internet gateway. The internet gateway must be specified as the target for the destination CIDR block 0.0.0.0/0 in a route rule in a worker node route table.

See **VCNs and Subnets** on page 2821 and **Example Network Resource Configurations** on page 840.

**NAT Gateway Configuration**

If you intend to deploy worker nodes in private subnets, and you expect deployed applications to require the worker nodes to initiate connections to the internet, the VCN must have a NAT gateway. The NAT gateway must be specified as the target for the destination CIDR block 0.0.0.0/0 in a route rule in a worker node route table.

See **NAT Gateway** on page 3247 and **Example Network Resource Configurations** on page 840.

**Service Gateway Configuration**

If you expect applications deployed on a cluster to pull images from Oracle Cloud Infrastructure Registry (or to use other Oracle Cloud Infrastructure resources) and you want to protect data from the public internet, you can set up a service gateway. Setting up a service gateway enables worker nodes to access other resources in the same region without exposing data to the public internet.
When setting up the service gateway, create it in the same VCN and compartment as the worker nodes, and select the **All <region> Services in Oracle Services Network** option.

Having created the service gateway, it must be specified as the target for **All <region> Services in Oracle Services Network** in a route rule in the worker node route table.

Note that if you expect deployed applications to require access to public endpoints or services not supported by a service gateway (for example, to download updates or patches), configure additional network resources (such as a NAT gateway) to access the internet.


### Route Table Configuration

If you intend to deploy worker nodes in public subnets, and you expect deployed applications to require the worker nodes to initiate connections to the internet, create an internet gateway. Then create a worker node route table with a route rule that specifies the internet gateway as the target for the destination CIDR block 0.0.0.0/0.

If you intend to deploy worker nodes in private subnets, and you expect deployed applications to require the worker nodes to initiate connections to the internet, create a NAT gateway. Then create a worker node route table with a route rule that specifies the NAT gateway as the target for the destination CIDR block 0.0.0.0/0.

If you expect applications deployed on a cluster to pull images from Oracle Cloud Infrastructure Registry (or to use other Oracle Cloud Infrastructure resources) and you don't want to expose the data to the public internet, create a service gateway. Then create a worker node route table with a route rule that specifies the service gateway as the target for **All <region> Services in Oracle Services Network**.

Note that to avoid the possibility of asymmetric routing, a route table for a public subnet cannot contain both a route rule that targets an internet gateway as well as a route rule that targets a service gateway (for more information, see [Issues with access from Oracle services through a service gateway to your public instances](https://docs.oracle.com/en-us/oracle-cloud/instances-cloud-infrastructure/1.1.0/oracle-cloud-infrastructure-user-guide/content/issue-with-access-from-oracle-services-through-service-gateway-to-your-public-instances.html)).


### DHCP Options Configuration

The VCN in which you want to create and deploy clusters must have DHCP Options configured. The default value for **DNS Type** of Internet and VCN Resolver is acceptable.


### Security List Configuration

The VCN in which you want to create and deploy clusters must have security lists defined for worker node subnets and load balancer subnets (if specified). The security lists for worker node subnets and load balancer subnets must be different. The security list for load balancer subnets must be unique and for their exclusive use.

Worker nodes are created with public or private IP addresses, according to whether you specify public or private subnets when defining the node pools in a cluster. Container Engine for Kubernetes must be able to access worker nodes.


### Public Worker Node Subnet Security List Configuration

When configuring a security list for public worker node subnets, the security list must have:

- Stateless ingress and egress rules that allow all traffic between different worker node subnets. (Usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this not required.)
- Stateless ingress and egress rules that allow all traffic between worker node subnets and load balancer subnets (if specified).
- Stateful egress rules that allow traffic between worker node subnets and Container Engine for Kubernetes.
Optionally, you can include ingress rules for public worker node subnets to:

- Explicitly allow SSH access to worker nodes on port 22 (see Connecting to Worker Nodes in Public Subnets Using SSH on page 904).
- Allow inbound traffic to the worker nodes on the default NodePort range of 30000 to 32767 (see the Kubernetes documentation).

Optionally, you can include an egress rule that allows all outbound traffic to the internet.

**Private Worker Node Subnet Security List configuration**

When configuring a security list for private worker node subnets, the security list must have:

- Stateless ingress and egress rules that allow all traffic between the different worker node subnets. (Usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this not required.)
- Stateless ingress and egress rules that allow all traffic between worker node subnets and load balancer subnets.
- Stateful egress rules that allow traffic between worker node subnets and Container Engine for Kubernetes.

Optionally, you can include ingress rules for private worker node subnets to:

- Explicitly allow SSH access to worker nodes on port 22 from within the VCN CIDR block (see Connecting to Worker Nodes in Private Subnets Using SSH on page 905).
- Allow inbound traffic to the worker nodes on the default NodePort range of 30000 to 32767 from within the VCN CIDR block (see the Kubernetes documentation).

Optionally, you can include an egress rule that allows all outbound traffic to the internet.

**Subnet Configuration**

The characteristics of the cluster you want to create, and the number of availability domains in the region in which you want to deploy the cluster, will determine the number of subnets to configure. For example, to create a highly available cluster in a region with three availability domains will require:

- For worker nodes: a regional subnet (recommended), or three AD-specific subnets (one in each of the availability domains).
- For load balancers: optionally (but usually) an additional regional subnet (recommended), or an additional two AD-specific subnets (each in a different availability domain).

Best practice is to use regional subnets to make failover across availability domains simpler to implement.

The VCN in which you want to create and deploy clusters must have at least one subnet defined in which to deploy worker nodes. Worker node subnets can be either public, or private for additional security (as specified by the Subnet access property). The number of worker node subnets to create depends on the region in which you are creating the cluster:

- If you are creating a cluster in a region with multiple availability domains, you can define a single regional subnet (recommended), or multiple AD-specific subnets (one in each of the availability domains).
- If you are creating a cluster in a region with a single availability domain, you can define a single regional subnet (recommended), or a single AD-specific subnet.

You have the option to define and use load balancers in clusters you create. If you want to define and use load balancers, the VCN in which you want to create and deploy clusters must have at least one subnet defined to host the load balancers. Load balancer subnets can be public or private (as specified by the Subnet access property). However, load balancers are optional, so you might not define load balancer subnets at all. The number of load balancer subnets to define depends on the region in which you are creating the cluster:

- If you are creating a cluster in a region with three availability domains, you can define:
  - zero or one load balancer regional subnet (recommended)
  - zero or two load balancer AD-specific subnets. If you define two load balancer AD-specific subnets, they must be in different availability domains.
• If you are creating a cluster in a region with a single availability domain, you can define zero or one load balancer subnet:
  • zero or one load balancer regional subnet (recommended)
  • zero or one load balancer AD-specific subnet.

In addition, all subnets must have the following properties set as shown:
• Route Table: The name of a route table, if one has been created, that has a route rule specifying an internet gateway (for public worker node subnets) or NAT gateway (for private worker node subnets) as the target for the destination CIDR block 0.0.0.0/0, and/or a route rule specifying a service gateway as the target for all `<region>` Services in Oracle Services Network.
• DHCP options: Default.

The CIDR blocks you specify for worker node and load balancer subnets must not overlap with CIDR blocks you specify for pods running in the cluster (see CIDR Blocks and Container Engine for Kubernetes on page 867).

Worker node subnets must have different security lists to load balancer subnets.

See VCNs and Subnets on page 2821 and Example Network Resource Configurations on page 840.

Example Network Resource Configurations

Before you can use Container Engine for Kubernetes to create and deploy clusters in the regions in a tenancy:
• Within the tenancy, there must already be a compartment to contain the necessary network resources (such as a VCN, subnets, internet gateway, route table, security lists). If such a compartment does not exist already, you will have to create it. Note that the network resources can reside in the root compartment. However, if you expect multiple teams to create clusters, best practice is to create a separate compartment for each team.
• Within the compartment, network resources (such as a VCN, subnets, internet gateway, route table, security lists) must be appropriately configured in each region in which you want to create and deploy clusters. When creating a new cluster, you can have Container Engine for Kubernetes automatically create and configure new network resources for a new 'quick cluster'. Alternatively, you can explicitly specify the existing network resources to use for a 'custom cluster'. If you specify existing network resources, you or somebody else must have already configured those resources appropriately. See Network Resource Configuration for Cluster Creation and Deployment on page 836.

This topic gives examples of how you might configure network resources for highly available 'custom cluster' creation and deployment in a region with three availability domains:
• for public clusters, where you want worker nodes hosted in public AD-specific subnets that can be accessed directly from the internet (see Example 1: Example Network Resource Configuration for a Highly Available Public Cluster in a Region with Three Availability Domains, Using AD-Specific Subnets on page 841)
• for private clusters, where you want worker nodes hosted in private AD-specific subnets that can only be accessed from within the VCN (see Example 2: Example Network Resource Configuration for a Highly Available Private Cluster in a Region with Three Availability Domains, Using AD-Specific Subnets on page 852)
• for public clusters, where you want worker nodes hosted in a public regional subnet that can be accessed directly from the internet (see Example 3: Example Network Resource Configuration for a Highly Available Public Cluster in a Region with Three Availability Domains, Using a Regional Subnet on page 861)

Note that all the examples in this topic include a service gateway to enable worker nodes to access other Oracle Cloud Infrastructure resources in the same region (such as Oracle Cloud Infrastructure Registry) without exposing data to the public internet. However, you might be expecting applications deployed on the cluster to require access to public endpoints or services not supported by a service gateway. For example, to download updates or patches. If so, configure additional network resources (such as a NAT gateway) to access the internet.

For an introductory tutorial, see Creating a Cluster with Oracle Cloud Infrastructure Container Engine for Kubernetes. A number of related Developer Tutorials are also available.
Example 1: Example Network Resource Configuration for a Highly Available Public Cluster in a Region with Three Availability Domains, Using AD-Specific Subnets

This example assumes you want worker nodes hosted in three public AD-specific subnets that can be accessed directly from the internet.

### Example Network Resource Configuration

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCN</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> acme-dev-vcn</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block:</strong> 10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution:</strong> Selected</td>
</tr>
<tr>
<td>Internet Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> gateway-0</td>
</tr>
<tr>
<td>Service Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> service-gateway-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Services:</strong> All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
<tr>
<td>Route Table</td>
<td>Two route tables created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> routetable-0, with a route rule defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination CIDR block:</strong> 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type:</strong> Internet Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Internet Gateway:</strong> gateway-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> routetable-1, with a route rule defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination:</strong> All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type:</strong> Service Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target:</strong> service-gateway-0</td>
</tr>
</tbody>
</table>

Note that to avoid the possibility of asymmetric routing, a route table for a public subnet cannot contain both a route rule that targets an internet gateway as well as a route rule that targets a service gateway (for more information, see Issues with access from Oracle services through a service gateway to your public instances).

<table>
<thead>
<tr>
<th>DHCP Options</th>
<th>Created automatically and defined as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>DNS Type</strong> set to Internet and VCN Resolver</td>
</tr>
<tr>
<td>Resource</td>
<td>Example</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Lists</td>
<td>Two created (in addition to the default security list) manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List Name:</strong> workers</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List Name:</strong> loadbalancers</td>
</tr>
<tr>
<td></td>
<td>For details of the ingress rules and egress rules defined for the workers security list and the loadbalancers security list, see Example Security List Configurations for a Highly Available Public Cluster Using AD-Specific Subnets on page 844.</td>
</tr>
</tbody>
</table>
Three worker node AD-specific subnets created manually, named, and defined as follows:

- **Name:** workers-1 with the following properties:
  - **Availability Domain:** AD1
  - **CIDR Block:** 10.0.10.0/25
  - **Route Table:** routetable-1
  - **Subnet access:** Public
  - **DNS Resolution:** Selected
  - **DHCP Options:** Default
  - **Security List:** workers

- **Name:** workers-2 with the following properties:
  - **Availability Domain:** AD2
  - **CIDR Block:** 10.0.11.0/25
  - **Route Table:** routetable-1
  - **Subnet access:** Public
  - **DNS Resolution:** Selected
  - **DHCP Options:** Default
  - **Security List:** workers

- **Name:** workers-3 with the following properties:
  - **Availability Domain:** AD3
  - **CIDR Block:** 10.0.12.0/25
  - **Route Table:** routetable-1
  - **Subnet access:** Public
  - **DNS Resolution:** Selected
  - **DHCP Options:** Default
  - **Security List:** workers

Two load balancer AD-specific subnets created, named, and defined as follows:

- **Name:** loadbalancers-1 with the following properties:
  - **Availability Domain:** AD1
  - **CIDR Block:** 10.0.20.0/24
  - **Route Table:** routetable-0
  - **Subnet access:** Public
  - **DNS Resolution:** Selected
  - **DHCP Options:** Default
  - **Security List:** loadbalancers

- **Name:** loadbalancers-2 with the following properties:
  - **Availability Domain:** AD2
  - **CIDR Block:** 10.0.21.0/24
  - **Route Table:** routetable-0
  - **Subnet access:** Public
  - **DNS Resolution:** Selected
  - **DHCP Options:** Default
  - **Security List:** loadbalancers

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnets</td>
<td>Three worker node AD-specific subnets created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> workers-1 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Availability Domain:</strong> AD1</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block:</strong> 10.0.10.0/25</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route Table:</strong> routetable-1</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet access:</strong> Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution:</strong> Selected</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP Options:</strong> Default</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List:</strong> workers</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> workers-2 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Availability Domain:</strong> AD2</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block:</strong> 10.0.11.0/25</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route Table:</strong> routetable-1</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet access:</strong> Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution:</strong> Selected</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP Options:</strong> Default</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List:</strong> workers</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> workers-3 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Availability Domain:</strong> AD3</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block:</strong> 10.0.12.0/25</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route Table:</strong> routetable-1</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet access:</strong> Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution:</strong> Selected</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP Options:</strong> Default</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List:</strong> workers</td>
</tr>
<tr>
<td></td>
<td>Two load balancer AD-specific subnets created, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> loadbalancers-1 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Availability Domain:</strong> AD1</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block:</strong> 10.0.20.0/24</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route Table:</strong> routetable-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet access:</strong> Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution:</strong> Selected</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP Options:</strong> Default</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List:</strong> loadbalancers</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name:</strong> loadbalancers-2 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Availability Domain:</strong> AD2</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block:</strong> 10.0.21.0/24</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route Table:</strong> routetable-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Subnet access:</strong> Public</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution:</strong> Selected</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP Options:</strong> Default</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security List:</strong> loadbalancers</td>
</tr>
</tbody>
</table>
Example Security List Configurations for a Highly Available Public Cluster Using AD-Specific Subnets

In the example VCN, two security lists have been created (in addition to the default security list) to control access to and from the public worker node AD-specific subnets and the load balancer AD-specific subnets. The two security lists are named 'workers' and 'loadbalancers' respectively.

Note that two sets of alternative ingress and egress rules are given for the 'loadbalancers' security list, showing how to allow either unrestricted access to/from the cluster, and how to restrict access to/from a specific CIDR range.

Example Ingress Rules in the 'workers' Security List for Public Worker Node AD-Specific Subnets:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State: Stateless Src. Type: CIDR</td>
<td>10.0.10.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports Description: This optional rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required.</td>
</tr>
<tr>
<td>----</td>
<td>------------------</td>
<td>----------</td>
<td>---------------------------------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>2</td>
<td>Stateless</td>
<td>10.0.11.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports</td>
</tr>
<tr>
<td>3</td>
<td>Stateless</td>
<td>10.0.12.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports</td>
</tr>
</tbody>
</table>
### Example Egress Rules in the 'workers' Security List for Public Worker Node AD-Specific Subnets:

Consider these egress rules as a minimum requirement. If applications deployed on worker nodes need to communicate with destinations outside of the Oracle Service Network, add additional egress rules. For example, if applications use Helm charts from the Helm stable repository, or Docker images from docker.io.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>State: Stateful</td>
<td>0.0.0.0/0</td>
<td>Protocol: ICMP</td>
<td></td>
<td>Type: 3</td>
<td>Allows:</td>
<td>ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set</td>
</tr>
<tr>
<td></td>
<td>Src. Type: CIDR</td>
<td></td>
<td>Src. Port Range: n/a</td>
<td></td>
<td>Code: 4</td>
<td></td>
<td>Description: This rule enables worker nodes to receive Path MTU Discovery fragmentation messages.</td>
</tr>
<tr>
<td></td>
<td>Src. CIDR: 0.0.0.0/0</td>
<td></td>
<td>Dest. Port Range: n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>State: Stateful</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP</td>
<td></td>
<td>n/a</td>
<td>Allows:</td>
<td>TCP traffic for ports: 22 SSH Remote Login Protocol</td>
</tr>
<tr>
<td></td>
<td>Src. Type: CIDR</td>
<td></td>
<td>Src. Port Range: All</td>
<td></td>
<td></td>
<td></td>
<td>Description: This <em>optional</em> rule enables inbound SSH traffic from the internet on port 22 to access worker nodes.</td>
</tr>
<tr>
<td></td>
<td>Src. CIDR: 0.0.0.0/0</td>
<td></td>
<td>Dest. Port Range: 22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>State: Stateful</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP</td>
<td></td>
<td>n/a</td>
<td>Allows:</td>
<td>TCP traffic for ports: 30000 - 32767</td>
</tr>
<tr>
<td></td>
<td>Src. Type: CIDR</td>
<td></td>
<td>Src. Port Range: All</td>
<td></td>
<td></td>
<td></td>
<td>Description: This <em>optional</em> rule enables inbound traffic to the worker nodes on the default NodePort range of 30000-32767 (see the Kubernetes documentation).</td>
</tr>
<tr>
<td></td>
<td>Src. CIDR: 0.0.0.0/0</td>
<td></td>
<td>Dest. Port Range: 30000 - 32767</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>State: Dest. Type</td>
<td>Dest. CIDR or Dest. Service</td>
<td>Protocol: Src. Port Range: Dest. Port Range:</td>
<td>Type and Code</td>
<td>Allows: and Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------</td>
<td>--------------</td>
<td>------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Stateless Dest. Type: CIDR</td>
<td>10.0.0.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports Description: This <em>optional</em> rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Stateless Dest. Type: CIDR</td>
<td>10.0.11.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports Description: This <em>optional</em> rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>State: Dest. Type:</td>
<td>Dest. CIDR or Dest. Service</td>
<td>Protocol: Src. Port Range: Dest. Port Range:</td>
<td>Type and Code</td>
<td>Allows: and Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>State: Stateless Dest. Type: CIDR</td>
<td>10.0.12.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports Description: This <em>optional</em> rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: ICMP Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>All</td>
<td>Allows: ICMP traffic for all ports. Description: This rule enables outbound ICMP traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 80 Dest. Port Range: 80</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 80. Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>State: Dest. Type:</td>
<td>Dest. CIDR or Dest. Service</td>
<td>Protocol: Src. Port Range: Dest. Port Range:</td>
<td>Type and Code</td>
<td>Allows: and Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>------------------</td>
<td>----------------------------</td>
<td>------------------------------------------</td>
<td>--------------</td>
<td>--------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 443 Dest. Port Range: 443</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 443 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 6443 Dest. Port Range: 6443</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 6443 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 12250 Dest. Port Range: 12250</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 12250 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Example Ingress Rules in the 'loadbalancers' Security List for Load Balancer AD-Specific Subnets:*

If you want to allow unrestricted incoming traffic through the load balancer from the public internet, set up the following security rule:
### Example Egress Rules in the 'loadbalancers' Security List for Load Balancer AD-Specific Subnets:

If you want to allow unrestricted outgoing response traffic through the load balancer to the public internet, set up the following security rules:

|---|------------------|-----------|-----------------------------|-------------------|-------------|---------|-------------|
| 1 | Stateful         | 160.34.126.216/30 | Protocol: TCP            | Src. Port Range: All | Dest. Port Range: All | n/a     | Allows: TCP traffic for all ports: all  
Description: This rule only allows incoming public traffic to service load balancers from a particular public CIDR range. |
<table>
<thead>
<tr>
<th>#</th>
<th>State:</th>
<th>Dest. Type:</th>
<th>Dest. CIDR</th>
<th>Protocol: Src. Port Range:</th>
<th>Type: Code:</th>
<th>Allows:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State:</td>
<td>Stateless</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dest. Type:</td>
<td></td>
<td>Src. Port Range: All</td>
<td></td>
<td>Description: This rule enables responses from a web application through the service load balancers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIDR</td>
<td></td>
<td></td>
<td>Dest. Port Range: All</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Alternatively, if you want to restrict outgoing response traffic through the load balancer to just that going to worker node subnets in the cluster, set up the following security rules:

<table>
<thead>
<tr>
<th>#</th>
<th>State:</th>
<th>Dest. Type:</th>
<th>Dest. CIDR</th>
<th>Protocol: Src. Port Range:</th>
<th>Type: Code:</th>
<th>Allows:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State: Stateful</td>
<td>Dest. Type:</td>
<td>10.0.10.0/25</td>
<td>Protocol: TCP</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CIDR</td>
<td></td>
<td>Src. Port Range: All</td>
<td></td>
<td>Description: This rule restricts responses of the web application to the workers-1 subnet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dest. Port Range: All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>State: Stateful</td>
<td>Dest. Type:</td>
<td>10.0.11.0/25</td>
<td>Protocol: TCP</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CIDR</td>
<td></td>
<td>Src. Port Range: All</td>
<td></td>
<td>Description: This rule restricts responses of the web application to the workers-2 subnet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dest. Port Range: All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>State: Stateful</td>
<td>Dest. Type:</td>
<td>10.0.12.0/25</td>
<td>Protocol: TCP</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CIDR</td>
<td></td>
<td>Src. Port Range: All</td>
<td></td>
<td>Description: This rule restricts responses of the web application to the workers-3 subnet.</td>
<td></td>
</tr>
</tbody>
</table>
Example 2: Example Network Resource Configuration for a Highly Available Private Cluster in a Region with Three Availability Domains, Using AD-Specific Subnets

This example assumes you want worker nodes hosted in three private AD-specific subnets that can only be accessed from within the VCN.

**Example Network Resource Configuration**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCN</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: acme-dev-vcn</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIDR Block</strong>: 10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS Resolution</strong>: Selected</td>
</tr>
<tr>
<td>Internet Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: gateway-0</td>
</tr>
<tr>
<td>NAT Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: nat-gateway-0</td>
</tr>
<tr>
<td>Service Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: service-gateway-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Services</strong>: All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
<tr>
<td>Route Table</td>
<td>Two route tables created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: routetable-0, with a route rule defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination CIDR block</strong>: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type</strong>: Internet Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Internet Gateway</strong>: gateway-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>: routetable-1, with two route rules defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rule 1:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination CIDR block</strong>: 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type</strong>: NAT Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target NAT Gateway</strong>: nat-gateway-0</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rule 2:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination</strong>: All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Type</strong>: Service Gateway</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target</strong>: service-gateway-0</td>
</tr>
</tbody>
</table>

Note that to avoid the possibility of asymmetric routing, a route table for a public subnet cannot contain both a route rule that targets an internet gateway as well as a route rule that targets a service gateway (for more information, see Issues with access from Oracle services through a service gateway to your public instances).
### DHCP Options

Created automatically and defined as follows:
- **DNS Type** set to Internet and VCN Resolver

### Security Lists

Two created (in addition to the default security list) manually, named, and defined as follows:
- **Security List Name**: workers
- **Security List Name**: loadbalancers

For details of the ingress rules and egress rules defined for these security lists, see Example Security List Configurations for a Highly Available Private Cluster Using AD-Specific Subnets on page 855.
Three worker node AD-specific subnets created manually, named, and defined as follows:

- **Name**: workers-1 with the following properties:
  - **Availability Domain**: AD1
  - **CIDR Block**: 10.0.10.0/25
  - **Route Table**: routetable-1
  - **Subnet access**: Private
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: workers

- **Name**: workers-2 with the following properties:
  - **Availability Domain**: AD2
  - **CIDR Block**: 10.0.11.0/25
  - **Route Table**: routetable-1
  - **Subnet access**: Private
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: workers

- **Name**: workers-3 with the following properties:
  - **Availability Domain**: AD3
  - **CIDR Block**: 10.0.12.0/25
  - **Route Table**: routetable-1
  - **Subnet access**: Private
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: workers

Two load balancer AD-specific subnets created, named, and defined as follows:

- **Name**: loadbalancers-1 with the following properties:
  - **Availability Domain**: AD1
  - **CIDR Block**: 10.0.20.0/24
  - **Route Table**: routetable-0
  - **Subnet access**: Public
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: loadbalancers

- **Name**: loadbalancers-2 with the following properties:
  - **Availability Domain**: AD2
  - **CIDR Block**: 10.0.21.0/24
  - **Route Table**: routetable-0
  - **Subnet access**: Public
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: loadbalancers

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnets</td>
<td>Three worker node AD-specific subnets created manually, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: workers-1 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Availability Domain: AD1</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.10.0/25</td>
</tr>
<tr>
<td></td>
<td>• Route Table: routetable-1</td>
</tr>
<tr>
<td></td>
<td>• Subnet access: Private</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>• DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>• Security List: workers</td>
</tr>
<tr>
<td></td>
<td>• Name: workers-2 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Availability Domain: AD2</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.11.0/25</td>
</tr>
<tr>
<td></td>
<td>• Route Table: routetable-1</td>
</tr>
<tr>
<td></td>
<td>• Subnet access: Private</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>• DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>• Security List: workers</td>
</tr>
<tr>
<td></td>
<td>• Name: workers-3 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Availability Domain: AD3</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.12.0/25</td>
</tr>
<tr>
<td></td>
<td>• Route Table: routetable-1</td>
</tr>
<tr>
<td></td>
<td>• Subnet access: Private</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>• DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>• Security List: workers</td>
</tr>
<tr>
<td></td>
<td>Two load balancer AD-specific subnets created, named, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: loadbalancers-1 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Availability Domain: AD1</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.20.0/24</td>
</tr>
<tr>
<td></td>
<td>• Route Table: routetable-0</td>
</tr>
<tr>
<td></td>
<td>• Subnet access: Public</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>• DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>• Security List: loadbalancers</td>
</tr>
<tr>
<td></td>
<td>• Name: loadbalancers-2 with the following properties:</td>
</tr>
<tr>
<td></td>
<td>• Availability Domain: AD2</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.21.0/24</td>
</tr>
<tr>
<td></td>
<td>• Route Table: routetable-0</td>
</tr>
<tr>
<td></td>
<td>• Subnet access: Public</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td></td>
<td>• DHCP Options: Default</td>
</tr>
<tr>
<td></td>
<td>• Security List: loadbalancers</td>
</tr>
</tbody>
</table>
Example Security List Configurations for a Highly Available Private Cluster Using AD-Specific Subnets

In the example VCN, two security lists have been created (in addition to the default security list) to control access to and from the private worker node AD-specific subnets and the load balancer AD-specific subnets. The two security lists are named 'workers' and 'loadbalancers' respectively.

Example Ingress Rules in the 'workers' Security List for Private Worker Node AD-Specific Subnets:

|----|------------------|--------------|---------------------------------------------|-------------|----------------------|
| 1  | State: Stateless Src. Type: CIDR | 10.0.10.0/25 | Protocol: All Src. Port Range: n/a Dest. Port Range: n/a | n/a         | Allows: All traffic for all ports
Description: This optional rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required. |
|----|------------------|--------------|---------------------------|-------------------|-------------|---------------------|
| 2  | State: Stateless | 10.0.11.0/25 | Protocol: All Src. Port Range: n/a | Dest. Port Range: n/a | n/a         | Allows: All traffic for all ports
Description: This *optional* rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. In the rare case where no inter-pod communication is expected, this rule is not required. |
| 3  | State: Stateless | 10.0.12.0/25 | Protocol: All Src. Port Range: n/a | Dest. Port Range: n/a | n/a         | Allows: All traffic for all ports
Description: This *optional* rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. In the rare case where no inter-pod communication is expected, this rule is not required. |
### Example Egress Rules in the 'workers' Security List for Private Worker Node AD-Specific Subnets:

Consider these egress rules as a minimum requirement. If applications deployed on worker nodes need to communicate with destinations outside of the Oracle Service Network, add additional egress rules. For example, if applications use Helm charts from the Helm stable repository, or Docker images from docker.io.

<table>
<thead>
<tr>
<th>#</th>
<th>State: Dest. Type:</th>
<th>Dest. CIDR or Dest. Service</th>
<th>Protocol: Src. Port Range: Dest. Port Range:</th>
<th>Type: Code:</th>
<th>Allows: Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State: Stateless</td>
<td>10.0.10.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports Description: This optional rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>State: Stateful</td>
<td>10.0.0.0/16</td>
<td>Protocol: TCP Src. Port Range: All Dest. Port Range: 22</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 22 SSH Remote Login Protocol Description: This optional rule enables inbound SSH traffic from the VCN on port 22 to access worker nodes.</td>
</tr>
<tr>
<td>#</td>
<td>State:</td>
<td>Dest. Type:</td>
<td>Dest. CIDR or Dest. Service</td>
<td>Protocol: Src. Port Range:</td>
<td>Dest. Port Range:</td>
</tr>
<tr>
<td>----</td>
<td>-------</td>
<td>-------------</td>
<td>-----------------------------</td>
<td>----------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>2</td>
<td>Stateless</td>
<td>CIDR</td>
<td>10.0.11.0/25</td>
<td>Protocol: All</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Src. Port Range:</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Stateless</td>
<td>CIDR</td>
<td>10.0.12.0/25</td>
<td>Protocol: All</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Src. Port Range:</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>State: Dest. Type:</td>
<td>Dest. CIDR or Dest. Service</td>
<td>Protocol: Src. Port Range: Dest. Port Range:</td>
<td>Type: Code:</td>
<td>Allows: Description:</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: ICMP Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>All</td>
<td>Allows: ICMP traffic for all ports. Description: This rule enables outbound ICMP traffic.</td>
</tr>
<tr>
<td>5</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 80 Dest. Port Range: 80</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 80. Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
</tr>
<tr>
<td>6</td>
<td>State: Stateful Dest. Type: Service</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 443 Dest. Port Range: 443</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 443 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
</tr>
<tr>
<td>#</td>
<td>State: Dest. Type:</td>
<td>Dest. CIDR or Dest. Service</td>
<td>Protocol: Src. Port Range: Dest. Port Range:</td>
<td>Type: Code:</td>
<td>Allows: Description:</td>
</tr>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>7</td>
<td>State: Stateful</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 6443 Dest. Port Range: 6443</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 6443 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
</tr>
<tr>
<td>8</td>
<td>State: Stateful</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 12250 Dest. Port Range: 12250</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 12250 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
</tr>
</tbody>
</table>

**Example Ingress Rules in the 'loadbalancers' Security List for a Load Balancer AD-Specific Subnet:**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State: Stateless</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP Src. Port Range: All Dest. Port Range: All</td>
<td>n/a</td>
<td>Allows: TCP traffic for all ports: all Description: This rule enables incoming public traffic to service load balancers.</td>
</tr>
</tbody>
</table>
Example Egress Rules in the 'loadbalancers' Security List for a Load Balancer AD-Specific Subnet:

<table>
<thead>
<tr>
<th>#</th>
<th>State: Dest. Type:</th>
<th>Dest. CIDR</th>
<th>Protocol: Src. Port Range: Dest. Port Range:</th>
<th>Type: Code:</th>
<th>Allows: Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stateless Dest. Type: CIDR</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP Src. Port Range: All Dest. Port Range: All</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: all Description: This rule enables responses from a web application through the service load balancers.</td>
</tr>
</tbody>
</table>

Example 3: Example Network Resource Configuration for a Highly Available Public Cluster in a Region with Three Availability Domains, Using a Regional Subnet

This example assumes you want worker nodes hosted in a public regional subnet that can be accessed directly from the internet.

Example Network Resource Configuration

<table>
<thead>
<tr>
<th>Resource</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCN</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: acme-dev-vcn</td>
</tr>
<tr>
<td></td>
<td>• CIDR Block: 10.0.0.0/16</td>
</tr>
<tr>
<td></td>
<td>• DNS Resolution: Selected</td>
</tr>
<tr>
<td>Internet Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: gateway-0</td>
</tr>
<tr>
<td>Service Gateway</td>
<td>Created manually, and defined as follows:</td>
</tr>
<tr>
<td></td>
<td>• Name: service-gateway-0</td>
</tr>
<tr>
<td></td>
<td>• Services: All &lt;region&gt; Services in Oracle Services Network</td>
</tr>
</tbody>
</table>
Two route tables created manually, named, and defined as follows:

- **Name**: routetable-0, with a route rule defined as follows:
  - **Destination CIDR block**: 0.0.0.0/0
  - **Target Type**: Internet Gateway
  - **Target Internet Gateway**: gateway-0

- **Name**: routetable-1, with a route rule defined as follows:
  - **Destination**: All <region> Services in Oracle Services Network
  - **Target Type**: Service Gateway
  - **Target**: service-gateway-0

Note that to avoid the possibility of asymmetric routing, a route table for a public subnet cannot contain both a route rule that targets an internet gateway as well as a route rule that targets a service gateway (for more information, see Issues with access from Oracle services through a service gateway to your public instances).

**DHCP Options**

Created automatically and defined as follows:

- **DNS Type** set to Internet and VCN Resolver

**Security Lists**

Two created (in addition to the default security list) manually, named, and defined as follows:

- **Security List Name**: workers
- **Security List Name**: loadbalancers

For details of the ingress rules and egress rules defined for the workers security list and the loadbalancers security list, see Example Security List Configurations for a Highly Available Public Cluster using Regional Subnets on page 863.

**Subnets**

One worker node regional subnet created manually, named, and defined as follows:

- **Name**: workers-rs with the following properties:
  - **CIDR Block**: 10.0.10.0/25
  - **Route Table**: routetable-1
  - **Subnet access**: Public
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: workers

One load balancer regional subnet created, named, and defined as follows:

- **Name**: loadbalancers-rs with the following properties:
  - **CIDR Block**: 10.0.20.0/24
  - **Route Table**: routetable-0
  - **Subnet access**: Public
  - **DNS Resolution**: Selected
  - **DHCP Options**: Default
  - **Security List**: loadbalancers
**Example Security List Configurations for a Highly Available Public Cluster using Regional Subnets**

In the example VCN, two security lists have been created (in addition to the default security list) to control access to and from a public worker node regional subnet and a load balancer regional subnet. The two security lists are named 'workers' and 'loadbalancers' respectively.

**Example Ingress Rules in the 'workers' Security List for a Public Worker Node Regional Subnet:**

|---|------------------|-----------|-----------------------------------------------|-------------|---------------------|
| 1 | **State**: Stateless  
**Src. Type**: CIDR | 10.0.10.0/25 | Protocol: All  
Src. Port Range: n/a  
Dest. Port Range: n/a | n/a | Allows: All traffic for all ports  
Description: This *optional* rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required. |
| 2 | **State**: Stateful  
**Src. Type**: CIDR | 0.0.0.0/0 | Protocol: ICMP  
Src. Port Range: n/a  
Dest. Port Range: n/a | 3  
Code: 4 | Allows: ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set  
Description: This rule enables worker nodes to receive Path MTU Discovery fragmentation messages. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>State: Stateful</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 22 SSH Remote Login Protocol. Description: This optional rule enables inbound SSH traffic from the internet on port 22 to access worker nodes.</td>
</tr>
<tr>
<td>4</td>
<td>State: Stateful</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 30000 - 32767. Description: This optional rule enables inbound traffic to the worker nodes on the default NodePort range of 30000-32767 (see the Kubernetes documentation).</td>
</tr>
</tbody>
</table>

Example Egress Rules in the 'workers' Security List for a Public Worker Node Regional Subnet:

Consider these egress rules as a minimum requirement. If applications deployed on worker nodes need to communicate with destinations outside of the Oracle Service Network, add additional egress rules. For example, if applications use Helm charts from the Helm stable repository, or Docker images from docker.io.
<table>
<thead>
<tr>
<th>#</th>
<th>State: Dest. Type:</th>
<th>Dest. CIDR or Dest. Service</th>
<th>Protocol: Src. Port Range: Dest. Port Range:</th>
<th>Type: Code:</th>
<th>Allows:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State: Stateless</td>
<td>10.0.10.0/25</td>
<td>Protocol: All Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>n/a</td>
<td>Allows: All traffic for all ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dest. Type: CIDR</td>
<td></td>
<td></td>
<td></td>
<td>Description: This <em>optional</em> rule enables intra-VCN traffic. Although optional, this rule is usually necessary to enable pods on one worker node to communicate with pods on other worker nodes. Only in the rare case where no inter-pod communication is expected, is this rule not required.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>State: Stateful</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: ICMP Src. Port Range: n/a Dest. Port Range: n/a</td>
<td>All</td>
<td>Allows: ICMP traffic for all ports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dest. Type: Service</td>
<td></td>
<td></td>
<td></td>
<td>Description: This rule enables outbound ICMP traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dest. Type: Service</td>
<td></td>
<td></td>
<td></td>
<td>Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dest. Type: Service</td>
<td></td>
<td></td>
<td></td>
<td>Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
<td></td>
</tr>
</tbody>
</table>
Container Engine for Kubernetes

<table>
<thead>
<tr>
<th>#</th>
<th>State: Dest. Type:</th>
<th>Dest. CIDR or Dest. Service</th>
<th>Protocol: Src. Port Range: Dest. Port Range:</th>
<th>Type: Code:</th>
<th>Allows: Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>State: Stateful</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 6443 Dest. Port Range: 6443</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 6443 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
</tr>
<tr>
<td>6</td>
<td>State: Stateful</td>
<td>All &lt;region&gt; Services in Oracle Services Network</td>
<td>Protocol: TCP Src. Port Range: 12250 Dest. Port Range: 12250</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 12250 Description: This rule enables worker nodes to communicate with Container Engine for Kubernetes to ensure correct start-up, and continued functioning.</td>
</tr>
</tbody>
</table>

Example Ingress Rules in the 'loadbalancers' Security List for a Load Balancer Regional Subnet:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>State: Stateless</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP Src. Port Range: All Dest. Port Range: All</td>
<td>n/a</td>
<td>Allows: TCP traffic for all ports: all Description: This rule enables incoming public traffic to service load balancers.</td>
</tr>
</tbody>
</table>
Example Egress Rules in the 'loadbalancers' Security List for a Load Balancer Regional Subnet:

<table>
<thead>
<tr>
<th>#</th>
<th>State: Dest. Type:</th>
<th>Dest. CIDR</th>
<th>Protocol: Src. Port Range: Dest. Port Range:</th>
<th>Type: Code:</th>
<th>Allows: Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stateless Dest. Type: CIDR</td>
<td>0.0.0.0/0</td>
<td>Protocol: TCP Src. Port Range: All Dest. Port Range: All</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: all Description: This rule enables responses from a web application through the service load balancers.</td>
</tr>
</tbody>
</table>

CIDR Blocks and Container Engine for Kubernetes

When configuring the VCN and the worker node and load balancer subnets for use with Container Engine for Kubernetes, you specify CIDR blocks to indicate the network addresses that can be allocated to the resources. See Network Resource Configuration for Cluster Creation and Deployment on page 836.

When creating a cluster with Container Engine for Kubernetes, you specify:

- CIDR blocks for the Kubernetes services
- CIDR blocks that can be allocated to pods running in the cluster (see Creating a Kubernetes Cluster on page 871)

Note the following:

- The CIDR block you specify for the VCN must not overlap with the CIDR block you specify for the Kubernetes services.
- The CIDR blocks you specify for pods running in the cluster must not overlap with CIDR blocks you specify for worker node and load balancer subnets.
- Each pod running on a worker node is assigned its own network address. Container Engine for Kubernetes allocates a /25 CIDR block of network addresses for each worker node in a cluster, to assign to pods running on that node. A /25 CIDR block equates to 128 distinct IP addresses, of which one is reserved. So a maximum of 127 network addresses are available to assign to pods running on each worker node (more than sufficient, given that the number of pods per node is capped at 110).
- When you create a cluster, you specify a value for the cluster's Pods CIDR Block property, either implicitly in the case of a 'quick cluster' or explicitly in the case of a 'custom cluster'. You cannot change the cluster's Pods CIDR Block property after the cluster has been created. The cluster's Pods CIDR Block property constrains the maximum total number of network addresses available for allocation to pods running on all the nodes in the cluster, and therefore effectively limits the number of nodes in the cluster. By default, the cluster's Pods CIDR Block property is set to a /16 CIDR block, making 65,536 network addresses available for all the nodes in the cluster. Since 128 network addresses are allocated for each node, specifying a /16 CIDR block for the cluster's Pods CIDR Block property limits the number of nodes in the cluster to 512. This is generally sufficient. To support more than 512 nodes in a cluster, create a 'custom cluster' and specify a larger value for the cluster's Pods CIDR Block property when you create the cluster. For example, specify a /14 CIDR block for the cluster's Pods CIDR Block property to create a cluster with 262,144 network addresses available for the nodes in the cluster (more than sufficient, given that the number of nodes per cluster is capped at 1000).
Policy Configuration for Cluster Creation and Deployment

When a tenancy is created, an Administrators group is automatically created for the tenancy. Users that are members of the Administrators group can perform any operation on resources in the tenancy. If all the users that will be working with Container Engine for Kubernetes are already members of the Administrators group, there's no need to create additional policies. However, if you want to enable users that are not members of the Administrators group to use Container Engine for Kubernetes, you must create policies to enable the groups to which those users do belong to perform operations on resources in the tenancy or in individual compartments. Some policies are required, some are optional. See Create Required Policy for Groups on page 868 and Create One or More Additional Policies for Groups on page 869.

Note that in addition to the above policies managed by IAM, you can also use the Kubernetes RBAC Authorizer to enforce additional fine-grained access control for users on specific clusters via Kubernetes RBAC roles and clusterroles. See About Access Control and Container Engine for Kubernetes on page 920.

Create Required Policy for Groups

To create, update, and delete clusters and node pools, users that are not members of the Administrators group must have permissions to work with cluster-related resources. To give users the necessary access, you must create a policy with a number of required policy statements for the groups to which those users do belong:

1. In the Console, open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed.
2. Select the tenancy's root compartment or an individual compartment containing cluster-related resources from the list on the left.
3. Click Create Policy.
4. Enter the following:

- **Name:** A name for the policy (for example, acme-dev-team-oke-required-policy) that is unique within the compartment. If you are creating the policy in the tenancy's root compartment, the name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
- **Description:** A friendly description. You can change this later if you want to.
- **Statement:** The following required policy statements to enable users to use Container Engine for Kubernetes to create, update, and delete clusters and node pools:

```
Allow group <group-name> to manage instance-family in <location>
Allow group <group-name> to use subnets in <location>
Allow group <group-name> to read virtual-network-family in <location>
Allow group <group-name> to use vnics in <location>
Allow group <group-name> to inspect compartments in <location>
```

The following required policy statement to enable users to perform any operation on cluster-related resources (this 'catch-all' policy effectively makes all users administrators insofar as cluster-related resources are concerned):

```
Allow group <group-name> to manage cluster-family in <location>
```

In the above policy statements, replace <location> with either tenancy (if you are creating the policy in the tenancy's root compartment) or compartment <compartment-name> (if you are creating the policy in an individual compartment).
- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more
information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Create.

Create One or More Additional Policies for Groups

To enable users that are not members of the Administrators group to use Container Engine for Kubernetes, create additional policies to enable the groups to which those users do belong to perform operations on cluster-related resources as follows:

1. In the Console, open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed.
2. Select the tenancy's root compartment or an individual compartment containing cluster-related resources from the list on the left.
3. Click Create Policy.
4. Enter the following:

   • Name: A name for the policy (for example, acme-dev-team-oke-additional-policy) that is unique within the compartment. If you are creating the policy in the tenancy's root compartment, the name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
   • Description: A friendly description. You can change this later if you want to.
   • Statement: A suitable policy statement to allow existing groups to perform operations on cluster-related resources. In the example policy statements below, replace <location> with either tenancy (if you are
creating the policy in the tenancy's root compartment) or **compartment <compartment-name>** (if you are creating the policy in an individual compartment):

- **To enable users in the acme-dev-team group to automatically create and configure associated new network resources when creating new 'quick clusters', policies must also grant the group:**
  - VCN_READ and VCN_CREATE permissions. Enter a policy statement like:
    
    ```
    Allow group acme-dev-team to manage vcns in <location>
    ```
  - SUBNET_READ and SUBNET_CREATE permissions. Enter a policy statement like:
    
    ```
    Allow group acme-dev-team to manage subnets in <location>
    ```
  - INTERNET_GATEWAY_CREATE permission. Enter a policy statement like:
    
    ```
    Allow group acme-dev-team to manage internet-gateways in <location>
    ```
  - NAT_GATEWAY_CREATE permission. Enter a policy statement like:
    
    ```
    Allow group acme-dev-team to manage nat-gateways in <location>
    ```
  - ROUTE_TABLE_UPDATE permission. Enter a policy statement like:
    
    ```
    Allow group acme-dev-team to manage route-tables in <location>
    ```
  - SECURITY_LIST_CREATE permission. Enter a policy statement like:
    
    ```
    Allow group acme-dev-team to manage security-lists in <location>
    ```

- **To enable users in the acme-dev-team-cluster-viewers group to simply list the clusters, enter a policy statement like:**
  
  ```
  Allow group acme-dev-team-cluster-viewers to inspect clusters in <location>
  ```

- **To enable users in the acme-dev-team-pool-admins group to list, create, update, and delete node pools, enter a policy statement like:**
  
  ```
  Allow group acme-dev-team-pool-admins to use cluster-node-pools in <location>
  ```

- **To enable users in the acme-dev-team-auditors group to see details of operations performed on clusters, enter a policy statement like:**
  
  ```
  Allow group acme-dev-team-auditors to read cluster-work-requests in <location>
  ```

- **To enable users in the acme-dev-team-sgw group to create a service gateway to enable worker nodes to access other resources in the same region without exposing data to the public internet, enter a policy statement like:**
  
  ```
  Allow group acme-dev-team-sgw to manage service-gateways in <location>
  ```

- **To enable users in the acme-dev-team group to access clusters using Cloud Shell, enter a policy statement like:**
  
  ```
  Allow group acme-dev-team to use cloud-shell in <location>
  ```

Note that to access clusters using Cloud Shell, you'll also need to set up the kubeconfig file appropriately (see Setting Up Cloud Shell Access to Clusters on page 876). For more information about Cloud Shell, see Cloud Shell.
Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Create.

Creating a Kubernetes Cluster

You can use Container Engine for Kubernetes to create new Kubernetes clusters. To create a cluster, you must either belong to the tenancy's Administrators group, or belong to a group to which a policy grants the CLUSTER_MANAGE permission. See Policy Configuration for Cluster Creation and Deployment on page 868.

You first specify basic details for the new cluster (the cluster name, and the Kubernetes version to install on control plane nodes). You can then create the cluster in one of two ways:

- Using default settings to create a 'quick cluster' with new network resources as required. This approach is the fastest way to create a new cluster. If you accept all the default values, you can create a new cluster in just a few clicks. New network resources for the 'quick cluster' are created automatically, including one regional subnet for worker nodes, and another regional subnet for load balancers. The regional subnet for load balancers will be public, but you can specify whether the regional subnet for worker nodes will be public or private. Note that if you specify a private regional subnet for worker nodes in the 'quick cluster', a NAT gateway is also created (in addition to an internet gateway). To create a 'quick cluster', you must belong to a group to which a policy grants the necessary permissions to create the new network resources (see Create One or More Additional Policies for Groups on page 869).

- Using custom settings to create a 'custom cluster'. This approach gives you the most control over the new cluster. You can explicitly define the new cluster's properties. And you can explicitly specify which existing network resources to use, including the existing public or private subnets in which to create worker nodes and load balancers. The subnets can be regional subnets (recommended) or AD-specific subnets.

Note that although you will usually define node pools immediately when defining a new 'custom cluster', you don't have to. You can create a 'custom cluster' with no node pools, and add node pools later. One reason to create a 'custom cluster' that initially has no node pools is if you intend to install and configure a CNI network provider like Calico to support Kubernetes NetworkPolicy resources. If you install Calico on a cluster that has existing node pools in which pods are already running, you'll have to recreate the pods when the Calico installation is complete. For example, by running the kubectl rollout restart command. If you install Calico on a cluster before creating any node pools in the cluster (recommended), you can be sure that there will be no pods to recreate. See Example: Installing Calico and Setting Up Network Policies on page 960.

Regardless of how you create a cluster, Container Engine for Kubernetes gives names to worker nodes in the following format:

oke-c<part-of-cluster-OCID>-n<part-of-node-pool-OCID>-s<part-of-subnet-OCID>-
[slot]

where:

- oke is the standard prefix for all worker nodes created by Container Engine for Kubernetes
- c<part-of-cluster-OCID> is a portion of the cluster's OCID, prefixed with the letter c
- n<part-of-node-pool-OCID> is a portion of the node pool's OCID, prefixed with the letter n
- s<part-of-subnet-OCID> is a portion of the subnet's OCID, prefixed with the letter s
- <slot> is an ordinal number of the node in the subnet (for example, 0, 1)

For example, if you specified a cluster is to have two nodes in a node pool, the two nodes might be named:

- oke-cywiqripuyg-nsgagklgnst-st2qczvnmba-0
- oke-cywiqripuyg-nsgagklgnst-st2qczvnmba-1

Do not change the auto-generated names that Container Engine for Kubernetes gives to worker nodes.

To ensure high availability, Container Engine for Kubernetes:
• creates the Kubernetes Control Plane on multiple Oracle-managed control plane nodes (distributing the control plane nodes across different availability domains in a region, where supported)
• creates worker nodes in each of the fault domains in an availability domain (distributing the worker nodes as evenly as possible across the fault domains, subject to any other infrastructure restrictions)

Using the Console to create a ‘Quick Cluster’ with Default Settings

To create a ‘quick cluster’ with default settings and new network resources using Container Engine for Kubernetes:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Kubernetes Clusters.
2. Choose a Compartment you have permission to work in.
3. On the Cluster List page, click Create Cluster.
4. In the Create Cluster dialog, select Quick Create and click Launch Workflow.
5. On the Create Cluster page, either just accept the default configuration details for the new cluster, or specify alternatives as follows:

- **Name**: The name of the new cluster. Either accept the default name or enter a name of your choice. Avoid entering confidential information.
- **Compartment**: The compartment in which to create the new cluster and the associated network resources.
- **Kubernetes Version**: The version of Kubernetes to run on the control plane nodes and worker nodes of the cluster. Either accept the default version or select a version of your choice. Amongst other things, the Kubernetes version you select determines the default set of admission controllers that are turned on in the created cluster (see Supported Admission Controllers on page 924).
- **Visibility Type**: Whether to create a private or a public regional subnet to host worker nodes (note that a public regional subnet is always created to host load balancers in a ‘quick cluster’, regardless of your selection here):
  - **Private**: Select to create a private regional subnet to host worker nodes (along with the public regional subnet to host load balancers).
  - **Public**: Select to create a public regional subnet to host worker nodes (along with the public regional subnet to host load balancers).
- **Shape**: The shape to use for each node in the node pool. The shape determines the number of CPUs and the amount of memory allocated to each node. If you select a flexible shape, you can explicitly specify the number of CPUs and the amount of memory. The list shows only those shapes available in your tenancy that are supported by Container Engine for Kubernetes. See Supported Images (Including Custom Images) and Shapes for Worker Nodes on page 923.
- **Number of Nodes**: The number of worker nodes to create in the node pool, placed in the regional subnet created for the ‘quick cluster’. The nodes are distributed as evenly as possible across the availability domains in a region (or in the case of a region with a single availability domain, across the fault domains in that availability domain).

6. Either accept the default size of worker node boot volumes (as determined from the default image used for worker nodes) or click Specify a Custom Boot Volume Size and specify an alternative size for worker node boot volumes in **Boot Volume Size in GB**. If you do specify a custom boot volume size, it must be larger than the image’s default boot volume size. The minimum and maximum sizes you can specify are 50 GB and 32 TB respectively. See Custom Boot Volume Sizes on page 610.

7. Either accept the defaults for advanced cluster options, or click Show Advanced Options and specify alternatives as follows:

- **Public SSH Key**: (Optional) The public key portion of the key pair you want to use for SSH access to each node in the node pool. The public key is installed on all worker nodes in the cluster. Note that if you don’t specify a public SSH key, Container Engine for Kubernetes will provide one. However, since you won’t have the corresponding private key, you will not have SSH access to the worker nodes. Note that if you specify that you want the worker nodes in the ‘quick cluster’ to be hosted in a private regional subnet, you cannot use SSH to access them directly (see Connecting to Worker Nodes in Private Subnets Using SSH on page 905).
- **Kubernetes Labels**: (Optional) One or more labels (in addition to a default label) to add to worker nodes in the node pool to enable the targeting of workloads at specific node pools.
8. Click **Next** to review the details you entered for the new cluster.

9. Click **Create Cluster** to create the new network resources and the new cluster.

   Container Engine for Kubernetes starts creating resources (as shown in the **Creating cluster and associated network resources** dialog):
   - the network resources (such as the VCN, internet gateway, NAT gateway, route tables, security lists, a regional subnet for worker nodes and another regional subnet for load balancers), with auto-generated names in the format `oke-<resource-type>-quick-<cluster-name>-<creation-date>`
   - the cluster, with the name you specified
   - the node pool, named pool1
   - worker nodes, with auto-generated names in the format `oke-c<part-of-cluster-OCID>-n<part-of-node-pool-OCID>-s<part-of-subnet-OCID>-<slot>`

   Do not change the resource names that Container Engine for Kubernetes has auto-generated. Note that if the cluster is not created successfully for some reason (for example, if you have insufficient permissions or if you’ve exceeded the cluster limit for the tenancy), any network resources created during the cluster creation process are not deleted automatically. You will have to manually delete any such unused network resources.

10. Click **Close** to return to the Console.

Initially, the new cluster appears in the Console with a status of Creating. When the cluster has been created, it has a status of Active.

Container Engine for Kubernetes also creates a Kubernetes kubeconfig configuration file that you use to access the cluster using `kubectl`.

### Using the Console to create a 'Custom Cluster' with Explicitly Defined Settings

To create a 'custom cluster' with explicitly defined settings and existing network resources using Container Engine for Kubernetes:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Cluster List** page, click **Create Cluster**.
4. In the **Create Cluster** dialog, select **Custom Create** and click **Launch Workflow**.
5. On the **Create Cluster** page, either just accept the default configuration details for the new cluster, or specify alternatives as follows:
   - **Name:** The name of the new cluster. Either accept the default name or enter a name of your choice. Avoid entering confidential information.
   - **Compartment:** The compartment in which to create the new cluster.
   - **Kubernetes Version:** The version of Kubernetes to run on the control plane nodes and worker nodes of the cluster. Either accept the default version or select a version of your choice. Amongst other things, the Kubernetes version you select determines the default set of admission controllers that are turned on in the created cluster (see **Supported Admission Controllers** on page 924).
6. Either accept the defaults for advanced cluster options, or click **Show Advanced Options** and set the options as follows:
   a. Specify whether to encrypt Kubernetes secrets at rest in the etcd key-value store for the cluster using the Vault service:
      - **No Encryption:** Kubernetes secrets at rest in the etcd key-value store are not encrypted.
      - **Encrypt Using Customer-Managed Keys:** Encrypt Kubernetes secrets in the etcd key-value store and specify:
         - **Choose a Vault in `<compartment-name>`:** The vault that contains the master encryption key, from the list of vaults in the specified compartment. By default, `<compartment-name>` is the compartment...
in which you are creating the cluster, but you can select a different compartment by clicking Change Compartment.

- **Choose a Key in <compartment-name>:** The name of the master encryption key, from the list of keys in the specified compartment. By default, <compartment-name> is the compartment in which you are creating the cluster, but you can select a different compartment by clicking Change Compartment. Note that you cannot change the master encryption key after the cluster has been created.

Note that if you do want to use encryption, a suitable master encryption key, dynamic group, and policy must already exist before you can create the cluster. For more information, see Encrypting Kubernetes Secrets at Rest in Etcd on page 900.

b. Specify whether to control the operations that pods are allowed to perform on the cluster by enforcing pod security policies:

- **Not Enforced:** Do not enforce pod security policies.
- **Enforced:** Do enforce pod security policies, by enabling the PodSecurityPolicy admission controller. Only pods that meet the conditions in a pod security policy are accepted by the cluster. For more information, see Using Pod Security Policies with Container Engine for Kubernetes on page 905.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is very important to note that when you enable a cluster's PodSecurityPolicy admission controller, no application pods can start on the cluster unless suitable pod security policies exist, along with roles (or clusterroles) and rolebindings (or clusterrolebindings) to associate pods with policies. You will not be able to run application pods on a cluster with an enabled PodSecurityPolicy admission controller unless these prerequisites are met.</td>
</tr>
</tbody>
</table>

We strongly recommend you use PodSecurityPolicy admission controllers as follows:

- Whenever you create a new cluster, enable the Pod Security Admission Controller.
- Immediately after creating a new cluster, create pod security policies, along with roles (or clusterroles) and rolebindings (or clusterrolebindings).

7. Click **Next** and specify the existing network resources to use for the new cluster on the **Network Setup** page:

- **VCN in <compartment-name>:** The existing virtual cloud network that has been configured for cluster creation and deployment. By default, <compartment-name> is the compartment in which you are creating the cluster, but you can select a different compartment by clicking Change Compartment. See VCN Configuration on page 837.

- **Kubernetes Service LB Subnets:** Optionally, the existing subnets that have been configured to host load balancers. Load balancer subnets must be different from worker node subnets, can be public or private, and can be regional (recommended) or AD-specific. You don't have to specify any load balancer subnets. However, if you do specify load balancer subnets, the number of load balancer subnets to specify depends on the region in which you are creating the cluster and whether the subnets are regional or AD-specific.

If you are creating a cluster in a region with three availability domains, you can specify:

- Zero or one load balancer regional subnet (recommended).
- Zero or two load balancer AD-specific subnets. If you specify two AD-specific subnets, the two subnets must be in different availability domains.

If you are creating a cluster in a region with a single availability domain, you can specify:

- Zero or one load balancer regional subnet (recommended).
- Zero or one load balancer AD-specific subnet.

See Subnet Configuration on page 839.
8. Either accept the defaults for advanced cluster options, or click Show Advanced Options and specify alternatives as follows:

- **Kubernetes Service CIDR Block**: The available group of network addresses that can be exposed as Kubernetes services (ClusterIPs), expressed as a single, contiguous IPv4 CIDR block. For example, 10.96.0.0/16. The CIDR block you specify must not overlap with the CIDR block for the VCN. See CIDR Blocks and Container Engine for Kubernetes on page 867.
- **Pods CIDR Block**: The available group of network addresses that can be allocated to pods running in the cluster, expressed as a single, contiguous IPv4 CIDR block. For example, 10.244.0.0/16. The CIDR block you specify must not overlap with the CIDR blocks for subnets in the VCN, and can be outside the VCN CIDR block. See CIDR Blocks and Container Engine for Kubernetes on page 867.

9. Click Next and specify configuration details for the first node pool in the cluster on the Node Pools page:

- **Name**: A name of your choice for the new node pool. Avoid entering confidential information.
- **Version**: The version of Kubernetes to run on each worker node in the node pool. By default, the version of Kubernetes specified for the control plane nodes is selected. The Kubernetes version on worker nodes must be either the same version as that on the control plane nodes, or an earlier version that is still compatible. See Kubernetes Versions and Container Engine for Kubernetes on page 926.
- **Image**: The image to use on each node in the node pool. An image is a template of a virtual hard drive that determines the operating system and other software for the node. See Supported Images (Including Custom Images) and Shapes for Worker Nodes on page 923.
- **Shape**: The shape to use for each node in the node pool. The shape determines the number of CPUs and the amount of memory allocated to each node. If you select a flexible shape, you can explicitly specify the number of CPUs and the amount of memory. The list shows only those shapes available in your tenancy that are supported by Container Engine for Kubernetes. See Supported Images (Including Custom Images) and Shapes for Worker Nodes on page 923.
- **Number of Nodes**: The number of worker nodes to create in the node pool, placed in the availability domains you select, and in the regional subnet (recommended) or AD-specific subnet you specify for each availability domain.
- **Availability Domain 1**:
  - **Availability Domain**: An availability domain in which to place worker nodes.
  - **Subnet**: A regional subnet (recommended) or AD-specific subnet configured to host worker nodes. If you specified load balancer subnets, the worker node subnets must be different. The subnets you specify can be public or private, and can be regional (recommended) or AD-specific. See Subnet Configuration on page 839.

Optionally click Add Availability Domain to select additional domains and subnets in which to place worker nodes.

When they are created, the worker nodes are distributed as evenly as possible across the availability domains you select (or in the case of a single availability domain, across the fault domains in that availability domain).

- **Specify a Custom Boot Volume Size**: Either accept the default size of worker node boot volumes (as determined from the image used for worker nodes) or click and specify an alternative size for worker node boot volumes in Boot Volume Size in GB:. If you do specify a custom boot volume size, it must be larger than the image's default boot volume size. The minimum and maximum sizes you can specify are 50 GB and 32 TB respectively. See Custom Boot Volume Sizes on page 610.
- **Public SSH Key**: (Optional) The public key portion of the key pair you want to use for SSH access to each node in the node pool. The public key is installed on all worker nodes in the cluster. Note that if you don't specify a public SSH key, Container Engine for Kubernetes will provide one. However, since you won't have the corresponding private key, you will not have SSH access to the worker nodes. Note that you cannot use SSH to access directly any worker nodes in private subnets (see Connecting to Worker Nodes in Private Subnets Using SSH on page 905).
- **Kubernetes Labels**: (Optional) One or more labels (in addition to a default label) to add to worker nodes in the node pool to enable the targeting of workloads at specific node pools.
10. (Optional) Click **Another node pool** and specify configuration details for a second and subsequent node pools in the cluster.

If you define multiple node pools in a cluster, you can host all of them on a single AD-specific subnet. However, it's best practice to host different node pools for a cluster on a regional subnet (recommended) or on different AD-specific subnets (one in each availability domain in the region).

11. Click **Next** to review the details you entered for the new cluster.

12. Click **Create Cluster** to create the new cluster.

Container Engine for Kubernetes starts creating the cluster with the name you specified.

If you specified details for one or more node pools, Container Engine for Kubernetes creates:

- node pools with the names you specified
- worker nodes with auto-generated names in the format `oke-c<part-of-cluster-OCID>-n<part-of-node-pool-OCID>-s<part-of-subnet-OCID>-<slot>`

Do not change the auto-generated names of worker nodes.

13. Click **Close** to return to the Console.

Initially, the new cluster appears in the Console with a status of Creating. When the cluster has been created, it has a status of Active.

Container Engine for Kubernetes also creates a Kubernetes kubeconfig configuration file that you use to access the cluster using kubectl.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the **CreateCluster** operation to create a cluster.

**Setting Up Cluster Access**

To access a cluster using kubectl, you have to set up a Kubernetes configuration file (commonly known as a 'kubeconfig' file) for the cluster. The kubeconfig file (by default named `config` and stored in the `$HOME/.kube` directory) provides the necessary details to access the cluster. Having set up the kubeconfig file, you can start using kubectl to manage the cluster.

The steps to follow when setting up the kubeconfig file depend on how you want to access the cluster:

- To access the cluster using kubectl in Cloud Shell, run an Oracle Cloud Infrastructure CLI command in the Cloud Shell window to set up the kubeconfig file.

  See Setting Up Cloud Shell Access to Clusters on page 876.

- To access the cluster using a local installation of kubectl:
  - Generate an API signing key pair (if you don't already have one).
  - Upload the public key of the API signing key pair.
  - Install and configure the Oracle Cloud Infrastructure CLI.
  - Set up the kubeconfig file.

  See Setting Up Local Access to Clusters on page 877.

**Setting Up Cloud Shell Access to Clusters**

To set up a kubeconfig file to enable access to a cluster using kubectl in Cloud Shell:

**Step 1: Set up the kubeconfig file**

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.

3. On the **Cluster List** page, click the name of the cluster you want to access using kubectl. The **Cluster** page shows details of the cluster.

4. Click the **Access Cluster** button to display the **Access Your Cluster** dialog box.

5. Click **Cloud Shell Access**.

6. Click **Launch Cloud Shell** to display the Cloud Shell window. For more information about Cloud Shell (including the required IAM policy), see **Cloud Shell**.

7. Run the Oracle Cloud Infrastructure CLI command to set up the kubeconfig file and save it in a location accessible to kubectl.

   For example, enter the following command (or copy and paste it from the **Access Your Cluster** dialog box) in the Cloud Shell window:

   ```bash
   oci ce cluster create-kubeconfig --cluster-id ocid1.cluster.oc1.phx.aaaaaaaaae... --file $HOME/.kube/config --region us-phoenix-1 --token-version 2.0.0
   ```

   where ocid1.cluster.oc1.phx.aaaaaaaaae... is the OCID of the current cluster. For convenience, the command in the **Access Your Cluster** dialog box already includes the cluster's OCID.

   Note that if a kubeconfig file already exists in the location you specify, details about the cluster will be added as a new context to the existing kubeconfig file. The current-context: element in the kubeconfig file will be set to point to the newly-added context.

   **Tip:**

   For clipboard operations in the Cloud Shell window, Windows users can use Ctrl-C or Ctrl-Insert to copy, and Shift-Insert to paste. For Mac OS users, use Cmd-C to copy and Cmd-V to paste.

8. If you don't save the kubeconfig file in the default location ($HOME/.kube) or with the default name (config), set the value of the KUBECONFIG environment variable to point to the name and location of the kubeconfig file. For example, enter the following command in the Cloud Shell window:

   ```bash
   export KUBECONFIG=$HOME/.kube/config
   ```

**Step 2: Verify that kubectl can access the cluster**

Verify that kubectl can connect to the cluster by entering the following command in the Cloud Shell window:

```bash
$ kubectl get nodes
```

Information about the nodes in the cluster is shown.

You can now use kubectl to perform operations on the cluster.

**Setting Up Local Access to Clusters**

To set up a kubeconfig file to enable access to a cluster using a local installation of kubectl:

**Step 1: Generate an API signing key pair**

If you already have an API signing key pair, go straight to the next step. If not:

1. Use OpenSSL commands to generate the key pair in the required PEM format. If you're using Windows, you'll need to install Git Bash for Windows and run the commands with that tool. See **How to Generate an API Signing Key** on page 4180.

2. Copy the contents of the public key to the clipboard (you'll need to paste the value into the Console later).
Step 2: Upload the public key of the API signing key pair

1. In the top-right corner of the Console, open the Profile menu () and then click User Settings to view the details.
2. Click Add Public Key.
3. Paste the public key's value into the window and click Add.


Step 3: Install and configure the Oracle Cloud Infrastructure CLI

1. Install the Oracle Cloud Infrastructure CLI version 2.6.4 (or later). See Quickstart on page 4195.
2. Configure the Oracle Cloud Infrastructure CLI. See Configuring the CLI on page 4202.

Step 4: Set up the kubeconfig file

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Kubernetes Clusters.
2. Choose a Compartment you have permission to work in.
3. On the Cluster List page, click the name of the cluster you want to access using kubectl. The Cluster page shows details of the cluster.
4. Click the Access Cluster button to display the Access Your Cluster dialog box.
5. Click Local Access.
6. Create a directory to contain the kubeconfig file. By default, the expected directory name is $HOME/.kube.

   For example, on Linux, enter the following command (or copy and paste it from the Access Your Cluster dialog box) in a local terminal window:

   ```bash
   mkdir -p $HOME/.kube
   ```

7. Run the Oracle Cloud Infrastructure CLI command to set up the kubeconfig file and save it in a location accessible to kubectl.

   For example, on Linux, enter the following command (or copy and paste it from the Access Your Cluster dialog box) in a local terminal window:

   ```bash
   oci ce cluster create-kubeconfig --cluster-id ocid1.cluster.oc1.phx.aaaaaaaaae... --file $HOME/.kube/config --region us-phoenix-1 --token-version 2.0.0
   ```

   where ocid1.cluster.oc1.phx.aaaaaaaaae... is the OCID of the current cluster. For convenience, the command in the Access Your Cluster dialog box already includes the cluster's OCID.

   Note that if a kubeconfig file already exists in the location you specify, details about the cluster will be added as a new context to the existing kubeconfig file. The current-context: element in the kubeconfig file will be set to point to the newly-added context.

8. If you don't save the kubeconfig file in the default location ($HOME/.kube) or with the default name (config), set the value of the KUBECONFIG environment variable to point to the name and location of the kubeconfig file.

   For example, on Linux, enter the following command (or copy and paste it from the Access Your Cluster dialog box) in a local terminal window:

   ```bash
   export KUBECONFIG=$HOME/.kube/config
   ```
**Step 5: Verify that kubectl can access the cluster**

1. Verify that kubectl is available by entering the following command in a local terminal window:

   ```
   kubectl version
   ```

   The response shows:
   - the version of kubectl installed and running locally
   - the version of Kubernetes (strictly speaking, the version of the kube-apiserver) running on the cluster's control plane nodes

   Note that the kubectl version must be within one minor version (older or newer) of the Kubernetes version running on the control plane nodes. If kubectl is more than one minor version older or newer, install an appropriate version of kubectl. See Kubernetes version and version skew support policy in the Kubernetes documentation.

   If the command returns an error indicating that kubectl is not available, install kubectl (see the kubectl documentation), and repeat this step.

2. Verify that kubectl can connect to the cluster by entering the following command in a local terminal window:

   ```
   kubectl get nodes
   ```

   Information about the nodes in the cluster is shown.

   You can now use kubectl to perform operations on the cluster.

**Notes about Kubeconfig Files**

Note the following about kubeconfig files:

- A single kubeconfig file can include the details for multiple clusters, as multiple contexts. The cluster on which operations will be performed is specified by the `current-context:` element in the kubeconfig file.
- A kubeconfig file includes an Oracle Cloud Infrastructure CLI command that dynamically generates an authentication token and inserts it when you run a kubectl command. The Oracle Cloud Infrastructure CLI must be available on your shell's executable path (for example, $PATH on Linux).
- The authentication tokens generated by the Oracle Cloud Infrastructure CLI command in the kubeconfig file are short-lived, cluster-scoped, and specific to individual users. As a result, you cannot share kubeconfig files between users to access Kubernetes clusters.
- The Oracle Cloud Infrastructure CLI command in the kubeconfig file uses your current CLI profile when generating an authentication token. If you have defined multiple profiles in different tenancies in the CLI configuration file (for example, in ~/.oci/config), specify which profile to use when generating the authentication token as follows. In both cases, `<profile-name>` is the name of the profile defined in the CLI configuration file:
  - Add `--profile` to the `args:` section of the kubeconfig file as follows:

    ```
    user:
    exec:
    apiVersion: client.authentication.k8s.io/v1beta1
    args:
    - ce
    - cluster
    - generate-token
    --cluster-id
    --profile
    - <cluster ocid>
    command: oci
    ```
• Set the OCI_CLI_PROFILE environment variable to the name of the profile defined in the CLI configuration file before running kubectl commands. For example:

```
export OCI_CLI_PROFILE=<profile-name>
```

```
kubectl get nodes
```

• The authentication tokens generated by the Oracle Cloud Infrastructure CLI command in the kubeconfig file are appropriate to authenticate individual users accessing the cluster using kubectl. However, the generated authentication tokens are unsuitable if you want other processes and tools to access the cluster, such as continuous integration and continuous delivery (CI/CD) tools. In this case, consider creating a Kubernetes service account and adding its associated authentication token to the kubeconfig file. For more information, see Adding a Service Account Authentication Token to a Kubeconfig File on page 894.

## Upgrading Kubeconfig Files from Version 1.0.0 to Version 2.0.0
Container Engine for Kubernetes currently supports kubeconfig version 2.0.0 files, and no longer supports kubeconfig version 1.0.0 files.

Enhancements in kubeconfig version 2.0.0 files provide security improvements for your Kubernetes environment, including short-lived cluster-scoped tokens with automated refreshing, and support for instance principals to access Kubernetes clusters. Additionally, authentication tokens are generated on-demand for each cluster, so kubeconfig version 2.0.0 files cannot be shared between users to access Kubernetes clusters (unlike kubeconfig version 1.0.0 files).

Note that kubeconfig version 2.0.0 files are not compatible with kubectl versions prior to version 1.11.9. If you are currently running kubectl version 1.10.x or older, upgrade kubectl to version 1.11.9 or later. For more information about compatibility between different versions of kubernetes and kubectl, see the Kubernetes documentation.

Follow the instructions below to determine the current version of kubeconfig files, and how to upgrade any remaining kubeconfig version 1.0.0 files to version 2.0.0.

### Determine the kubeconfig file version
To determine the version of a cluster's kubeconfig file:

1. In a terminal window (the Cloud Shell window or a local terminal window as appropriate), enter the following command to see the format of the kubeconfig file currently pointed at by the KUBECONFIG environment variable:

```
kubectl config view
```

2. If the kubeconfig file is version 1.0.0, you see a response in the following format:

```
users:
  - name: <username>
    user:
      token: <token-value>
```

If you see a response in the above format, you have to upgrade the kubeconfig file. See Upgrading Kubeconfig Files from Version 1.0.0 to Version 2.0.0 on page 880.

3. If the kubeconfig file is version 2.0.0, you see a response in the following format:

```
user:
  exec:
    apiVersion: client.authentication.k8s.io/v1beta1
    args:
      - ce
```
Upgrade a kubeconfig version 1.0.0 file to version 2.0.0

To upgrade a kubeconfig version 1.0.0 file:

1. In the case of a local installation of kubectl, confirm that Oracle Cloud Infrastructure CLI version 2.6.4 (or later) is installed by entering:
   
   ```
   oci -version
   ```

   If the Oracle Cloud Infrastructure CLI version is earlier than version 2.6.4, upgrade the CLI to a later version. See Upgrading the CLI on page 4220.

2. Follow the appropriate instructions to set up the kubeconfig file for use in Cloud Shell or locally (see Setting Up Cloud Shell Access to Clusters on page 876 or Setting Up Local Access to Clusters on page 877). Running the `oci ce cluster create-kubeconfig` command shown in the Access Your Cluster dialog box upgrades the existing kubeconfig version 1.0.0 file. If you change the name or location of the kubeconfig file, set the KUBECONFIG environment variable to point to the new name and location of the file.

3. Confirm the kubeconfig file is now version 2.0.0:
   
a. In a terminal window (the Cloud Shell window or a local terminal window as appropriate), enter:
   
   ```
   kubectl config view
   ```

   b. Confirm that that the response is in the following format:

   ```
   user:
   exec:
     apiVersion: client.authentication.k8s.io/v1beta1
     args:
       - ce
       - cluster
       - generate-token
       - --cluster-id
       - <cluster ocid>
     command: oci
   env: []
   ```

Modifying Kubernetes Cluster Properties

You can use Container Engine for Kubernetes to modify the properties of existing Kubernetes clusters.

You can change:

- the number of node pools in a cluster by adding new node pools, or deleting existing node pools
- the version of Kubernetes to run on control plane nodes
- the enforcement of pod security policies
- some properties of node pools and worker nodes (see Modifying Node Pool and Worker Node Properties on page 883)

However, note that you cannot change:

- the name of the cluster
- the master encryption key (if specified when the cluster was created)
Also note that you must not change the auto-generated names of resources that Container Engine for Kubernetes has created (such as the names of worker nodes).

**Using the Console**

To modify an existing Kubernetes cluster:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Cluster List** page, click the name of the cluster you want to modify.
4. Use the buttons across the top of the **Cluster** page as follows:
   - If you want to set up the kubeconfig configuration file for the cluster, click the **Access Cluster** button (see **Setting Up Cluster Access** on page 876).
   - If you want to delete the cluster along with its control plane nodes and worker nodes, click the **Delete Cluster** button.
   - If a newer version of Kubernetes is available than the one running on the control plane nodes in the cluster, the **Upgrade** button is enabled. If you want to upgrade the control plane nodes to a newer version, click **Upgrade** (see **Upgrading the Kubernetes Version on Control Plane Nodes in a Cluster** on page 930).
5. Use the **Cluster Details** tab to see information about the cluster, including:
   - The status of the cluster, and of the node pools in the cluster.
   - The cluster's OCID.
   - The Kubernetes version running on the control plane nodes in the cluster. If a newer version of Kubernetes is available than the one running on the control plane nodes in the cluster, the **Upgrade** link is shown. If you want to upgrade the control plane nodes to a newer version, click the **Upgrade** link (see **Upgrading the Kubernetes Version on Control Plane Nodes in a Cluster** on page 930).
   - The address of the Kubernetes endpoint.
   - Whether pod security policies are being enforced (by enabling the cluster's PodSecurityPolicy admission controller). Note that you must create pod security policies before enabling the PodSecurityPolicy admission controller of an existing cluster that is already in production. We also strongly recommend you first verify the cluster's pod security policies in a development or test environment. That way, you can be sure the pod security policies work as you expect and correctly allow (or refuse) pods to start on the cluster. Also note that if you disable a cluster's PodSecurityPolicy admission controller, any pod security policies (along with roles, rolebindings, clusterroles, and clusterrolebindings) you've defined are not deleted, they are simply not enforced. See **Using Pod Security Policies with Container Engine for Kubernetes** on page 905.
6. Use the **Node Pools** tab to:
   - View information about each of the node pools in the cluster, including:
     - The status of the node pool.
     - The node pool's OCID.
     - The configuration currently used when starting new worker nodes in the node pool, including the Kubernetes version, the shape, and the image.
     - The availability domains, and different regional subnets (recommended) or AD-specific subnets hosting worker nodes.
   
   Note that you can change some of these node pool and worker node properties (see **Modifying Node Pool and Worker Node Properties** on page 883).
   - Add a new node pool to the cluster by clicking the **Add Node Pool** button and entering details for the new node pool.
   - Delete a node pool by selecting **Delete Node Pool** from the **Actions** menu.
7. Use the **Quick Start** tab to:
   - Set up access to the cluster (see **Setting Up Cluster Access** on page 876).
   - Download and deploy a sample Nginx application using the Kubernetes command line tool kubectl from the instructions in a manifest file (see **Deploying a Sample Nginx App on a Cluster Using Kubectl** on page 896).

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the **Update Cluster** operation to modify an existing Kubernetes cluster.

**Modifying Node Pool and Worker Node Properties**

You can use Container Engine for Kubernetes to modify the properties of node pools and worker nodes in existing Kubernetes clusters.

You can change:
- the name of a node pool
- the version of Kubernetes to run on new worker nodes
- the number of worker nodes in a node pool, and the availability domains and subnets in which to place them
- the image to use for new worker nodes
- the shape to use for new worker nodes
- the boot volume size to use for new worker nodes
- the public SSH key to use to access new worker nodes

Note that you must not change the auto-generated names of resources that Container Engine for Kubernetes has created (such as the names of worker nodes).

Also note the following:
- Any changes you make to worker node properties will only apply to new worker nodes. You cannot change the properties of existing worker nodes.
- In some situations, you might want to update properties of all the worker nodes in a node pool simultaneously, rather than just the properties of new worker nodes that start in the node pool. For example, to upgrade all worker nodes to a new version of Oracle Linux. In this case, you can create a new node pool with worker nodes that have the required properties, and shift work from the original node pool to the new node pool using the `kubectl drain` command and pod disruption budgets. For more information, see **Updating Worker Nodes by Creating a New Node Pool** on page 885.
- If you use the **UpdateNodePool** API operation to modify properties of an existing node pool, be aware of the **Worker node properties out-of-sync with updated node pool properties** known issue and its workarounds.
- Do not use the `kubectl delete node` command to scale down or terminate worker nodes in a cluster that was created by Container Engine for Kubernetes. Instead, reduce the number of worker nodes by changing the corresponding node pool properties using the Console or the API. The `kubectl delete node` command does not change a node pool's properties, which determine the desired state (including the number of worker nodes). Also, although the `kubectl delete node` command removes the worker node from the cluster's etcd key-value store, the command does not delete the underlying compute instance.

**Using the Console**

To modify the properties of node pools and worker nodes of existing Kubernetes clusters:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Cluster List** page, click the name of the cluster you want to modify.
4. On the Cluster page, click the name of the node pool that you want to modify.
5. Use the Node Pool Details tab to view information about the node pool, including:
   • The status of the node pool.
   • The node pool's OCID.
   • The configuration currently used when starting new worker nodes in the node pool, including:
     • the version of Kubernetes to run on worker nodes
     • the shape to use for worker nodes
     • the image to use on worker nodes
   • The availability domains, and different regional subnets (recommended) or AD-specific subnets hosting worker nodes.
6. (optional) Change properties of the node pool and worker nodes by clicking Edit and specifying:
   • Name: A different name for the node pool. Avoid entering confidential information.
   • Version: A different version of Kubernetes to run on new worker nodes in the node pool when performing an in-place upgrade. The Kubernetes version on worker nodes must be either the same version as that on the control plane nodes, or an earlier version that is still compatible (see Kubernetes Versions and Container Engine for Kubernetes on page 926). To start new worker nodes running the Kubernetes version you specify, 'drain' existing worker nodes in the node pool (to prevent new pods starting and to delete existing pods) and then terminate each of the existing worker nodes in turn.
     You can also specify a different version of Kubernetes to run on new worker nodes by performing an out-of-place upgrade. For more information about upgrading worker nodes, see Upgrading the Kubernetes Version on Worker Nodes in a Cluster on page 930.
   • Image: A different image to use on the nodes in the node pool. An image is a template of a virtual hard drive that determines the operating system and other software for the node. See Supported Images (Including Custom Images) and Shapes for Worker Nodes on page 923.
   • Shape: A different shape to use for the nodes in the node pool. The shape determines the number of CPUs and the amount of memory allocated to each node. The list shows only those shapes available in your tenancy that are supported by Container Engine for Kubernetes. See Supported Images (Including Custom Images) and Shapes for Worker Nodes on page 923.
   • Boot Volume Size in GB: A different boot volume size for worker nodes. The default size of worker node boot volumes is determined from the image specified for worker nodes, but you can specify a custom boot volume size. If you do specify a custom boot volume size, it must be larger than the image's default boot volume size. The minimum and maximum sizes you can specify are 50 GB and 32 TB respectively (see Custom Boot Volume Sizes on page 610). If you change the boot volume size for worker nodes, consider extending the partition for the boot volume to take advantage of the larger size (see Extending the Partition for a Boot Volume on page 612).
   • Public SSH Key: (Optional) A different public key portion of the key pair you want to use for SSH access to the nodes in the node pool. The public key is installed on all worker nodes in the cluster. Note that if you don't specify a public SSH key, Container Engine for Kubernetes will provide one. However, since you won't have the corresponding private key, you will not have SSH access to the worker nodes. Note that you cannot use SSH to access directly any worker nodes in private subnets (see Connecting to Worker Nodes in Private Subnets Using SSH on page 905).
7. (optional) Change the number and placement of worker nodes in the node pool by clicking Scale and specifying:
   • the number of worker nodes you want in the node pool after the scale operation is complete
   • the availability domains in which to place the worker nodes
   • the regional subnets (recommended) or AD-specific subnets to host the worker nodes
8. Use the Nodes tab to see information about specific worker nodes in the node pool. Optionally edit the configuration details of a specific worker node by clicking the worker node's name.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use the `UpdateNodePool` operation to modify an existing node pool.

**Updating Worker Nodes by Creating a New Node Pool**

You can modify the properties of new worker nodes that start in an existing node pool (see Modifying Node Pool and Worker Node Properties on page 883). However, in some situations, you might want to update properties of all the worker nodes in a node pool simultaneously, rather than just the properties of new worker nodes that start in the node pool. For example, to upgrade all worker nodes to a new version of Oracle Linux.

In this case, you can create a new node pool with worker nodes that have the required properties, and shift work from the original node pool to the new node pool. Having 'drained' existing worker nodes in the original node pool to prevent new pods starting and to delete existing pods, you can then delete the original node pool.

To update the properties of all worker nodes in a node pool by creating a new node pool:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Cluster List** page, click the name of the cluster where you want to update worker node properties.
4. On the **Cluster** page, display the **Node Pools** tab, and then click **Add Node Pool** to create a new node pool and specify the required properties for its worker nodes.
5. If there are labels attached to worker nodes in the original node pool and those labels are used by selectors (for example, to determine the nodes on which to run pods), then use the `kubectl label nodes` command to attach the same labels to the new worker nodes in the new node pool. See Assigning Pods to Nodes in the Kubernetes documentation.
6. For each worker node in the original node pool, prevent new pods from starting and delete existing pods by entering `kubectl drain <node_name>` for each worker node.

For more information:
- about using `kubectl`, see Accessing a Cluster Using Kubectl on page 890
- about the `drain` command, see `drain` in the Kubernetes documentation

**Recommended:** Leverage pod disruption budgets as appropriate for your application to ensure that there's a sufficient number of replica pods running throughout the drain operation.

After all the worker nodes have been drained from the original node pool and pods are running on worker nodes in the new node pool, you can delete the original node pool.

7. On the **Cluster** page, display the **Node Pools** tab, and then select **Delete Node Pool** from the **Actions** menu beside the original node pool.

The original node pool and all its worker nodes are deleted.

**Deleting a Kubernetes Cluster**

You can delete a cluster along with its control plane nodes, worker nodes, and node pools.

Note the following:
- When you delete a cluster, no other resources created during the cluster creation process or associated with the cluster (such as VCNs, internet gateways, NAT gateways, route tables, security lists, load balancers, and block volumes) are deleted automatically. If you want to delete these resources, you have to do so manually.

Do not change the auto-generated names of worker nodes. If you do change the auto-generated name of a worker node and then delete the cluster, the renamed worker node is not deleted. You would have to delete the renamed worker node manually.
Using the Console

To delete a Kubernetes cluster using Container Engine for Kubernetes:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Cluster List** page, click the Delete icon beside the cluster to delete, and confirm that you want to delete it.

You can also delete a cluster using the **Delete Cluster** button on the **Cluster** page.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the **DeleteCluster** operation to delete a cluster.

Monitoring Clusters

Having created a cluster, you can monitor the overall status of the cluster itself, and the nodes and node pools within it.

In addition to monitoring the overall status of clusters, node pools, and nodes, you can monitor their health, capacity, and performance at a more granular level using **metrics**, **alarms**, and **notifications**. See Container Engine for Kubernetes Metrics on page 963.

Using the Console

To monitor a Kubernetes cluster:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.

The **Status** column on the **Cluster List** page shows a summary status for each individual cluster and its control plane nodes. Clusters can have one of the following statuses:

<table>
<thead>
<tr>
<th>Cluster Status</th>
<th>Explanation</th>
<th>Possible Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Creating</strong></td>
<td>Cluster is in the process of being created.</td>
<td>Application is being deployed.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Cluster is running normally.</td>
<td>Control plane nodes are running normally.</td>
</tr>
</tbody>
</table>
| **Failed**     | Cluster is not running due to an unrecoverable error. | Possible reasons:  
• a problem setting up load balancers  
• conflicts in networking ranges |
| **Deleting**   | Cluster is in the process of being deleted. Application no longer required, so resources in the process of being released. | Application no longer required, so resources in the process of being released. |
| **Deleted**    | Cluster has been deleted. Application no longer required, so resources have been released. | Application no longer required, so resources have been released. |
Cluster Status | Explanation | Possible Reason
--- | --- | ---
**Updating** | Version of Kubernetes on the control plane nodes is in the process of being upgraded. | A newly supported version of Kubernetes has become available.

Note that the cluster's summary status is not necessarily directly related to the status of node pools and nodes within the cluster.

3. On the **Cluster List** page, click the name of the cluster for which you want to see detailed status.
4. Display the cluster's **Metrics** tab to see more granular information about the health, capacity, and performance of the cluster. See Container Engine for Kubernetes Metrics on page 963.
5. Display the **Node Pools** tab to see the summary status of each node pool in the cluster.
6. On the **Node Pools** tab, click the name of a node pool for which you want to see detailed status.
7. Display the node pool's **Metrics** tab to see more granular information about the health, capacity, and performance of the node pool. See Container Engine for Kubernetes Metrics on page 963.
8. Display the **Nodes** tab to see the summary status of each worker node in the node pool.

Worker nodes can have one of the following statuses:

| Node Status | Explanation | Possible Reason |
| --- | --- | ---
**Creating** | Node is being created. | Compute instance in the process of being created. |
**Active** | Node is running normally. | Node is running normally. |
**Updating** | Node is in the process of being updated. | Container Engine for Kubernetes is performing an operation on the node. |
**Deleting** | Node is in the process of being deleted. | Application no longer required, so resources in the process of being released. |
**Deleted** | Node has been deleted. | Application no longer required, so resources have been released. |
**Inactive** | Node still exists, but is not running. | Compute resource has a status of Stopped, Stopping, or Down For Maintenance. |

9. Click **View Metrics** beside a worker node to see more granular information about the health, capacity, and performance of that node. See Container Engine for Kubernetes Metrics on page 963.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the **GetCluster** and **GetNodePool** operations to monitor the status of Kubernetes clusters.
Viewing Work Requests and Kubernetes API Server Audit Logs

It's often useful to understand the context behind activities happening in a cluster. For example, to perform compliance checks, to identify security anomalies, and to troubleshoot errors by identifying who did what and when.

You can view operations performed by Container Engine for Kubernetes and the Kubernetes API server as follows:

- You can use the **Work Requests** tab of the cluster's **Summary** page to view and manage operations performed on a particular cluster by Container Engine for Kubernetes.
- You can use the Oracle Cloud Infrastructure Audit service to view all operations performed by:
  - Container Engine for Kubernetes, which emits audit events whenever you perform actions on a cluster, such as create and delete.
  - The Kubernetes API server, which emits audit events whenever you use tools like kubectl to make administrative changes to a cluster, such as creating a service. Kubernetes API server audit events are shown in the Oracle Cloud Infrastructure Audit service for clusters running Kubernetes version 1.13.x (or later). Note that events are only shown from 15 July, 2020 onward.

Note that in addition to viewing operations as described in this topic, you can also monitor the health, capacity, and performance of Kubernetes clusters themselves using metrics, alarms, and notifications. See Container Engine for Kubernetes Metrics on page 963.

**Using the Console**

To view and manage operations performed by Container Engine for Kubernetes on a particular cluster:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Choose a **Compartment** you have permission to work in.
3. On the **Cluster List** page, click the name of the cluster for which you want to view and manage operations.
   - The **Cluster** page shows information about the cluster.
4. Display the **Work Requests** tab, showing the recent operations performed on the cluster.

To view operations performed by Container Engine for Kubernetes and the Kubernetes API server as log events in the Oracle Cloud Infrastructure Audit service:

1. In the Console, open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Audit**.
2. Choose a **Compartment** you have permission to work in.
3. Search and filter to show the operations you're interested in:
   - To view operations performed by Container Engine for Kubernetes, enter **ClustersAPI** in the **Keywords** field and click **Search**.
   - To view operations performed by the Kubernetes API server, enter **OKE API Server Admin Access** in the **Keywords** field and click **Search**.

   For more information about using the Oracle Cloud Infrastructure Audit service, see Viewing Audit Log Events on page 494.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the GetWorkRequest, DeleteWorkRequest, ListWorkRequestErrors, ListWorkRequestLogs, and ListWorkRequests operations to view and manage operations performed by Container Engine for Kubernetes.

**Viewing Application Logs on Worker Nodes**

Having created a cluster using Container Engine for Kubernetes, you can use Oracle Cloud Infrastructure Logging to view and search the logs of applications running on worker node compute instances in the cluster.
Before you can collect and parse the application logs using Oracle Cloud Infrastructure Logging:

- You must have already:
  - Enabled monitoring for worker node compute instances (see Enabling Monitoring for Compute Instances on page 783).
  - Installed the Oracle Cloud Agent software on worker node compute instances. The agent enables you to specify which logs to collect and how to parse them. The agent is installed by default on worker node compute instances. To confirm that the agent is already installed, see Verify Agent Installation on page 2623.
- You must have already:
  - Created a dynamic group with a rule that includes worker nodes in the cluster's node pools as target hosts (see About Dynamic Groups on page 2422 and Selecting Target Hosts with Dynamic Groups on page 2625). For example:
    
    ```java
    instance.compartment.id = 'ocid1.tenancy.oc1..<unique-id>'
    ```
  - Created a policy for the dynamic group with a policy statement to allow the target hosts in the dynamic group to push logs to Oracle Cloud Infrastructure Logging (see Selecting Target Hosts with Dynamic Groups on page 2625). For example:
    
    ```java
    allow dynamic group <dynamic-group-name> to use log-content in tenancy
    ```

Having completed the above prerequisites, you can then define custom logs and associated agent configurations to view application logs on worker node compute instances. For more information about custom logs and agent configurations, see Custom Logs on page 2619.

Note that in addition to viewing application logs on worker node compute instances, you can also:

- Monitor the overall status of the cluster itself, node pools, and nodes. See Monitoring Clusters on page 886.
- Monitor the health, capacity, and performance of clusters, node pools, and nodes at a more granular level using *metrics*, *alarms*, and *notifications*. See Container Engine for Kubernetes Metrics on page 963.

**Using the Console**

To define a new custom log object and an associated agent configuration to enable you to view and search the logs of applications running on a cluster's worker node compute instances:

1. Open the navigation menu. Under *Solutions and Platform*, go to *Logging*, and then click *Logs*.
2. Choose a *Compartment* you have permission to work in.
3. Click *Create custom log* to create a new custom log.
4. On the *Create custom log* page, specify:
   - **Custom Log Name**: A name of your choosing for the new custom log. Avoid entering confidential information.
   - **Compartment**: The compartment in which to create the new custom log.
   - **Log Group**: The log group in which to place the custom log. Optionally, click *Create New Group* to create a new log group (see Managing Logs and Log Groups on page 2577).
5. Click *Create custom log*.
   
   A new custom log is created, and the *Create agent configuration* page is displayed.

   For convenience, these instructions now describe how to create a new agent configuration associated with the new custom log (although you can create a new agent configuration later if you prefer).

6. On the *Create agent configuration* page, select *Create new configuration* and specify:
   - **Configuration Name**: A name of your choosing for the new agent configuration. Avoid entering confidential information.
   - **Compartment**: The compartment in which to create the new agent configuration.
7. In the **Agent configuration** panel on the **Create agent configuration** page, specify:

   • **Choose host groups**: One or more host groups, as follows:
      
      • **Group type**: Select **Dynamic group**.
      
      • **Group**: An existing dynamic group that includes worker nodes in the cluster's node pools as target hosts. The dynamic group you select must have permission to access the compartment you specified for the agent configuration, and must also allow target hosts to push logs to Oracle Cloud Infrastructure Logging.
      
      • **Configure log inputs**: One or more locations from which to obtain application logs as inputs to the custom log, as follows:
         
         • **Input type**: Select **Log path**.
         
         • **Input name**: A name of your choosing for the new log input.
         
         • **File paths**: The path to application logs on the worker node compute instance. For example, `/var/log/containers/*`

     The **Select log destination** options are pre-populated with the custom log details you specified previously.

8. Click **Create custom log** to create the agent configuration associated with the custom log.

To view and search the contents of a custom log created for an application running on a cluster's worker node compute instances:

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Logs**.
2. Click the name of the custom log that you want to view. You can sort log entries by age, and filter by time.
3. (Optional) Click **Explore with Log Search** to open the central logging **Search** page. You can apply filters, and explore and visualize the log data in different ways (see **Viewing Custom Logs in a Compute Instance** on page 2627).

### Accessing a Cluster Using Kubectl

You can use the Kubernetes command line tool kubectl to perform operations on a cluster you've created with Container Engine for Kubernetes. You can use the kubectl installation included in Cloud Shell, or you can use a local installation of kubectl. In both cases, before you can use kubectl to access a cluster, you have to specify the cluster on which to perform operations by setting up the cluster's kubeconfig file.

Note that an Oracle Cloud Infrastructure CLI command in the kubeconfig file generates authentication tokens that are short-lived, cluster-scoped, and specific to individual users. As a result, you cannot share kubeconfig files between users to access Kubernetes clusters. The generated authentication tokens are also unsuitable if you want other processes and tools to access the cluster, such as continuous integration and continuous delivery (CI/CD) tools. In this case, consider creating a Kubernetes service account and adding its associated authentication token to the kubeconfig file. For more information, see **Adding a Service Account Authentication Token to a Kubeconfig File** on page 894.

Note also that the version of kubectl you use must be compatible with the version of Kubernetes running on clusters created by Container Engine for Kubernetes. In the case of Cloud Shell, kubectl is regularly updated so it is always compatible with the versions of Kubernetes currently supported by Container Engine for Kubernetes. In the case of a local installation of kubectl, it is your responsibility to update kubectl regularly. For more information about compatibility between different versions of Kubernetes and kubectl, see the **Kubernetes documentation**.

### Accessing a Cluster Using kubectl in Cloud Shell

To access a cluster using kubectl in Cloud Shell:

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file for use in Cloud Shell, and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See **Setting Up Cloud Shell Access to Clusters** on page 876.
2. In the Cloud Shell window, enter `kubectl` followed by the command for the operation you want to perform on the cluster. For a list of available commands and options, see the **kubectl documentation**.

   Note that you must have the appropriate permissions to run the command you enter. See **About Access Control and Container Engine for Kubernetes** on page 920.
Accessing a Cluster Using kubectl Installed Locally

To access a cluster using kubectl installed locally:

1. If you haven't already done so, install kubectl (see the kubectl documentation).
2. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file for use locally, and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Local Access to Clusters on page 877.
3. In a local terminal window, enter `kubectl` followed by the command for the operation you want to perform on the cluster. For a list of available commands and options, see the kubectl documentation.

Note that you must have the appropriate permissions to run the command you enter. See About Access Control and Container Engine for Kubernetes on page 920.

Accessing a Cluster Using the Kubernetes Dashboard

The Kubernetes Dashboard is a web-based management interface that enables you to:

- deploy and edit containerized applications
- assess the status of containerized applications
- troubleshoot containerized applications

For more information about the Kubernetes Dashboard (sometimes called the Web UI or the Dashboard UI), see the Web UI (Dashboard) topic in the Kubernetes documentation.

The Kubernetes Dashboard is not deployed in clusters by default. However, you can deploy the Kubernetes Dashboard in clusters you create with Container Engine for Kubernetes in the following ways:

- To manually deploy the Kubernetes Dashboard on an existing cluster, see the Kubernetes documentation. When you follow the instructions to manually deploy the Kubernetes Dashboard, it is deployed in the `kube-dashboard` namespace (not the `kube-system` namespace). The URL to display a manually deployed Kubernetes Dashboard is:

  http://localhost:8001/api/v1/namespaces/kube-dashboard/services/
  https:kubernetes-dashboard:/proxy/#!/login

- To have Container Engine for Kubernetes automatically deploy the Kubernetes Dashboard during cluster creation, create the cluster using the API and set the isKubernetesDashboardEnabled attribute to true. When Container Engine for Kubernetes automatically deploys the Kubernetes Dashboard, it is deployed in the `kube-system` namespace. The URL to display an automatically deployed Kubernetes Dashboard is:

  http://localhost:8001/api/v1/namespaces/kube-system/services/
  https:kubernetes-dashboard:/proxy/#!/login

Note the following:

- You cannot run the Kubernetes Dashboard in Cloud Shell.
- You cannot use Container Engine for Kubernetes to deploy the Kubernetes Dashboard on existing clusters. You have to manually deploy the Kubernetes Dashboard on existing clusters.
- The commands to use to delete the Kubernetes Dashboard from a cluster will depend on the version of Kubernetes running on the cluster. See Notes about Deleting the Kubernetes Dashboard on page 893.
- An Oracle Cloud Infrastructure CLI command in the kubeconfig file generates authentication tokens that are short-lived, cluster-scoped, and specific to individual users. As a result, you cannot share kubeconfig files between users to access Kubernetes clusters. The generated authentication tokens are also unsuitable if you want other processes and tools to access the cluster, such as continuous integration and continuous delivery (CI/CD) tools. In this case, consider creating a Kubernetes service account and adding its associated authentication token to the kubeconfig file. For more information, see Adding a Service Account Authentication Token to a Kubeconfig File on page 894.
### Accessing a Cluster using the Kubernetes Dashboard

To access a cluster using the Kubernetes Dashboard:

1. If you haven’t already done so, follow the steps to set up the cluster’s kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. In a text editor, create a file (for example, called oke-admin-service-account.yaml) with the following content:

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: oke-admin
  namespace: kube-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: oke-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: oke-admin
  namespace: kube-system
```

The file defines an administrator service account and a clusterrolebinding, both called oke-admin.

3. Create the service account and the clusterrolebinding in the cluster by entering:

   ```
   kubectl apply -f <filename>
   ```

   where `<filename>` is the name of the file you created earlier. For example:

   ```
   kubectl apply -f oke-admin-service-account.yaml
   ```

   The output from the above command confirms the creation of the service account and the clusterrolebinding:

   ```
   serviceaccount "oke-admin" created
   clusterrolebinding.rbac.authorization.k8s.io "oke-admin" created
   ```

   You can now use the oke-admin service account to view and control the cluster, and to connect to the Kubernetes dashboard.

4. Obtain an authentication token for the oke-admin service account by entering:

   ```
   kubectl -n kube-system describe secret $(kubectl -n kube-system get secret | grep oke-admin | awk '{print $1}')
   ```

   The output from the above command includes an authentication token (a long alphanumeric string) as the value of the `token:` element, as shown below:

   ```
   Name:         oke-admin-token-gwbp2
   Namespace:    kube-system
   Labels:       <none>
   Annotations:  kubernetes.io/service-account.name: oke-admin
   kubernetes.io/service-account.uid: 3a7fcd8e-e123-11e9-81ca-0a580aed8570
   Type:         kubernetes.io/service-account-token
   ```
In the example above, eyJh________px1Q (abbreviated for readability) is the authentication token.

5. Copy the value of the token: element from the output. You will use this token to connect to the dashboard.

6. In a terminal window, enter `kubectl proxy` to make the Kubernetes Dashboard available.

7. Open a browser and go to the following URL to display the Kubernetes Dashboard that was deployed when cluster was created:

```
http://localhost:8001/api/v1/namespaces/kube-system/services/
https:kubernetes-dashboard:/proxy/#!/login
```

Note that if you followed the instructions in the Kubernetes documentation to manually deploy the Kubernetes Dashboard on an existing cluster, it is deployed in the `kube-dashboard` namespace rather than the `kube-system` namespace. As a result, the URL to display the manually deployed Kubernetes Dashboard is:

```
http://localhost:8001/api/v1/namespaces/kube-dashboard/services/
https:kubernetes-dashboard:/proxy/#!/login.
```

8. In the Kubernetes Dashboard, select **Token** and paste the value of the token: element you copied earlier into the **Token** field.

9. In the Kubernetes Dashboard, click **Sign In**, and then click **Overview** to see the applications deployed on the cluster.

### Notes about Deleting the Kubernetes Dashboard

If you want to delete the Kubernetes Dashboard from a cluster, the commands to use will depend on the version of Kubernetes running on the cluster:

- For clusters running Kubernetes versions prior to version 1.16.8, run the following kubectl commands to delete the Kubernetes Dashboard:

  ```
kubectl delete deployment kubernetes-dashboard -n kube-system
kubectl delete sa -n kube-system kubernetes-dashboard
kubectl delete svc -n kube-system kubernetes-dashboard
kubectl delete secret -n kube-system kubernetes-dashboard-cert
kubectl delete secret -n kube-system kubernetes-dashboard-key-holder
kubectl delete cm -n kube-system kubernetes-dashboard-settings
kubectl delete role -n kube-system kubernetes-dashboard-minimal
kubectl delete rolebinding -n kube-system kubernetes-dashboard-minimal
kubectl delete deploy -n kube-system kubernetes-dashboard
```

- For clusters running Kubernetes version 1.16.8 (or later), run the following kubectl commands to delete the Kubernetes Dashboard:

  ```
kubectl delete deployment kubernetes-dashboard -n kube-system
kubectl delete sa -n kube-system kubernetes-dashboard
kubectl delete svc -n kube-system kubernetes-dashboard
kubectl delete secret -n kube-system kubernetes-dashboard-cert
kubectl delete secret -n kube-system kubernetes-dashboard-csrf
kubectl delete secret -n kube-system kubernetes-dashboard-key-holder
kubectl delete cm -n kube-system kubernetes-dashboard-settings
kubectl delete role -n kube-system kubernetes-dashboard
kubectl delete rolebinding -n kube-system kubernetes-dashboard
kubectl delete clusterrole -n kube-system kubernetes-dashboard
kubectl delete clusterrolebinding -n kube-system kubernetes-dashboard
kubectl delete deploy -n kube-system kubernetes-dashboard
```
Adding a Service Account Authentication Token to a Kubeconfig File

When you set up the kubeconfig file for a cluster, by default it contains an Oracle Cloud Infrastructure CLI command to generate a short-lived, cluster-scoped, user-specific authentication token. The authentication token generated by the CLI command is appropriate to authenticate individual users accessing the cluster using kubectl and the Kubernetes Dashboard.

However, the generated authentication token is not appropriate to authenticate processes and tools accessing the cluster, such as continuous integration and continuous delivery (CI/CD) tools. To ensure access to the cluster, such tools require long-lived, non-user-specific authentication tokens.

One solution is to use a Kubernetes service account, as described in this topic. A service account has an associated service account authentication token, which is stored as a Kubernetes secret. Having created a service account, you bind it to a clusterrolebinding that has cluster administration permissions. You can then add the service account (and its service account authentication token) as a user definition in the kubeconfig file itself. Other tools can then use the service account authentication token when accessing the cluster.

Note that to run the commands in this topic, you must have the appropriate permissions. See About Access Control and Container Engine for Kubernetes on page 920.

To add a service account authentication token to a kubeconfig file:

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. In a terminal window, create a new service account in the kube-system namespace by entering the following kubectl command:

   ```
   kubectl -n kube-system create serviceaccount <service-account-name>
   ```

   For example, to create a service account called kubeconfig-sa, enter:

   ```
   kubectl -n kube-system create serviceaccount kubeconfig-sa
   ```

   The output from the above command confirms the creation of the service account. For example:

   ```
   serviceaccount/kubeconfig-sa created
   ```

   Note that creating the service account in the kube-system namespace is recommended good practice, and is assumed in the instructions in this topic. However, if you prefer, you can create the service account in another namespace to which you have access.

3. Create a new clusterrolebinding with cluster administration permissions and bind it to the service account you just created by entering the following kubectl command:

   ```
   kubectl create clusterrolebinding <binding-name> --clusterrole=cluster-admin --serviceaccount=kube-system:<service-account-name>
   ```

   For example, to create a clusterrolebinding called add-on-cluster-admin and bind it to the kubeconfig-sa service account, enter:

   ```
   kubectl create clusterrolebinding add-on-cluster-admin --clusterrole=cluster-admin --serviceaccount=kube-system:kubeconfig-sa
   ```

   The output from the above command confirms the creation of the clusterrolebinding. For example:

   ```
   clusterrolebinding.rbac.authorization.k8s.io/add-on-cluster-admin created
   ```
4. Obtain the name of the service account authentication token and assign its value to an environment variable by entering the following command (these instructions assume you specify TOKENNAME as the name of the environment variable):

```
TOKENNAME=`kubectl -n kube-system get serviceaccount/<service-account-name> -o jsonpath='{.secrets[0].name}'`
```

For example:

```
TOKENNAME=`kubectl -n kube-system get serviceaccount/kubeconfig-sa -o jsonpath='{.secrets[0].name}'`
```

5. Obtain the value of the service account authentication token and assign its value (decoded from base64) to an environment variable. These instructions assume you specify TOKEN as the name of the environment variable. The commands to enter depend on the operating system:

- To obtain the value of the service account authentication token in a MacOS, Linux, or Unix environment, enter the following command:

```
TOKEN=`kubectl -n kube-system get secret $TOKENNAME -o jsonpath='{.data.token}'| base64 --decode`
```

- To obtain the value of the service account authentication token in a Windows environment:
  a. Enter the following command:

```
kubectl -n kube-system get secret $TOKENNAME -o jsonpath='{.data.token}'
```
  b. Copy the output from the above command and paste it into a base64 decoder (for example, https://www.base64decode.org, https://www.base64decode.net, or similar).
  c. Copy the output from the base64 decoder.
  d. Enter the following command:

```
TOKEN=`[<base64-decoded-output>]`
```

where `<base64-decoded-output>` is the output you copied from the base64 decoder.

6. Add the service account (and its authentication token) as a new user definition in the kubeconfig file by entering the following kubectl command:

```
kubectl config set-credentials <service-account-name> --token=$TOKEN
```

The service account (and its authentication token) is added to the list of users defined in the kubeconfig file. For example, to add the kubeconfig-sa service account and its authentication token to the kubeconfig file, enter:

```
kubectl config set-credentials kubeconfig-sa --token=$TOKEN
```

The output from the above command confirms the service account has been added to the kubeconfig file. For example:

```
User "kubeconfig-sa" set.
```
7. Set the user specified in the kubeconfig file for the current context to be the new service account user you created, by entering the following kubectl command:

```
kubectl config set-context --current --user=<service-account-name>
```

For example:

```
kubectl config set-context --current --user=kubeconfig-sa
```

The output from the above command confirms the current context has been changed. For example:

```
Context "context-ctdiztdhezd" modified.
```

8. (Optional) To verify that authentication works as expected, run a kubectl command to confirm that the service account user can be successfully authenticated using the service account authentication token.

For example, if you have previously deployed a sample Nginx application on the cluster (see Deploying a Sample Nginx App on a Cluster Using Kubectl on page 896), enter the following command:

```
kubectl get pods
```

The output from the above command shows the pods running on the cluster. If the command runs successfully, the service account user in the kubeconfig file has been successfully authenticated using the service account authentication token.

9. Distribute the kubeconfig file as necessary to enable other processes and tools (such as continuous integration and continuous delivery (CI/CD) tools) to access the cluster.

```
Note:

If you subsequently want to remove access to the cluster from the service account, delete the Kubernetes secret containing the service account authentication token by entering the following command:

```
kubectl -n kube-system delete secret $TOKENNAME
```
```

Deploying a Sample Nginx App on a Cluster Using Kubectl

Having created a Kubernetes cluster using Container Engine for Kubernetes, you'll typically want to try it out by deploying an application on the nodes in the cluster. For convenience, the Quick Start tab (available from the Cluster page) makes it easy to view and copy the commands to:

- set up access to the cluster
- download and deploy a sample Nginx application using the Kubernetes command line tool kubectl from the instructions in a manifest file

To deploy the sample nginx application:

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. In a terminal window, deploy the sample Nginx application by entering:

```
kubectl create -f https://k8s.io/examples/application/deployment.yaml
```

```
Tip:

If the command fails to connect to https://k8s.io/examples/application/deployment.yaml, go to the url in a browser and
```

Oracle Cloud Infrastructure User Guide
download the manifest file `deployment.yaml` to a local directory.
Repeat the `kubectl create` command and specify the local location of the `deployment.yaml` file.

3. Confirm that the sample application has been deployed successfully by entering:

```
kubectl get pods
```

You can see the Nginx sample application has been deployed as two pods, on two nodes in the cluster.

### Pulling Images from Registry during Deployment

During the deployment of an application to a Kubernetes cluster, you'll typically want one or more images to be pulled from a Docker registry. In the application's manifest file you specify the images to pull, the registry to pull them from, and the credentials to use when pulling the images. The manifest file is commonly also referred to as a pod spec, or as a deployment.yaml file (although other filenames are allowed).

If you want the application to pull images that reside in Oracle Cloud Infrastructure Registry, you have to perform two steps:

- You have to use `kubectl` to create a Docker registry secret. The secret contains the Oracle Cloud Infrastructure credentials to use when pulling the image. When creating secrets, Oracle strongly recommends you use the latest version of `kubectl` (see the `kubectl` documentation).
- You have to specify the image to pull from Oracle Cloud Infrastructure Registry, including the repository location and the Docker registry secret to use, in the application's manifest file.

To create a Docker registry secret:

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. In a terminal window, enter:

```
kubectl create secret docker-registry <secret-name> --docker-server=<region-key>.ocir.io --docker-username='<tenancy-namespace>/<oci-username>' --docker-password='<oci-auth-token>' --docker-email='<email-address>'
```

where:

- `<secret-name>` is a name of your choice, that you will use in the manifest file to refer to the secret. For example, `ocirsecret`
- `<region-key>` is the key for the Oracle Cloud Infrastructure Registry region you're using. For example, `iad`. See Availability by Region on page 3508.
- `ocir.io` is the Oracle Cloud Infrastructure Registry name.
- `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy containing the repository from which the application is to pull the image (as shown on the Tenancy Information page). For example, the namespace of the acme-dev tenancy might be `ansh81vru1zp`. Note that for some older
tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, acme-dev).

- `<oci-username>` is the username to use when pulling the image. The username must have access to the tenancy specified by `<tenancy-name>`. For example, `jdoe@acme.com`. If your tenancy is federated with Oracle Identity Cloud Service, use the format `oracleidentitycloudservice/<username>`.
- `<oci-auth-token>` is the auth token of the user specified by `<oci-username>`. For example, `k\j64r{1sJSSF-;)K8`.
- `<email-address>` is an email address. An email address is required, but it doesn't matter what you specify. For example, `jdoe@acme.com`.

Note the use of single quotes around strings containing special characters.

For example, combining the previous examples, you might enter:

```bash
kubectl create secret docker-registry ocirsecret --docker-server=phx.ocir.io --docker-username='ansh81vru1zp/jdoe@acme.com' --docker-password='k\j64r{1sJSSF-;)K8' --docker-email='jdoe@acme.com'
```

Having created the Docker secret, you can now refer to it in the application manifest file.

To specify the image to pull from Oracle Cloud Infrastructure Registry, along with the Docker secret to use, during deployment of an application to a cluster:

1. Open the application's manifest file in a text editor.
2. Add the following sections to the manifest file:
   a. Add a `containers` section that specifies the name and location of the container you want to pull from Oracle Cloud Infrastructure Registry, along with other deployment details.
   b. Add an `imagePullSecrets` section to the manifest file that specifies the name of the Docker secret you created to access the Oracle Cloud Infrastructure Registry.

Here's an example of what the manifest might look like when you've added the `containers` and `imagePullSecrets` sections:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: ngnix-image
spec:
  containers:
  - name: ngnix
    image: phx.ocir.io/ansh81vru1zp/project01/ngnix-lb:latest
    imagePullPolicy: Always
    ports:
    - name: ngnix
      containerPort: 8080
      protocol: TCP
    imagePullSecrets:
    - name: ocirsecret
```

3. Save and close the manifest file.

**Supported Labels for Different Usecases**

Container Engine for Kubernetes uses a number of different labels when creating and managing clusters, including:

- `failure-domain.beta.kubernetes.io/zone` on page 899
- `oci.oraclecloud.com/fault-domain` on page 899
- `node.kubernetes.io/exclude-from-external-load-balancers` on page 900

For more information about Kubernetes labels, see the Kubernetes documentation.
Container Engine for Kubernetes automatically adds the `failure-domain.beta.kubernetes.io/zone` label to each worker node (compute instance) in a cluster, according to the availability domain in which it is placed.

An availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Availability domains are isolated from each other, fault tolerant, and very unlikely to fail simultaneously. See Regions and Availability Domains on page 180.

You can use the `failure-domain.beta.kubernetes.io/zone` label in different ways:

- You can use the `failure-domain.beta.kubernetes.io/zone` label (in conjunction with the `oci.oraclecloud.com/fault-domain` label) to constrain the worker nodes on which to run a pod, in the case of a cluster with worker nodes in multiple availability domains. Include the `failure-domain.beta.kubernetes.io/zone` label in the pod specification to specify the availability domain in which worker nodes must have been placed.
- You can use the `failure-domain.beta.kubernetes.io/zone` label to specify the availability domain and region to provision persistent volume claims on the Block Volume service when using the FlexVolume plugin. See Creating a Persistent Volume Claim on page 947.

When you specify a value for the `failure-domain.beta.kubernetes.io/zone` label, you must use the correct shortened version of the availability domain name in an Oracle Cloud Infrastructure region. In most cases, the shortened versions of availability domain names are in the format `<region-identifier>-<availability-domain-number>`. For example, `UK-LONDON-1-AD-1`, `UK-LONDON-1-AD-2`, `UK-LONDON-1-AD-3`, `AP-MELBOURNE-1-AD-1`, `ME-JEDDAH-1-AD-1`. To find out the region identifiers and availability domains to use, see Availability by Region on page 836.

Note that the shortened versions of availability domain names in the Ashburn and Phoenix regions are exceptions, as shown below:

- For the Phoenix region, shortened versions of availability domain names are in the format `PHX-AD-<availability-domain-number>`. For example, `PHX-AD-1`, `PHX-AD-2`, `PHX-AD-3`.

Container Engine for Kubernetes automatically adds the `oci.oraclecloud.com/fault-domain` label to each worker node (compute instance) in a cluster, according to the fault domain in which it is placed.

A fault domain is a grouping of hardware and infrastructure that is distinct from other fault domains in the same availability domain. Each availability domain has three fault domains (named FAULT-DOMAIN-1, FAULT-DOMAIN-2, FAULT-DOMAIN-3). Every compute instance is placed in a fault domain. See Fault Domains on page 182.

You can constrain the worker nodes on which to run a pod by including the `oci.oraclecloud.com/fault-domain` label in the pod specification. Use the `oci.oraclecloud.com/fault-domain` label to specify the fault domain in which worker nodes must have been placed.

You'll typically use the `oci.oraclecloud.com/fault-domain` label to achieve high availability when a cluster is located in a region with a single availability domain.

For example:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
    - name: nginx
```
If you apply the above example pod spec to a cluster, an nginx pod is only created if the cluster has worker nodes in FAULT-DOMAIN-3 in the availability domain. If the cluster only has worker nodes in FAULT-DOMAIN-1 or FAULT-DOMAIN-2, the pod is not created and remains in a pending status.

If a cluster has worker nodes in multiple availability domains, include both the failure-domain.beta.kubernetes.io/zone label and the oci.oraclecloud.com/fault-domain label in a pod specification to specify both the availability domain and the fault domain of the worker nodes on which to run the pod.

### node.kubernetes.io/exclude-from-external-load-balancers

Container Engine for Kubernetes automatically enables the ServiceNodeExclusion feature gate on the clusters it creates. With the ServiceNodeExclusion feature gate enabled on a cluster, you can add a label to particular worker nodes to exclude them from the list of backend servers in an Oracle Cloud Infrastructure load balancer backend set. The fewer worker nodes included in a backend set, the faster the load balancer can be updated.

To exclude a worker node from the list of backend servers in a backend set, add the node.kubernetes.io/exclude-from-external-load-balancers label to the node by entering:

```bash
tool label nodes <node-name> node.kubernetes.io/exclude-from-external-load-balancers=true
```

For example:

```bash
tool label nodes 10.0.1.2 node.kubernetes.io/exclude-from-external-load-balancers=true
```

Note that having added the label to a node, the node is excluded from the list of backend servers regardless of the value of the label. For example, even if you specify node.kubernetes.io/exclude-from-external-load-balancers label=false, the worker node is still excluded from the list of backend servers.

To remove the label from the node, enter:

```bash
tool label nodes <node-name> node.kubernetes.io/exclude-from-external-load-balancers=
```

### Encrypting Kubernetes Secrets at Rest in Etcd

The control plane nodes in a Kubernetes cluster store sensitive configuration data (such as authentication tokens, passwords, and SSH keys) as Kubernetes secret objects in etcd. Etcd is an open source distributed key-value store that Kubernetes uses for cluster coordination and state management. In the Kubernetes clusters created by Container Engine for Kubernetes, etcd writes and reads data to and from block storage volumes in the Oracle Cloud Infrastructure Block Volume service. Although the data in block storage volumes is encrypted, Kubernetes secrets at rest in etcd itself are not encrypted by default.

For additional security, when you create a new cluster you can specify that Kubernetes secrets at rest in etcd are to be encrypted using the Oracle Cloud Infrastructure Vault service (see Overview of Vault on page 3952). Before you can create a cluster where Kubernetes secrets are encrypted in the etcd key-value store, you have to:

- know the name and OCID of a suitable master encryption key in Vault
- create a dynamic group that includes all clusters in the compartment in which you are going to create the new cluster
- create a policy authorizing the dynamic group to use the master encryption key
Having created the cluster and specified that you want Kubernetes secrets at rest in the etcd key-value store to be encrypted, you can optionally restrict the use of the master encryption key by modifying the dynamic group to include just that cluster.

Note the following:

- You can only select the option to encrypt the Kubernetes secrets in the cluster's etcd key-value store when creating a new 'custom cluster'. You cannot encrypt Kubernetes secrets in the etcd key-value stores of existing 'custom clusters', or in the etcd key-value stores of 'quick clusters'.
- You can only select the option to encrypt Kubernetes secrets in the cluster's etcd key-value store if you specify Kubernetes version 1.13.x or later as the version of Kubernetes to run on the control plane nodes of the cluster.
- Policies must have been defined to authorize Container Engine for Kubernetes to use the master encryption key, and to authorize users to delegate key usage to Container Engine for Kubernetes in the first place. For more information, see Let a user group delegate key usage in a compartment and Let Block Volume, Object Storage, File Storage, and Container Engine for Kubernetes services encrypt and decrypt volumes, buckets, file systems, and Kubernetes secrets in Common Policies on page 2142.
- Policies must have been defined to authorize Container Engine for Kubernetes to use the master encryption key, and to authorize users to delegate key usage to Container Engine for Kubernetes in the first place. For more information, see Let a user group delegate key usage in a compartment and Let Block Volume, Object Storage, File Storage, and Container Engine for Kubernetes services encrypt and decrypt volumes, buckets, file systems, and Kubernetes secrets in Common Policies on page 2142.
- After you've specified a master encryption key for a new cluster and created the cluster, do not subsequently delete the master encryption key in the Vault service. As soon as you schedule a key for deletion in Vault, the Kubernetes secrets stored for the cluster in etcd become inaccessible. If you have already scheduled the key for deletion, it might still be in the Pending Deletion state. If that is the case, cancel the scheduled key deletion (see To cancel the deletion of a key on page 3966) to restore access to the Kubernetes secrets. If you allow the scheduled key deletion operation to complete and the master encryption key to be deleted, the Kubernetes secrets stored for the cluster in etcd are permanently inaccessible. As a result, cluster upgrades will fail. In this situation, you have no choice but to delete and recreate the cluster.

Master Encryption Keys in Other Tenancies

You can create a cluster in one tenancy that uses a master encryption key in a different tenancy. In this case, you have to write cross-tenancy policies to enable the cluster in its tenancy to access the master encryption key in the Vault service’s tenancy. Note that if you want to create a cluster and specify a master encryption key that’s in a different tenancy, you cannot use the Console to create the cluster.

For example, assume the cluster is in the ClusterTenancy, and the master encryption key is in the KeyTenancy. Users belonging to a group (OKEAdminGroup) in the ClusterTenancy have permissions to create clusters. A dynamic group (OKEAdminDynGroup) has been created in the cluster, with the rule ALL {resource.type = 'cluster', resource.compartment.id = 'ocid1.compartment.oc1..<unique_ID>'}, so all clusters created in the ClusterTenancy belong to the dynamic group.

In the root compartment of the KeyTenancy, the following policies:

- use the ClusterTenancy's OCID to map ClusterTenancy to the alias OKE_Tenancy
- use the OCIDs of OKEAdminGroup and OKEAdminDynGroup to map them to the aliases RemoteOKEAdminGroup and RemoteOKEClusterDynGroup respectively
- give RemoteOKEAdminGroup and RemoteOKEClusterDynGroup the ability to list, view, and perform cryptographic operations with a particular master key in the KeyTenancy

```sh
Define tenancy OKE_Tenancy as ocid1.tenancy.oc1..<unique_ID>
Define dynamic-group RemoteOKEClusterDynGroup as ocid1.dynamicgroup.oc1..<unique_ID>
Define group RemoteOKEAdminGroup as ocid1.group.oc1..<unique_ID>
Admit dynamic-group RemoteOKEClusterDynGroup of tenancy ClusterTenancy to use keys in tenancy where target.key.id = 'ocid1.key.oc1..<unique_ID>'
Admit group RemoteOKEAdminGroup of tenancy ClusterTenancy to use keys in tenancy where target.key.id = 'ocid1.key.oc1..<unique_ID>'
```

In the root compartment of the ClusterTenancy, the following policies:

- use the KeyTenancy's OCID to map KeyTenancy to the alias KMS_Tenancy
- give OKEAdminGroup and OKEAdminDynGroup the ability to use master keys in the KeyTenancy

```sh
Define tenancy KMS_Tenancy as ocid1.tenancy.oc1..<unique_ID>
Define dynamic-group RemoteOKEClusterDynGroup as ocid1.dynamicgroup.oc1..<unique_ID>
Define group RemoteOKEAdminGroup as ocid1.group.oc1..<unique_ID>
Admit dynamic-group RemoteOKEClusterDynGroup of tenancy ClusterTenancy to use keys in tenancy where target.key.id = 'ocid1.key.oc1..<unique_ID>'
Admit group RemoteOKEAdminGroup of tenancy ClusterTenancy to use keys in tenancy where target.key.id = 'ocid1.key.oc1..<unique_ID>'
```

In the root compartment of the ClusterTenancy, the following policies:

- use the KeyTenancy's OCID to map KeyTenancy to the alias KMS_Tenancy
- give OKEAdminGroup and OKEAdminDynGroup the ability to use master keys in the KeyTenancy
• allow OKEAdminDynGroup to use a specific master key obtained from the KeyTenancy in the ClusterTenancy

Define tenancy KMS_Tenancy as ocid1.tenancy.oc1..<unique_ID>
Endorse group OKEAdminGroup to use keys in tenancy KMS_Tenancy
Endorse dynamic-group OKEAdminDynGroup to use keys in tenancy KMS_Tenancy
Allow dynamic-group OKEAdminDynGroup to use keys in tenancy where target.key.id = 'ocid1.key.oc1..<unique_ID>'

See Accessing Object Storage Resources Across Tenancies on page 3503 for more examples of writing cross-tenancy policies.

Having entered the policies, you can now run a command similar to the following to create a cluster in the ClusterTenancy that uses the master key obtained from the KeyTenancy:

oci ce cluster create --name oke-with-cross-kms --kubernetes-version v1.16.8 --vcn-id ocid1.vcn.oc1.iad.<unique_ID> --service-lb-subnet-ids '["ocid1.subnet.oc1.iad.<unique_ID>"]' --compartment-id ocid1.compartment.oc1..<unique_ID> --kms-key-id ocid1.key.oc1.iad.<unique_ID>

Using the Console

To create a new 'custom cluster' where Kubernetes secrets are encrypted in the cluster's etcd key-value store:

1. Log in to the Console.
2. If you know the OCID of the master encryption key to use to encrypt Kubernetes secrets, go straight to the next step. Otherwise:
   • If a suitable master encryption key already exists in Vault but you're not sure of its OCID, follow the instructions in To view key details on page 3963 and make a note of the master encryption key's OCID.
   • If a suitable master encryption key does not already exist in Vault, follow the instructions in To create a new master encryption key on page 3963 to create one. Having created a new master encryption key, make a note of its OCID.
3. Create a new dynamic group containing all the clusters in the compartment in which you intend to create the new cluster:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Dynamic Groups.
   b. Follow the instructions in To create a dynamic group on page 2423, and give the dynamic group a name (for example, acme-oke-kms-dyn-grp).
   c. Enter a rule that includes all clusters in the compartment in the format:

\[
\text{ALL \{resource.type = 'cluster', resource.compartment.id = 'ocid1.compartment.oc1..<unique_ID>'\}}
\]

where <compartment-ocid> is the OCID of the compartment in which you intend to create the new cluster.

For example:

\[
\text{ALL \{resource.type = 'cluster', resource.compartment.id = 'ocid1.compartment.oc1..aaaaaaaa23______smwa'\}}
\]

d. Click Create Dynamic Group.

Having created a dynamic group that includes all clusters in the compartment, you can now create a policy to give the dynamic group access to the master encryption key in Vault.
4. Create a new policy to enable use of the master encryption key:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
   b. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acme-oke-kms-dyn-grp-policy).
   c. Enter a policy statement to give the dynamic group access to the master encryption key, in the format:

   
   ```allow dynamic-group <dynamic-group-name> to use keys in compartment <compartment-name> where target.key.id = '<key-OCID>'
   
   where:
   
   • <dynamic-group-name> is the name of the dynamic group you created earlier.
   • <compartment-name> is the name of the compartment containing the master encryption key.
   • <key-OCID> is the OCID of the master encryption key in Vault.
   
   For example:

   ```allow dynamic-group acme-oke-kms-dyn-grp to use keys in compartment acme-kms-key-compartment where target.key.id = 'ocid1.key.oct1.iad.annrl______trfg'
   
   d. Click Create to create the new policy.

5. Follow the instructions to create a new 'custom cluster' in Using the Console to create a 'Custom Cluster' with Explicitly Defined Settings on page 873, select the Encrypt Using Customer-Managed Keys option, and select:

   • Choose a Vault in <compartment-name>: The vault that contains the master encryption key, from the list of vaults in the specified compartment. By default, <compartment-name> is the compartment in which you are creating the cluster, but you can select a different compartment by clicking Change Compartment.
   
   • Choose a Key in <compartment-name>: The name of the master encryption key, from the list of keys in the specified compartment. By default, <compartment-name> is the compartment in which you are creating the cluster, but you can select a different compartment by clicking Change Compartment. Note that you cannot change the master encryption key after the cluster has been created.

6. (Optional) Having created the cluster, for additional security:
   a. Make a note of the OCID of the new cluster you just created.
   b. Restrict the use of the master encryption key by modifying the dynamic group rule you created earlier to explicitly specify the OCID of the new cluster, rather than all clusters in the compartment. For example:

   ```resource.id = 'ocid1.cluster.oct1.iad.aaaaaaaaaf______yg5q'
   
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225. Use the CreateCluster operation to create a cluster.

Connecting to Worker Nodes Using SSH

If you provided a public SSH key when creating the node pool in a cluster, the public key is installed on all worker nodes in the cluster. On UNIX and UNIX-like platforms (including Solaris and Linux), you can then connect through SSH to the worker nodes using the ssh utility (an SSH client) to perform administrative tasks.

Note the following instructions assume the UNIX machine you use to connect to the worker node:

• Has the ssh utility installed.
• Has access to the SSH private key file paired with the SSH public key that was specified when the cluster was created.
How to connect to worker nodes using SSH depends on whether you specified public or private subnets for the worker nodes when defining the node pools in the cluster.

### Connecting to Worker Nodes in Public Subnets Using SSH

Before you can connect to a worker node in a public subnet using SSH, you must define an ingress rule in the subnet's security list to allow SSH access. The ingress rule must allow access to port 22 on worker nodes from source 0.0.0.0/0 and any source port, as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Source CIDR</th>
<th>IP Protocol</th>
<th>Source Port Range</th>
<th>Dest. Port Range</th>
<th>Type and Code</th>
<th>Allows: and Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
<td>n/a</td>
<td>Allows: TCP traffic for ports: 22 SSH Remote Login Protocol Description: Enables SSH access.</td>
</tr>
</tbody>
</table>

To connect to a worker node in a public subnet through SSH from a UNIX machine using the ssh utility:

1. Find out the IP address of the worker node to which you want to connect. You can do this in a number of ways:
   - Using kubectl. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876. Then in a terminal window, enter `kubectl get nodes` to see the public IP addresses of worker nodes in node pools in the cluster.
   - Using the Console. In the Console, display the Cluster List page and then select the cluster to which the worker node belongs. On the Node Pools tab, click the name of the node pool to which the worker node belongs. On the Nodes tab, you see the public IP address of every worker node in the node pool.
   - Using the REST API. Use the ListNodePools operation to see the public IP addresses of worker nodes in a node pool.

2. In the terminal window, enter `ssh opc@<node_ip_address>` to connect to the worker node, where `<node_ip_address>` is the IP address of the worker node that you made a note of earlier. For example, you might enter `ssh opc@192.0.2.254`.

   Note that if the SSH private key is not stored in the file or in the path that the ssh utility expects (for example, the ssh utility might expect the private key to be stored in `~/.ssh/id_rsa`), you must explicitly specify the private key filename and location in one of two ways:
   - Use the `-i` option to specify the filename and location of the private key. For example, `ssh -i ~/.ssh/my_keys/my_host_key_filename opc@192.0.2.254`
   - Add the private key filename and location to an SSH configuration file, either the client configuration file (`~/.ssh/config`) if it exists, or the system-wide client configuration file (`/etc/ssh/ssh_config`). For example, you might add the following:

     ```
     Host 192.0.2.254
     IdentityFile ~/.ssh/my_keys/my_host_key_filename
     ```

For more about the ssh utility's configuration file, enter `man ssh_config`

Note also that permissions on the private key file must allow you read/write/execute access, but prevent other users from accessing the file. For example, to set appropriate permissions, you might enter `chmod 600 ~/.ssh/my_keys/my_host_key_filename`. If permissions are not set correctly and the private key file is accessible to other users, the ssh utility will simply ignore the private key file.
Connecting to Worker Nodes in Private Subnets Using SSH

Worker nodes in private subnets have private IP addresses only (they do not have public IP addresses). They can only be accessed by other resources inside the VCN. Oracle recommends using bastion hosts to control external access (such as SSH) to worker nodes in private subnets. A bastion host is in a public subnet, has a public IP address, and is accessible from the internet. For more information about bastion hosts, see the white paper Bastion Hosts: Protected Access for Virtual Cloud Networks.

Using Pod Security Policies with Container Engine for Kubernetes

You can control the operations that pods are allowed to perform on a cluster you have created with Container Engine for Kubernetes by setting up pod security policies for the cluster. Pod security policies are a way to ensure that pods meet security-related conditions before they can be accepted by a cluster. For example, you can use pod security policies to:

- limit the storage choices available to pods
- restrict the host networking and ports that pods can access
- prevent pods from running as the root user
- prevent pods from running in privileged mode

You can also use pod security policies to provide default values for pods, by 'mutating' the pod.

Having defined a pod security policy for a cluster, you have to authorize the requesting user or target pod's service account to use the policy. You do this by creating a role (or clusterrole) to access the pod security policy, and then creating a rolebinding (or clusterrolebinding) between the role (or clusterrole) and the requesting user or target pod's service account. For more information about roles, clusterroles, and bindings, see About Access Control and Container Engine for Kubernetes on page 920.

You specify whether a cluster enforces the pod security policies defined for it by enabling the cluster's PodSecurityPolicy admission controller. The PodSecurityPolicy admission controller acts on creation and modification of a pod and determines if the pod should be admitted to the cluster based on the requested security context in the pod spec and the cluster's pod security policies. If multiple pod security policies exist, the PodSecurityPolicy admission controller first compares the pod against non-mutating policies in alphabetical order and uses the first policy that successfully validates the pod. If no non-mutating pods validate the pod, the PodSecurityPolicy admission controller compares the pod against mutating policies in alphabetical order and uses the first policy that successfully validates the pod.

Caution:

Warning 1:

It is very important to note that when you enable a cluster's PodSecurityPolicy admission controller, no application pods can start on the cluster unless suitable pod security policies exist, along with roles (or clusterroles) and rolebindings (or clusterrolebindings) to associate pods with policies. You will not be able to run application pods on a cluster with an enabled PodSecurityPolicy admission controller unless these prerequisites are met.

We strongly recommend you use PodSecurityPolicy admission controllers as follows:

- Whenever you create a new cluster, enable the Pod Security Admission Controller.
- Immediately after creating a new cluster, create pod security policies, along with roles (or clusterroles) and rolebindings (or clusterrolebindings).

Warning 2:
You must create pod security policies before enabling the PodSecurityPolicy admission controller of an existing cluster that is already in production (that is, some time after you created it). If you decide to enable an existing cluster's PodSecurityPolicy admission controller, we strongly recommend you first verify the cluster's pod security policies in a development or test environment. That way, you can be sure the pod security policies work as you expect and correctly allow (or refuse) pods to start on the cluster.

When you enable the PodSecurityPolicy admission controller of a cluster you've created with Container Engine for Kubernetes, a pod security policy for Kubernetes system privileged pods is automatically created (along with the associated clusterrole and clusterrolebinding). This pod security policy, and the clusterrole and clusterrolebinding, enable the Kubernetes system pods to run. The pod security policy, clusterrole, and clusterrolebinding are defined in the kube-system.yaml file (see kube-system.yaml Reference on page 908).

Note that you can create pod security policies for a cluster before enabling the cluster's PodSecurityPolicy admission controller. Also note that you can disable a cluster's PodSecurityPolicy admission controller that was previously enabled. In this case, any previously created pod security policies, roles (or clusterroles), and rolebindings (or clusterrolebindings) are not deleted. The pod security policies are simply not enforced. Any application pod will be able to run on the cluster.

For more information about pod security policies and the PodSecurityPolicy admission controller, see the Kubernetes documentation.

Creating a Pod Security Policy for Application Pods

To create a pod security policy for application pods, create a role to access the pod security policy, and create a rolebinding to enable the application pods to use the pod security policy:

1. Create the pod security policy for application pods:

   **a.** Define and save the pod security policy in a file. For example, in `acme-app-psp.yaml`.

   For example, this policy (taken from the Kubernetes documentation) simply prevents the creation of privileged pods:

   ```yaml
   apiVersion: policy/v1beta1
   kind: PodSecurityPolicy
   metadata:
     name: acme-app-psp
   spec:
     privileged: false  # Don't allow privileged pods!
     # The rest fills in some required fields.
     seLinux:
       rule: RunAsAny
     supplementalGroups:
       rule: RunAsAny
     runAsUser:
       rule: RunAsAny
     fsGroup:
       rule: RunAsAny
     volumes:
       - '*'
   ```

   **b.** Enter the following command to create the pod security policy:

   ```bash
   kubectl create -f <filename>.yaml
   ```

   For example:

   ```bash
   kubectl create -f acme-app-psp.yaml
   ```
2. Create the role (or clusterrole) to access the pod security policy:
   a. Define and save a role (or clusterrole) in a file. For example, in `acme-app-psp-crole.yaml`.
      For example:

      ```yaml
      # Cluster role which grants access to the app pod security policy
      apiVersion: rbac.authorization.k8s.io/v1
      kind: ClusterRole
      metadata:
        name: acme-app-psp-crole
      rules:
        - apiGroups:
          - policy
          resourceNames:
            - acme-app-psp
          resources:
            - podsecuritypolicies
          verbs:
            - use
      
      b. Enter the following command to create the role (or clusterrole):

      ```bash
      kubectl create -f <filename>.yaml
      ```
      For example:

      ```bash
      kubectl create -f acme-app-psp-crole.yaml
      ```

3. Create the rolebinding (or clusterrolebinding) to authorize the application pods to use the pod security policy:
   a. Define and save the rolebinding (or clusterrolebinding) in a file. For example, in `acme-app-psp-crole-bind.yaml`.
      For example:

      ```yaml
      # Role binding which grants access to the app pod security policy
      apiVersion: rbac.authorization.k8s.io/v1
      kind: RoleBinding
      metadata:
        name: acme-app-psp-binding
        namespace: acme-namespace
      roleRef:
        apiGroup: rbac.authorization.k8s.io
        kind: ClusterRole
        name: acme-app-psp-crole
      subjects:
        # For all service accounts in acme-namespace
        - apiGroup: rbac.authorization.k8s.io
          kind: Group
          name: system:serviceaccounts:acme-namespace
      
      b. Enter the following command to create the rolebinding (or clusterrolebinding):

      ```bash
      kubectl create -f <filename>.yaml
      ```
      For example:

      ```bash
      kubectl create -f acme-app-psp-crole-bind.yaml
      ```
Having defined a pod security policy and authorized application pods to use it by creating a role and rolebinding (or a clusterrole and clusterrolebinding), enable the cluster's PodSecurityPolicy admission controller to enforce the pod security policy (if it's not enabled already).

**Using the Console to Enable the PodSecurityPolicy Admission Controller**

To enable the PodSecurityPolicy admission controller when creating new clusters using the Console:

1. **Log** in to the Console.
2. **Follow** the instructions to create a new 'custom cluster' in Using the Console to create a 'Custom Cluster' with Explicitly Defined Settings on page 873, click **Show Advanced Options**, and select the **Pod Security Policies - Enforced** option. This option enables the PodSecurityPolicy admission controller.

   No application pods will be accepted into the new cluster unless suitable pod security policies exist, along with roles (or clusterroles) and rolebindings (or clusterrolebindings) to associate pods with policies.
3. **Follow** the instructions to set the remaining cluster details, and click **Create Cluster** to create the new cluster.
4. **Follow** the instructions in Creating a Pod Security Policy for Application Pods on page 906 to create pod security policies for the PodSecurityPolicy admission controller to enforce when accepting pods into the new cluster.

To enable the PodSecurityPolicy admission controller in existing clusters using the Console:

1. **Follow** the instructions in Creating a Pod Security Policy for Application Pods on page 906 to create pod security policies for the PodSecurityPolicy admission controller to enforce when accepting pods into the existing cluster.

   We strongly recommend you first verify the pod security policies in a development or test environment. That way, you can be sure the pod security policies work as you expect and correctly allow (or refuse) pods to start on the cluster.
2. **In** the Console, open the navigation menu. Under **Solutions and Platform**, go to Developer Services and click Kubernetes Clusters.
3. **Choose** a Compartment you have permission to work in.
4. **On** the Cluster List page, click the name of the cluster you want to modify.
5. **On** the Cluster Details tab, click **Not Enforced** beside **Pod Security Policies**.
6. **In** the Pod Security Policies window, select **Enforced**.

   From now on, no new application pods will be accepted into the cluster unless suitable pod security policies exist, along with roles (or clusterroles) and rolebindings (or clusterrolebindings) to associate pods with policies. Note that any currently running pods will continue to run regardless.
7. **Click** Save Changes.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To enable the PodSecurityPolicy admission controller, use the:

- **CreateCluster** operation when creating new clusters
- **Update Cluster** operation when modifying existing clusters

**kube-system.yaml Reference**

The pod security policy, and the associated clusterrole and clusterrolebinding, for Kubernetes system privileged pods are automatically created when you enable a cluster's PodSecurityPolicy admission controller. These allow any pod in the kube-system namespace to run. They are created from definitions in the kube-system.yaml shown below:

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
```
metadata:
  annotations:
    # See https://kubernetes.io/docs/concepts/policy/pod-security-policy/
    # seccomp
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
  name: oke-privileged
spec:
  allowedCapabilities:
    - '*'
  allowPrivilegeEscalation: true
  fsGroup:
    rule: 'RunAsAny'
  hostIPC: true
  hostNetwork: true
  hostPID: true
  hostPorts:
    - min: 0
      max: 65535
  privileged: true
  readOnlyRootFilesystem: false
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  volumes:
    - '*'

---

# Cluster role which grants access to the privileged pod security policy
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: oke-privileged-psp
rules:
  - apiGroups:
      - policy
    resourceNames:
      - oke-privileged
    resources:
      - podsecuritypolicies
    verbs:
      - use

---

# Role binding for kube-system - allow kube-system service accounts - should take care of CNI i.e. flannel running in the kube-system namespace
# Assumes access to the kube-system is restricted
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: kube-system-psp
  namespace: kube-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: oke-privileged-psp
subjects:
  # For all service accounts in the kube-system namespace
  - apiGroup: rbac.authorization.k8s.io
    kind: Group
Autoscaling Kubernetes Clusters

You can automatically scale the clusters you create using Container Engine for Kubernetes to optimize resource usage.

To enable autoscaling, you can deploy the Kubernetes Metrics Server to collect resource metrics from each worker node in the cluster (see Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl on page 910).

Having deployed the Kubernetes Metrics Server, you can then use:

- the Kubernetes Horizontal Pod Autoscaler to adjust the number of pods in a deployment (see Using the Kubernetes Horizontal Pod Autoscaler on page 911)
- the Kubernetes Vertical Pod Autoscaler to adjust the resource requests and limits for containers running in a deployment's pods (see Using the Kubernetes Vertical Pod Autoscaler on page 915)

Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl

You can deploy the Kubernetes Metrics Server on clusters you create using Container Engine for Kubernetes to enable autoscaling.

The Kubernetes Metrics Server is a cluster-wide aggregator of resource usage data. The Kubernetes Metrics Server collects resource metrics from the kubelet running on each worker node and exposes them in the Kubernetes API server through the Kubernetes Metrics API. Other Kubernetes add-ons require the Kubernetes Metrics Server, including:

- the Horizontal Pod Autoscaler (see Using the Kubernetes Horizontal Pod Autoscaler on page 911)
- the Vertical Pod Autoscaler (see Using the Kubernetes Vertical Pod Autoscaler on page 915)

Note that the Kubernetes Metrics Server is not intended to be used for anything other than autoscaling. For example, it is not recommended that you use the Kubernetes Metrics Server to forward metrics to monitoring solutions, nor as a source of monitoring solution metrics. For more information, see the Kubernetes Metrics Server documentation.

To deploy the Kubernetes Metrics Server on a cluster you've created with Container Engine for Kubernetes:

1. If you haven't already done so, follow the steps to set up the cluster's kubectl configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.
2. If your Oracle Cloud Infrastructure user is a tenancy administrator or cluster administrator, skip the next step and go straight to the following step.
3. If your Oracle Cloud Infrastructure user is not a tenancy administrator or cluster administrator, ask a tenancy administrator or cluster administrator to grant your user the Kubernetes RBAC cluster-admin clusterrole on the cluster by entering:

   ```bash
   kubectl create clusterrolebinding <my-cluster-admin-binding> --clusterrole=cluster-admin --user=<user-OCID>
   ```

   For more information, see About Access Control and Container Engine for Kubernetes on page 920.
4. In a terminal window, deploy the Kubernetes Metrics Server by entering:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/download/<version-number>/components.yaml
```

where `<version-number>` is the Kubernetes Metrics Server version that you want to deploy. For example, v0.3.6.

Note that the Kubernetes Metrics Server is being actively developed, so the version number to specify will change over time. To find out the currently available versions, see the Kubernetes Metrics Server documentation.

**Tip:**

If the command fails to connect to https://github.com/kubernetes-sigs/metrics-server/releases/download/<version-number>/components.yaml, go to the url in a browser and download the manifest file components.yaml to a local directory. Repeat the `kubectl apply` command and specify the local location of the components.yaml file.

5. Confirm that the Kubernetes Metrics Server has been deployed successfully and is available by entering:

```
kubectl get deployment metrics-server -n kube-system
```

**Using the Kubernetes Horizontal Pod Autoscaler**

You can use the Kubernetes Horizontal Pod Autoscaler to automatically scale the number of pods in a deployment, replication controller, replica set, or stateful set, based on that resource's CPU or memory utilization, or on other metrics. The Horizontal Pod Autoscaler can help applications scale out to meet increased demand, or scale in when resources are no longer needed. You can set a target metric percentage for the Horizontal Pod Autoscaler to meet when scaling applications. For more information, see Horizontal Pod Autoscaler in the Kubernetes documentation.

The Horizontal Pod Autoscaler is a standard API resource in Kubernetes that requires the installation of a metrics source, such as the Kubernetes Metrics Server, in the cluster. For more information, see Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl on page 910.

**Notes about the Horizontal Pod Autoscaler**

Note the following:

- The Kubernetes Metrics Server only supports scaling based on CPU and memory utilization. Other implementations of the Kubernetes Metrics API support scaling based on custom metrics. Refer to the Kubernetes documentation for a list of alternative implementations (see Implementations), and for more information about scaling based on custom metrics (see Autoscaling on multiple metrics and custom metrics).
- You can scale applications manually by updating manifest files, without using the Horizontal Pod Autoscaler.

**Working with the Horizontal Pod Autoscaler**

The instructions below are based on the Horizontal Pod Autoscaler Walkthrough topic in the Kubernetes documentation. They describe how to:

- Verify that the Kubernetes Metrics Server has been installed on a cluster.
- Deploy a sample php-apache web server.
- Create a Horizontal Pod Autoscaler resource that will scale based on CPU utilization.
- Start generation of a sample load.
- View the scaling operation in action.
- Stop the sample load generation.
- Clean up, by removing the php-apache web server and the Horizontal Pod Autoscaler.
Step 1: Verify the Kubernetes Metrics Server Installation

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. Confirm that the Kubernetes Metrics Server has been deployed successfully on the cluster and is available by entering:

   kubectl -n kube-system get deployment/metrics-server

   If the command returns a ‘Not Found’ error, then you must deploy the Kubernetes Metrics Server on the cluster before proceeding. See Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl on page 910.

Step 2: Deploy a Sample Application

Deploy a simple Apache web server application by entering:

   kubectl apply -f https://k8s.io/examples/application/php-apache.yaml

The output from the above command confirms the deployment:

   deployment.apps/php-apache created
   service/php-apache created

The Apache web server pod that is created from the manifest file:

- Has a 500m CPU limit, which ensures the container will never use more than 500 millicores, or 1/2 of a core.
- Has a 200m CPU request allowance, which allows the container to use 200 millicores of CPU resources, or 1/5 of a core.

Step 3: Create a Horizontal Pod Autoscaler Resource

1. Create a Horizontal Pod Autoscaler resource to maintain a minimum of 1 and a maximum of 10 replicas, and an average CPU utilization of 50%, by entering:

   kubectl autoscale deployment php-apache --cpu-percent=50 --min=1 --max=10

   The output from the above command confirms the Horizontal Pod Autoscaler has been created.

   horizontalpodautoscaler.autoscaling/php-apache autoscaled

   The command creates a Horizontal Pod Autoscaler for the Apache web server deployment that:

   - Maintains a minimum of 1 and a maximum of 10 replicas of the previously created pods controlled by the Apache web server deployment.
   - Increases and decreases the number of replicas of the deployment to maintain an average CPU utilization of 50% across all pods.

   If the average CPU utilization falls below 50%, the Horizontal Pod Autoscaler tries to reduce the number of pods in the deployment to the minimum (in this case, 1). If the average CPU utilization goes above 50 percent, the Horizontal Pod Autoscaler tries to increase the number of pods in the deployment to the maximum (in this case, 10). For more information, see How does the Horizontal Pod Autoscaler work? in the Kubernetes documentation.

   For more information about the kubectl autoscale command, see autoscale in the Kubernetes documentation.
2. After a minute, confirm the current status of the Horizontal Pod Autoscaler by entering:

```bash
kubectl get hpa
```

The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>REFERENCE</th>
<th>TARGETS MINPODS MAXPODS REPLICAS AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>Deployment/php-apache</td>
<td>0%/50%  1 10 1 10s</td>
</tr>
</tbody>
</table>

The `TARGETS` column shows the average CPU utilization across all pods controlled by the Apache web server deployment. Since no requests are being sent to the server, the above example shows the current CPU utilization is 0%, compared to the target utilization of 50%. Note that you might see different numbers, depending on how long you wait before running the command.

**Step 4: Start Sample Load Generation**

1. Run a container with a busybox image to create a load for the Apache web server by entering:

```bash
kubectl run -it --rm load-generator --image=busybox /bin/sh --
generator=run-pod/v1
```

2. Generate a load for the Apache web server that will cause the Horizontal Pod Autoscaler to scale out the deployment by entering:

```bash
while true; do wget -q -O- http://php-apache; done
```

**Step 5: View the Scaling Operation**

1. After a minute, open a new terminal window and confirm the current status of the Horizontal Pod Autoscaler by entering:

```bash
kubectl get hpa
```

The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>REFERENCE</th>
<th>TARGETS MINPODS MAXPODS REPLICAS AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>Deployment/php-apache</td>
<td>250%/50%  1 10 1 1m</td>
</tr>
</tbody>
</table>

In the above example, you can see the current CPU utilization has increased to 250%, compared to the target utilization of 50%. Note that you might see different numbers, depending on how long you wait before running the command.

To achieve the utilization target of 50%, the Horizontal Pod Autoscaler will have to increase the number of replicas to scale out the deployment.

2. After another few minutes, view the increased number of replicas by re-entering:

```bash
kubectl get hpa
```

The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>REFERENCE</th>
<th>TARGETS MINPODS MAXPODS REPLICAS AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>Deployment/php-apache</td>
<td>50%/50%  1 10 5 5m</td>
</tr>
</tbody>
</table>

In the above example, you can see that the Horizontal Pod Autoscaler has resized the deployment to 5 replicas, and the utilization target of 50% has been achieved. Note that you might see different numbers, depending on how long you wait before running the command.
3. Verify the deployment has been scaled out by entering:

    kubectl get deployment php-apache

The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>5/5</td>
<td>5</td>
<td>5</td>
<td>5m</td>
</tr>
</tbody>
</table>

Note that you might see different numbers, depending on how long you wait before running the command.

**Step 6: Stop Sample Load Generation**

1. In the terminal window where you created the container with the busybox image and generated the load for the Apache web server:
   a. Terminate the load generation by pressing Ctrl+C
   b. Close the command prompt by entering:

       exit

   The output from the above command confirms the session has ended:

   Session ended, resume using 'kubectl attach load-generator -c load-generator -i -t' command when the pod is running
   pod "load-generator" deleted

2. After a minute, confirm the current status of the Horizontal Pod Autoscaler by entering:

    kubectl get hpa

The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>REFERENCE</th>
<th>TARGETS</th>
<th>MINPODS</th>
<th>MAXPODS</th>
<th>REPLICAS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>Deployment/php-apache</td>
<td>0%/50%</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>10m</td>
</tr>
</tbody>
</table>

In the above example, you can see the current CPU utilization has reduced to 0%, compared to the target utilization of 50%. However, there are still 5 replicas in the deployment. Note that you might see different numbers, depending on how long you wait before running the command.

3. After another few minutes, view the reduced number of replicas by re-entering:

    kubectl get hpa

The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>REFERENCE</th>
<th>TARGETS</th>
<th>MINPODS</th>
<th>MAXPODS</th>
<th>REPLICAS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>Deployment/php-apache</td>
<td>0%/50%</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>15m</td>
</tr>
</tbody>
</table>

In the above example, you can see that the Horizontal Pod Autoscaler has resized the deployment to 1 replica.

Be aware that it will take time for the replica count to reduce to 1. Five minutes is the default timeframe for scaling in. Note that you might see different numbers, depending on how long you wait before running the command.
4. Verify the deployment has been scaled in by entering:

   ```bash
   kubectl get deployment php-apache
   ```

   The output from the above command shows the current status:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-apache</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>15m</td>
</tr>
</tbody>
</table>

   Note that you might see different numbers, depending on how long you wait before running the command.

**Step 7: Clean Up**

1. Delete the Horizontal Pod Autoscaler by entering:

   ```bash
   kubectl delete horizontalpodautoscaler.autoscaling/php-apache
   ```

   Note that when you delete a Horizontal Pod Autoscaler, the number of replicas remains the same. A deployment does not automatically revert back to the state it had prior to the creation of the Horizontal Pod Autoscaler.

2. Delete the Apache web server deployment by entering:

   ```bash
   kubectl delete deployment.apps/php-apache service/php-apache
   ```

**Using the Kubernetes Vertical Pod Autoscaler**

You can use the Kubernetes Vertical Pod Autoscaler to automatically adjust the resource requests and limits for containers running in a deployment's pods. The Vertical Pod Autoscaler can improve cluster resource utilization by:

- Setting the requests automatically based on usage to make sure the appropriate resource amount is available for each pod.
- Maintaining ratios between limits and requests that were specified in containers' initial configurations.
- Scaling down pods that are over-requesting resources, based on their usage over time.
- Scaling up pods that are under-requesting resources, based on their usage over time.

The Vertical Pod Autoscaler has three components:

- **Recommender**: Monitors the current and past resource consumption and provides recommended CPU and memory request values for a container.
- **Updater**: Checks for pods with incorrect resources and deletes them, so that the pods can be recreated with the updated request values.
- **Admission Plugin**: Sets the correct resource requests on new pods (that is, pods just created or recreated by their controller due to changes made by the Updater).

For more information, see [Vertical Pod Autoscaler](https://kubernetes.io/docs/concepts/workloads/pods/vpa/) and [Managing Resources for Containers](https://kubernetes.io/docs/concepts/workloads/pods/resource/) in the Kubernetes documentation.

You configure the Vertical Pod Autoscaler using the `VerticalPodAutoscaler` custom resource definition object. The `VerticalPodAutoscaler` object enables you to specify the pods to vertically autoscale, and which resource recommendations to apply (if any). For more information, see [VerticalPodAutoscaler](https://kubernetes.io/docs/concepts/workloads/pods/vpa/) and [Custom Resource Definition object](https://kubernetes.io/docs/concepts/extend-kubernetes/api-extension/custom-resources/) in the Kubernetes documentation.

The Vertical Pod Autoscaler requires the installation of a metrics source, such as the Kubernetes Metrics Server, in the cluster. For more information, see [Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl](https://kubernetes.io/docs/tasks/administer-cluster/deploy/metrics-server/) on page 910.

**Overriding Limit Ranges**

The Vertical Pod Autoscaler attempts to make recommendations within the minimum and maximum values specified by a limit range, if one has been defined. However, if the applicable limit range conflicts with the values specified in
the resourcePolicy section of the VerticalPodAutoscaler manifest, the Vertical Pod Autoscaler gives priority to the resource policy and makes recommendations accordingly (even if the values fall outside the limit range). For more information, see Limit Ranges and Resource Policy Overriding Limit Range in the Kubernetes documentation.

Creating Recommendations without Applying them

You can use the Vertical Pod Autoscaler to create and apply recommendations, or simply to create recommendations (without updating pods). To simply create recommendations without applying them, set updateMode: "Off" in the updatePolicy section of the VerticalPodAutoscaler manifest.

When pods are created, the Vertical Pod Autoscaler analyzes the CPU and memory needs of the containers and records those recommendations in its Status field. The Vertical Pod Autoscaler does not take any action to update the resource requests for the running containers.

Excluding Specific Containers

You can use the Vertical Pod Autoscaler to create and apply recommendations to all the containers in a pod, or you can selectively exclude particular containers. To turn off recommendations for a particular container, in the resourcePolicy section of the VerticalPodAutoscaler manifest, specify a containerName and set mode: "Off" in the containerPolicies section.

Notes about the Vertical Pod Autoscaler

Note the following:

• Currently, you are recommended not to use the Vertical Pod Autoscaler with the Horizontal Pod Autoscaler on CPU or memory utilization metrics. However, note that you can use the Vertical Pod Autoscaler with the Horizontal Pod Autoscaler on custom and external metrics. See Support for custom metrics in the Kubernetes documentation.

• The Vertical Pod Autoscaler recommendations might exceed available resources (for example, node size, available size, available quota). Note that applying the recommendations might cause pods to go into a pending status.

• Whenever the Vertical Pod Autoscaler updates pod resources, the pod is recreated, which causes all running containers to be restarted. Note that the pod might be recreated on a different node.

Working with the Vertical Pod Autoscaler

The instructions below walk you through deploying the Vertical Pod Autoscaler on a cluster. They describe how to:

• Verify that the Kubernetes Metrics Server has been installed on a cluster.
• Download and deploy the Vertical Pod Autoscaler.
• Deploy a sample application.
• View the scaling operation in action.
• View the recommendation.
• Clean up, by removing the sample application and the Vertical Pod Autoscaler.

Step 1: Verify the Kubernetes Metrics Server Installation

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.
2. Confirm that the Kubernetes Metrics Server has been deployed successfully on the cluster and is available by entering:

```
kubectl -n kube-system get deployment/metrics-server
```

If the command returns a `Not Found` error, then you must deploy the Kubernetes Metrics Server on the cluster before proceeding. See Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl on page 910.

**Step 2: Download and Deploy the Vertical Pod Autoscaler**

1. Download the Vertical Pod Autoscaler source code from GitHub. For example, by entering:

```
git clone -b vpa-release-0.8 https://github.com/kubernetes/autoscaler.git
```
2. Change to the `vertical-pod-autoscaler` directory:

```
cd autoscaler/vertical-pod-autoscaler
```
3. If you have previously deployed the Vertical Pod Autoscaler, delete it by entering:

```
./hack/vpa-down.sh
```
4. Deploy the Vertical Pod Autoscaler by entering:

```
./hack/vpa-up.sh
```
5. Verify that the Vertical Pod Autoscaler pods have been created successfully by entering:

```
kubectl get pods -n kube-system
```

The output from the above command shows the pods:

```
vpa-admission-controller-59d9965cfb-bzs8l 1/1 Running 0 6m34s
vpa-recommender-5bcb58569-mqdds 1/1 Running 0 6m43s
vpa-updater-5979cbf757-scw2d 1/1 Running 0 6m46s
```

Note that you will probably see different names and numbers.

**Step 3: Deploy the Sample Application**

1. Deploy the sample hamster application to create a deployment and a corresponding Vertical Pod Autoscaler by entering:

```
kubectl apply -f examples/hamster.yaml
```

The output from the above command confirms the deployment and creation:

```
verticalpodautoscaler.autoscaling.k8s.io/hamster-vpa created
deployment.apps/hamster created
```

Deploying the hamster application creates a deployment with two pods and a Vertical Pod Autoscaler pointing at the deployment.
2. Verify that the hamster pods have been created successfully by entering:

```
kubectl get pods -l app=hamster
```

The output from the above command confirms the creation:

```
NAME                     READY STATUS  RESTARTS AGE
hamster-7cbfd64f57-mqqnk 1/1   Running 0 54s
```
Note that you will probably see different names for the hamster pods.

3. View the CPU and memory reservations using the `kubectl describe pod` command and one of the hamster pod names returned in the previous step. For example:

```
kubectl describe pod hamster-7cbfd64f57-rq6wv
```

Note that the above command is an example only. You must use one of the hamster pod names that was returned when you ran the `kubectl get pods -l app=hamster` command in the previous step.

In the requests section of the output, you can see the pod's current CPU and memory reservations. For example:

```
Requests:
cpu:        100m
memory:     50Mi
```

The Vertical Pod Autoscaler (specifically, the Recommender) analyzes the pods and observes their behavior to determine whether these CPU and memory reservations are appropriate. Note that you might see different CPU and memory reservations.

The reservations are not sufficient because the sample hamster application is deliberately under-resourced. Each pod runs a single container that:

- requests 100 millicores, but tries to utilize more than 500 millicores
- reserves much less memory than it needs to run

### Step 4: View the Scaling Operation

Having analyzed the original pods in the sample hamster application and determined that the CPU and memory reservations are inadequate, the Vertical Pod Autoscaler (specifically the Updater) relaunches the pods with different values as proposed by the Recommender. Note that the Vertical Pod Autoscaler does not modify the template in the deployment, but updates the actual requests of the pods.

1. Monitor the pods in the sample hamster application, and wait for the Updater to start a new hamster pod with a new name, by entering:

```
kubectl get --watch pods -l app=hamster
```

2. When you see that a new hamster pod has started, view its CPU and memory reservations using the `kubectl describe pod` command and the pod's name. For example:

```
kubectl describe pod hamster-7cbfd64f57-wmg4
```

In the requests section of the output, you can see the new pod's CPU and memory reservations:

```
Requests:
cpu:        587m
memory:     262144k
```

In the above example, notice that the CPU reservation has increased to 587 millicores and the memory reservation has increased to 262,144 Kilobytes. The original pod was under-resourced and the Vertical Pod Autoscaler has corrected the original reservations with more appropriate values. Note that you might see different CPU and memory reservations.
Step 5: View the Recommendation

View the recommendations made by the Vertical Pod Autoscaler (specifically, by the Recommender) by entering:

```
kubectl describe vpa/hamster-vpa
```

The output from the above command shows the recommendations:

```yaml
Name:         hamster-vpa
Namespace:    default
Labels:       <none>
Annotations:  kubectl.kubernetes.io/last-applied-configuration:
               {
                 "apiVersion": "autoscaling.k8s.io/v1beta2",
                 "kind": "VerticalPodAutoscaler",
                 "metadata": {
                   "annotations": {},
                   "name": "hamster-vpa",
                   "namespace": "default"
               }
API Version:  autoscaling.k8s.io/v1
Kind:         VerticalPodAutoscaler
Metadata:
   Creation Timestamp:  2020-09-22T18:08:09Z
   Generation:          27
   Resource Version:    19466955
   Self Link:           /apis/autoscaling.k8s.io/v1/namespaces/default/verticalpodautoscalers/hamster-vpa
   UID:                 689cee90-6fed-404d-adf9-b6fa8c1da660
Spec:
   Resource Policy:
     Container Policies:
       Container Name:  *
       Controlled Resources:
       cpu
       memory
       Max Allowed:
       Cpu:     1
       Memory:  500Mi
       Min Allowed:
       Cpu:     100m
       Memory:  50Mi
   Target Ref:
     API Version:  apps/v1
     Kind:         Deployment
     Name:         hamster
   Update Policy:
     Update Mode:  Auto
Status:
   Conditions:
     Last Transition Time:  2020-09-22T18:10:10Z
     Status:                True
     Type:                  RecommendationProvided
   Recommendation:
     Container Recommendations:
       Container Name:  hamster
       Lower Bound:
       Cpu:     519m
       Memory:  262144k
     Target:
       Cpu:     587m
       Memory:  262144k
     Uncapped Target:
       Cpu:     587m
       Memory:  262144k
     Upper Bound:
       Cpu:     1
       Memory:  500Mi
```
Note that you might see different recommendations.

**Step 6: Clean Up**

1. Remove the sample application by entering:

   ```bash
   kubectl delete -f examples/hamster.yaml
   ```

2. In the `vertical-pod-autoscaler` directory, delete the Vertical Pod Autoscaler deployment by entering:

   ```bash
   ./hack/vpa-down.sh
   ```

**About Access Control and Container Engine for Kubernetes**

To perform operations on a Kubernetes cluster, you must have appropriate permissions to access the cluster.

For most operations on Kubernetes clusters created and managed by Container Engine for Kubernetes, Oracle Cloud Infrastructure Identity and Access Management (IAM) provides access control. A user's permissions to access clusters comes from the groups to which they belong. The permissions for a group are defined by policies. Policies define what actions members of a group can perform, and in which compartments. Users can then access clusters and perform operations based on the policies set for the groups they are members of.

IAM provides control over:

- whether a user can create or delete clusters
- whether a user can add, remove, or modify node pools
- which Kubernetes object create/delete/view operations a user can perform on all clusters within a compartment or tenancy

See [Policy Configuration for Cluster Creation and Deployment](#) on page 868.

In addition to IAM, the Kubernetes RBAC Authorizer can enforce additional fine-grained access control for users on specific clusters via Kubernetes RBAC roles and clusterroles. A Kubernetes RBAC role is a collection of permissions. For example, a role might include read permission on pods and list permission for pods. A Kubernetes RBAC clusterrole is just like a role, but can be used anywhere in the cluster. A Kubernetes RBAC rolebinding maps a role to a user or set of users, granting that role's permissions to those users for resources in that namespace. Similarly, a Kubernetes RBAC clusterrolebinding maps a clusterrole to a user or set of users, granting that clusterrole's permissions to those users across the entire cluster.

IAM and the Kubernetes RBAC Authorizer work together to enable users who have been successfully authorized by at least one of them to complete the requested Kubernetes operation.

When a user attempts to perform any operation on a cluster (except for create role and create clusterrole operations), IAM first determines whether the group to which the user belongs has the appropriate and sufficient permissions. If so, the operation succeeds. If the attempted operation also requires additional permissions granted via a Kubernetes RBAC role or clusterrole, the Kubernetes RBAC Authorizer then determines whether the user has been granted the appropriate Kubernetes role or clusterrole.

Typically, you'll want to define your own Kubernetes RBAC roles and clusterroles when deploying a Kubernetes cluster to provide additional fine-grained control. When you attempt to perform a create role or create clusterrole operation, the Kubernetes RBAC Authorizer first determines whether you have sufficient Kubernetes privileges. To create a role or clusterrole, you must have been assigned an existing Kubernetes RBAC role (or clusterrole) that has at least the same or higher privileges as the new role (or clusterrole) you're attempting to create.

By default, users are not assigned any Kubernetes RBAC roles (or clusterroles) by default. So before attempting to create a new role (or clusterrole), you must be assigned an appropriately privileged role (or clusterrole). A number of such roles and clusterroles are always created by default, including the cluster-admin clusterrole (for a full list, see [Default Roles and Role Bindings](#) in the Kubernetes documentation). The cluster-admin clusterrole essentially confers
super-user privileges. A user granted the cluster-admin clusterrole can perform any operation across all namespaces in a given cluster.

Note that Oracle Cloud Infrastructure tenancy administrators already have sufficient privileges, and do not require the cluster-admin clusterrole.

**Example: Granting the Kubernetes RBAC cluster-admin clusterrole**

**Note:**

The following instructions assume:

- You have the required access to create Kubernetes RBAC roles and clusterroles, either because you're in the tenancy's Administrators group, or because you have the Kubernetes RBAC cluster-admin clusterrole.
- The user to which you want to grant the RBAC cluster-admin clusterrole is not an OCI tenancy administrator. If they are an OCI tenancy administrator, they do not require the Kubernetes RBAC cluster-admin clusterrole.

Follow these steps to grant a user who is not a tenancy administrator the Kubernetes RBAC cluster-admin clusterrole on a cluster deployed on Oracle Cloud Infrastructure:

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. In a terminal window, grant the Kubernetes RBAC cluster-admin clusterrole to the user by entering:

   ```
   kubectl create clusterrolebinding <my-cluster-admin-binding> --clusterrole=cluster-admin --user=<user_OCID>
   ```

   where:

   - `<my-cluster-admin-binding>` is a string of your choice to be used as the name for the binding between the user and the Kubernetes RBAC cluster-admin clusterrole. For example, `jdoe_clst_adm`
   - `<user_OCID>` is the user's OCID (obtained from the Console). For example, `ocid1.user.oc1..aaaaa...zutq` (abbreviated for readability).

   For example:

   ```
   kubectl create clusterrolebinding jdoe_clst_adm --clusterrole=cluster-admin --user=ocid1.user.oc1..aaaaa...zutq
   ```

**Example: Giving a developer user the ability to read pods in a new cluster**

**Note:**

The following instructions assume you're in the tenancy's Administrators group, and therefore have:

- the required permissions to create clusters, and to manage users and groups
- the required access to create Kubernetes RBAC roles and clusterroles

Follow these steps to give a developer the necessary Oracle Cloud Infrastructure and Kubernetes RBAC permissions to use kubectl to view pods running on a cluster deployed on Oracle Cloud Infrastructure:
1. Create a new Oracle Cloud Infrastructure user for the developer to use (for example, called jdoe@acme.com), and make a note of the new user's OCID (for example, ocid1.user.oc1..aaaaa...tx5a, abbreviated for readability). See To create a user on page 2417.

2. Create a new Oracle Cloud Infrastructure group and add the new user to the group (for example, called acme-dev-pod-vwr). See To create a group on page 2420.

3. Create a new Oracle Cloud Infrastructure policy that grants the new group the CLUSTER_USE permission on clusters, with a policy statement like:

   Allow group acme-dev-pod-vwr to use clusters in <location>

   In the above policy statement, replace <location> with either tenancy (if you are creating the policy in the tenancy's root compartment) or compartment <compartment-name> (if you are creating the policy in an individual compartment).

   See To create a policy on page 2454.


5. Follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

6. In a text editor, create a file (for example, called role-pod-reader.yaml) with the following content. This file defines a Kubernetes RBAC role that enables users to read pod details.

   kind: Role
   apiVersion: rbac.authorization.k8s.io/v1
   metadata:
     namespace: default
     name: pod-reader
   rules:
   - apiGroups: ["" ] # "" indicates the core API group
     resources: ["pods"]
     verbs: ["get", "watch", "list"]

7. In a terminal window, create the new role in the cluster using kubectl. For example, if you gave the yaml file that defines the new role the name role-pod-reader.yaml, enter the following:

   kubectl create -f role-pod-reader.yaml

8. In a terminal window, bind the Kubernetes RBAC role you just created to the Oracle Cloud Infrastructure user account you created earlier by entering the following to create a new rolebinding (in this case, called pod-reader-binding):

   kubectl create rolebinding pod-reader-binding --role=pod-reader --user=ocid1.user.oc1..aaaaa...tx5a

9. Give the developer the credentials of the new Oracle Cloud Infrastructure user you created earlier, and tell the developer they can now see details of pods running on the cluster deployed on Oracle Cloud Infrastructure by:

   • Signing in to the Console using the new user's credentials.
   • Following the instructions in Setting Up Cluster Access on page 876 to set up their own copy of the cluster's kubeconfig file. If the file does not have the expected default name and location of $HOME/.kube/config, the developer will also have to set the KUBECONFIG environment variable to point to the file. Note that the developer must set up their own kubeconfig file. They cannot access a cluster using a kubeconfig file that you (or a different user) set up.
   • Using kubectl to see details of the pods by entering:

   kubectl get pods
Supported Images (Including Custom Images) and Shapes for Worker Nodes

When creating a cluster using Container Engine for Kubernetes, you can customize the worker nodes in the cluster by specifying:

- The operating system image to use for worker nodes. The image is a template of a virtual hard drive that determines the operating system and other software for the worker node.
- The shape to use for worker nodes. The shape is the number of CPUs and the amount of memory to allocate to each newly created compute instance to be used as a worker node.

This topic includes information about the images and shapes provided by Oracle Cloud Infrastructure that are supported by Container Engine for Kubernetes for use in node pools. Note that some of the shapes might not be available in your particular tenancy.

To see a list of the supported images and the shapes available in your tenancy, enter:

```
oci ce node-pool-options get --node-pool-option-id all
```

Supported Images

Container Engine for Kubernetes supports the provisioning of worker nodes using some, but not all, of the latest Oracle Linux images provided by Oracle Cloud Infrastructure.

To see the images supported by Container Engine for Kubernetes:

- When using the Console to create a 'custom cluster', view the list of values in the Image drop-down menu to see the list of supported images.
- When using the CLI, view the supported images (in the data: sources: section of the response) by entering:

```
oci ce node-pool-options get --node-pool-option-id all
```

Custom Images

When specifying the image that Container Engine for Kubernetes uses to provision worker nodes in a node pool, you can specify your own custom image rather than one of the explicitly supported Oracle Linux images returned by the `oci ce node-pool-options get --node-pool-option-id all` command. Worker nodes provisioned from a custom image include the customizations, configuration, and software that were present when the image was created. Note that Container Engine for Kubernetes only supports custom images that are based on one of the Oracle Linux images returned by the `oci ce node-pool-options get` command.

To provision worker nodes from a custom image, you must use the CLI or API and specify the custom image’s OCID when creating the node pool. For example, by running the `oci ce node-pool create` command and using the `--node-image-id` parameter to specify a custom image's OCID, as follows:

```
oci ce node-pool create \
--cluster-id ocid1.cluster.oc1.iad.aaaaaaaaaf______jrd \
--name my-custom-linux-image \
--node-image-id ocid1.image.oc1.iad.aaaaaaaa6______nha \
--compartment-id ocid1.compartment.oc1..aaaaaaaay______t6q \
--kubernetes-version v1.15.7 \
--node-shape VM.Standard2.1 \
--placement-configs "[ { "availabilityDomain": "nFuS:US-ASHBURN-AD-1", \
"subnetId": "ocid1subnet.oc1.iad.aaaaaaa3______a6q" } ]" \
--size 1 \
--region=us-ashburn-1
```

Note the following additional considerations when using custom images:

- Container Engine for Kubernetes installs Kubernetes on top of a custom image, and Kubernetes or the installation software might change certain kernel configurations.
- Custom images must have access to a yum repository (public or internal).
• Custom images must not use a customized cloud-init. You can perform post-provisioning customization using
SSH or Daemonset.
• For the best support, ensure you create a custom image from the most up-to-date base image.

For more information about custom images and Oracle Cloud Infrastructure, see Managing Custom Images on page 665.

**Supported Shapes**

Container Engine for Kubernetes supports the provisioning of worker nodes using many, but not all, of the shapes
provided by Oracle Cloud Infrastructure. More specifically:

• **Supported:** Flexible shapes; Bare Metal shapes, including standard shapes; HPC shapes, except in
  RDMA networks; VM shapes, including standard shapes; Dense I/O shapes.

• **Not Supported:** Dedicated VM host shapes; GPU shapes on VMs and Bare Metal instances; Micro VM shapes;
  HPC shapes on Bare Metal instances in RDMA networks.

Note that you might be unable to select some shapes in your particular tenancy due to service limits and compartment
quotas, even though those shapes are supported by Container Engine for Kubernetes.

To see the shapes that are supported by Container Engine for Kubernetes and available in your tenancy:

• When using the Console to create a 'custom cluster', view the list of values in the **Shape** drop-down menu to see
  the list of supported shapes.

• When using the CLI, view the supported shapes (in the **data: shapes:** section of the response) by entering:

  ```
  oci ce node-pool-options get --node-pool-option-id all
  ```

You might be able to use the Compute service's Console pages (or the Compute service's CLI or API) to subsequently
change the shape of a worker node after it has been created. However, bear in mind that Container Engine for
Kubernetes only supports those shapes shown in the **Shape** drop-down menu or returned by the `oci ce node-
pool-options get --node-pool-option-id all` command.

For more information about all the shapes provided by Oracle Cloud Infrastructure, see Compute Shapes on page 655.

**Supported Admission Controllers**

The Kubernetes version you select when you create a cluster using Container Engine for Kubernetes determines the
default set of admission controllers that are turned on in the created cluster. The set follows the recommendation
given in the Kubernetes documentation for that version. This topic shows the supported admission controllers, the
Kubernetes versions in which they are supported, and the order in which they run in the Kubernetes API server.

**Admission Controllers (sorted alphabetically)**

The table lists, in alphabetical order, the admission controllers that are turned on in the Kubernetes clusters you create
using Container Engine for Kubernetes. For each admission controller, the table shows the Kubernetes version in
which it is supported.

<table>
<thead>
<tr>
<th>Admission Controllers (in alphabetical order)</th>
<th>Supported in 1.16?</th>
<th>Supported in 1.17?</th>
<th>Supported in 1.18?</th>
</tr>
</thead>
<tbody>
<tr>
<td>DefaultIngressClass</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DefaultStorageClass</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DefaultValueTolerationSeconds</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ExtendedResourceTolerationSeconds</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LimitRanger</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MutatingAdmissionWebhook</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Admission Controllers (in alphabetical order)</td>
<td>Supported in 1.16?</td>
<td>Supported in 1.17?</td>
<td>Supported in 1.18?</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>NamespaceLifecycle</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NodeRestriction</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PersistentVolumeClaimResize</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PodSecurityPolicy (optional, see Using Pod Security Polices with Container Engine for Kubernetes)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Priority</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ResourceQuota</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RuntimeClass</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ServiceAccount</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>StorageObjectInUseProtection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TaintNodesByCondition</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ValidatingAdmissionWebhook</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Supported Admission Controllers (sorted by run order)

The table lists the admission controllers that are turned on in the Kubernetes clusters you create using Container Engine for Kubernetes. The table shows the order in which supported admission controllers run in the Kubernetes API server. Note that the run order is different in different Kubernetes versions.
Kubernetes Versions and Container Engine for Kubernetes

When you create a new Kubernetes cluster using Container Engine for Kubernetes, you specify:

- The version of Kubernetes to run on the control plane nodes in the cluster.
- The version of Kubernetes to run on the worker nodes in each node pool. Different worker nodes in the same node pool can run different versions of Kubernetes. Different node pools in a cluster can run different versions of Kubernetes.

The version of Kubernetes that you specify for the worker nodes in a node pool must be either the same Kubernetes version as that running on the control plane nodes, or an earlier Kubernetes version that is still compatible. In other words:

- The control plane nodes in a new cluster must run the same version of Kubernetes as the version running on worker nodes, or must be no more than two versions ahead.
- The worker nodes in a node pool must not run a more recent version of Kubernetes than the associated control plane nodes.

New Versions of Kubernetes

New Kubernetes versions are released periodically that contain new features and bug fixes. Kubernetes version numbers have the format x.y.z where x is a major release, y is a minor release, and z is a patch release. For example, 1.18.10.

Kubernetes itself is supported for three minor versions at a time (the current release version and two previous versions).

As described in the Kubernetes documentation, a certain amount of version variation is permissible between control plane nodes and worker nodes in a cluster:

- The Kubernetes version on worker nodes can lag behind the version on the control plane nodes by up to two versions, but no more. If the version on the worker nodes is more than two versions behind the version on the control plane nodes, the Kubernetes versions on the worker nodes and the control plane nodes are incompatible.
- The Kubernetes version on worker nodes must never be more recent than the version on the control plane nodes.

For the Kubernetes versions currently and previously supported by Container Engine for Kubernetes, see Supported Versions of Kubernetes on page 926.

Supported Versions of Kubernetes

When Container Engine for Kubernetes support for a new version of Kubernetes is announced, an older Kubernetes version ceases to be supported.

This topic lists:

- Kubernetes Versions Supported by Container Engine for Kubernetes on page 926
- Kubernetes Versions Previously Supported by Container Engine for Kubernetes on page 928

Kubernetes Versions Supported by Container Engine for Kubernetes

Container Engine for Kubernetes supports the following versions of Kubernetes:
<table>
<thead>
<tr>
<th>Kubernetes Version</th>
<th>Supported by Container Engine for Kubernetes?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.18.10</td>
<td>Yes</td>
<td>Support introduced: 1 December, 2020</td>
</tr>
<tr>
<td>1.17.13</td>
<td>Yes</td>
<td>Support for 1.17.x versions (initially 1.17.9) introduced: 3 November, 2020</td>
</tr>
<tr>
<td>1.16.15</td>
<td>Yes</td>
<td>Support for 1.16.x versions (initially 1.16.8) introduced: 22 June, 2020 See Notes about Container Engine for Kubernetes Support for Kubernetes Version 1.16 on page 927</td>
</tr>
</tbody>
</table>

**Notes about Container Engine for Kubernetes Support for Kubernetes Version 1.16**

Note that Kubernetes version 1.16 deprecates:

- A number of versions of the following Kubernetes APIs, in favor of more stable versions (as described in this [kubernetes.io blog post](#)):
  - NetworkPolicy
  - PodSecurityPolicy
  - DaemonSet
  - Deployment
  - StatefulSet
  - ReplicaSet

If a deprecated API version is used, workloads running on Kubernetes version 1.16 clusters are subject to disruption.

- Any labels in the k8s.io and kubernetes.io namespaces, except for the following:
  - kubernetes.io/hostname
  - kubernetes.io/instance-type
  - kubernetes.io/os
  - kubernetes.io/arch
  - beta.kubernetes.io/instance-type
  - beta.kubernetes.io/os
  - beta.kubernetes.io/arch
  - failure-domain.beta.kubernetes.io/zone
  - failure-domain.beta.kubernetes.io/region
  - failure-domain.kubernetes.io/zone
  - failure-domain.kubernetes.io/region
  - [*.]kubelet.kubernetes.io/*
  - [*.]node.kubernetes.io/*

If a disallowed label is used, errors occur when creating or updating node pools in Kubernetes version 1.16 clusters.

Before upgrading clusters to Kubernetes version 1.16, Oracle strongly recommends you prepare as follows:
Container Engine for Kubernetes

- Migrate to the stable API versions as soon as possible. Container Engine for Kubernetes already supports Kubernetes versions that support the stable API versions, so you can do this immediately. Depending on your use of the Kubernetes APIs, your migration tasks might include:
  - changing manifest files to reference the stable API versions
  - updating custom integrations and controllers to call the stable API versions
  - updating third party tools (ingress controllers, continuous delivery systems) to call stable API versions
  - verifying your version of kubectl adheres to the Kubernetes version skew support policy described in the Kubernetes documentation
  - making sure any references to documented Kubernetes examples are using stable API versions
- Update the Kubernetes labels in the k8s.io and kubernetes.io namespaces to just the following:
  - kubernetes.io/hostname
  - kubernetes.io/instance-type
  - kubernetes.io/os
  - kubernetes.io/arch
  - beta.kubernetes.io/instance-type
  - beta.kubernetes.io/os
  - beta.kubernetes.io/arch
  - failure-domain.beta.kubernetes.io/zone
  - failure-domain.beta.kubernetes.io/region
  - failure-domain.kubernetes.io/zone
  - failure-domain.kubernetes.io/region
  - [*]kubelet.kubernetes.io/*
  - [*]node.kubernetes.io/*

**Kubernetes Versions Previously Supported by Container Engine for Kubernetes**

Container Engine for Kubernetes previously supported the following versions of Kubernetes:

<table>
<thead>
<tr>
<th>Kubernetes Version</th>
<th>Supported by Container Engine for Kubernetes?</th>
<th>Support Ended</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.15.12</td>
<td>No</td>
<td>2 February, 2021</td>
</tr>
<tr>
<td>1.15.7</td>
<td>No</td>
<td>2 February, 2021</td>
</tr>
<tr>
<td>1.14.8</td>
<td>No</td>
<td>15 December 2020</td>
</tr>
<tr>
<td>1.13.x</td>
<td>No</td>
<td>21 March, 2020</td>
</tr>
<tr>
<td>1.12.7</td>
<td>No</td>
<td>29 January, 2020</td>
</tr>
<tr>
<td>1.12.6</td>
<td>No</td>
<td>15 April, 2019</td>
</tr>
<tr>
<td>1.11.9</td>
<td>No</td>
<td>9 September, 2019</td>
</tr>
<tr>
<td>1.11.8</td>
<td>No</td>
<td>15 April, 2019</td>
</tr>
<tr>
<td>1.11.x versions prior to 1.11.8</td>
<td>No</td>
<td>13 March, 2019</td>
</tr>
<tr>
<td>1.10.x</td>
<td>No</td>
<td>12 April, 2019</td>
</tr>
<tr>
<td>1.9.x</td>
<td>No</td>
<td>11 December, 2019</td>
</tr>
<tr>
<td>1.8.x</td>
<td>No</td>
<td>7 September, 2018</td>
</tr>
</tbody>
</table>
Upgrading Clusters to Newer Kubernetes Versions

After a new version of Kubernetes has been released and when Container Engine for Kubernetes supports the new version, you can upgrade the Kubernetes version running on control plane nodes and worker nodes in a cluster.

The control plane nodes and worker nodes that comprise the cluster can run different versions of Kubernetes, provided you follow the Kubernetes version skew support policy described in the Kubernetes documentation.

You upgrade control plane nodes and worker nodes differently:

• You upgrade control plane nodes by upgrading the cluster and specifying a more recent Kubernetes version for the cluster. Control plane nodes running older versions of Kubernetes are upgraded. Because Container Engine for Kubernetes distributes the Kubernetes Control Plane on multiple Oracle-managed control plane nodes to ensure high availability (distributed across different availability domains in a region where supported), you're able to upgrade the Kubernetes version running on control plane nodes with zero downtime.

Having upgraded control plane nodes to a new version of Kubernetes, you can subsequently create new node pools with worker nodes running the newer version. Alternatively, you can continue to create new node pools with worker nodes running older versions of Kubernetes (providing those older versions are compatible with the Kubernetes version running on the control plane nodes).

For more information about control plane node upgrade, see Upgrading the Kubernetes Version on Control Plane Nodes in a Cluster on page 930.

• You upgrade worker nodes in one of two ways:
  • By performing an 'in-place' upgrade of a node pool in the cluster, specifying a more recent Kubernetes version for the existing node pool.
  • By performing an 'out-of-place' upgrade of a node pool in the cluster, replacing the original node pool with a new node pool for which you've specified a more recent Kubernetes version.

For more information about worker node upgrade, see Upgrading the Kubernetes Version on Worker Nodes in a Cluster on page 930.

To find out more about the Kubernetes versions currently and previously supported by Container Engine for Kubernetes, see Supported Versions of Kubernetes on page 926.

Notes about Upgrading Clusters

Note the following when upgrading clusters:

• Container Engine for Kubernetes only upgrades the Kubernetes version running on control plane nodes when you explicitly initiate the upgrade operation.

• After upgrading control plane nodes to a newer version of Kubernetes, you cannot downgrade the control plane nodes to an earlier Kubernetes version.

• Before you upgrade the version of Kubernetes running on the control plane nodes, it is your responsibility to test that applications deployed on the cluster are compatible with the new Kubernetes version. For example, before upgrading the existing cluster, you might create a new separate cluster with the new Kubernetes version to test your applications.

• The versions of Kubernetes running on the control plane nodes and the worker nodes must be compatible (that is, the Kubernetes version on the control plane nodes must be no more than two minor versions ahead of the Kubernetes version on the worker nodes). See the Kubernetes version skew support policy described in the Kubernetes documentation.

• If the version of Kubernetes currently running on the control plane nodes is more than one version behind the most recent supported version, you are given a choice of versions to upgrade to. If you want to upgrade to a version of Kubernetes that is more than one version ahead of the version currently running on the control plane nodes, you must upgrade to each intermediate version in sequence without skipping versions (as described in the Kubernetes documentation).

• To successfully upgrade control plane nodes in a cluster, the Kubernetes Dashboard service must be of type ClusterIP. If the Kubernetes Dashboard service is not of type ClusterIP (for example, if the service is of type NodePort), the upgrade will fail. In this case, change the type of the Kubernetes Dashboard service back to
ClusterIP (for example, by entering `kubectl -n kube-system edit service kubernetes-dashboard` and changing the type).

- Prior to Kubernetes version 1.14, Container Engine for Kubernetes created clusters with kube-dns as the DNS server. However, from Kubernetes version 1.14 onwards, Container Engine for Kubernetes creates clusters with CoreDNS as the DNS server. When you upgrade a cluster created by Container Engine for Kubernetes from an earlier version to Kubernetes 1.14 or later, the cluster's kube-dns server is automatically replaced with the CoreDNS server. Note that if you customized kube-dns behavior using the original kube-dns ConfigMap, those customizations are not carried forward to the CoreDNS ConfigMap. You will have to create and apply a new ConfigMap containing the customizations to override settings in the CoreDNS Corefile. For more information about upgrading to CoreDNS, see Configuring DNS Servers for Kubernetes Clusters on page 932.

**Upgrading the Kubernetes Version on Control Plane Nodes in a Cluster**

When Container Engine for Kubernetes supports a newer version of Kubernetes than the version currently running on the control plane nodes in a cluster, you can upgrade the Kubernetes version running on the control plane nodes.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you’ve upgraded control plane nodes to a newer Kubernetes version, you can’t downgrade the control plane nodes to an earlier Kubernetes version. It’s therefore important that before you upgrade the Kubernetes version running on the control plane nodes, you test that applications deployed on the cluster are compatible with the new Kubernetes version.</td>
</tr>
</tbody>
</table>

**Using the Console**

To upgrade the version of Kubernetes running on the control plane nodes:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Kubernetes Clusters.
2. Choose a Compartment you have permission to work in.
3. On the Cluster List page, click the name of the cluster where you want to upgrade the Kubernetes version running on the control plane nodes.

   If a newer Kubernetes version is available than the one running on the control plane nodes in the cluster, the Upgrade button is enabled at the top of the Cluster page.
4. Click Upgrade to upgrade the control plane nodes to a newer version.
5. In the Upgrade Cluster Master dialog box, select the Kubernetes version to which to upgrade the control plane nodes, and click Upgrade.

The Kubernetes version running on the control plane nodes is upgraded. From now on, the new Kubernetes version will appear as an option when you’re defining new node pools for the cluster.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the UpdateCluster operation to upgrade the version of Kubernetes running on the control plane nodes.

**Upgrading the Kubernetes Version on Worker Nodes in a Cluster**

You can upgrade the version of Kubernetes running on the worker nodes in a cluster in two ways:

- Perform an ‘in-place’ upgrade of a node pool in the cluster, by specifying a more recent Kubernetes version for new worker nodes starting in the existing node pool. First, you modify the existing node pool's properties to specify the more recent Kubernetes version. Then, you 'drain' existing worker nodes in the node pool to prevent new pods starting, and to delete existing pods. Finally, you terminate each of the worker nodes in turn. When new worker nodes are started in the existing node pool, they run the more recent Kubernetes version you specified. See Performing an In-Place Worker Node Upgrade by Updating an Existing Node Pool on page 931.
• Perform an 'out-of-place' upgrade of a node pool in the cluster, by replacing the original node pool with a new node pool. First, you create a new node pool with a more recent Kubernetes version. Then, you 'drain' existing worker nodes in the original node pool to prevent new pods starting, and to delete existing pods. Finally, you delete the original node pool. When new worker nodes are started in the new node pool, they run the more recent Kubernetes version you specified. See Performing an Out-of-Place Worker Node Upgrade by Replacing an Existing Node Pool with a New Node Pool on page 932.

Note that in both cases:

• The more recent Kubernetes version you specify for the worker nodes in the node pool must be compatible with the Kubernetes version running on the control plane nodes in the cluster. See Upgrading Clusters to Newer Kubernetes Versions on page 929).
• You must drain existing worker nodes in the original node pool. If you don't drain the worker nodes, workloads running on the cluster are subject to disruption.

Performing an In-Place Worker Node Upgrade by Updating an Existing Node Pool

You can upgrade the version of Kubernetes running on worker nodes in a node pool by specifying a more recent Kubernetes version for the existing node pool. For each worker node, you first drain it to prevent new pods starting and to delete existing pods. You then terminate the worker node so that a new worker node is started, running the more recent Kubernetes version you specified. When new worker nodes are started in the existing node pool, they run the more recent Kubernetes version you specified.

To perform an in-place upgrade of a node pool in a cluster, by specifying a more recent Kubernetes version for the existing node pool:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Kubernetes Clusters.
2. Choose a Compartment you have permission to work in.
3. On the Cluster List page, click the name of the cluster where you want to change the Kubernetes version running on worker nodes.
4. On the Cluster page, display the Node Pools tab, and click the name of the node pool where you want to upgrade the Kubernetes version running on the worker nodes.
5. On the Node Pool page, click Edit and in the Version field, specify the required Kubernetes version for worker nodes.

The Kubernetes version you specify must be compatible with the version that is running on the control plane nodes.
6. Click Edit to save the change.

You now have to terminate existing worker nodes so that new worker nodes are started, running the Kubernetes version you specified.
7. For the first worker node in the node pool:
   a. Prevent new pods from starting and delete existing pods by entering:

```
  kubectl drain <node_name>
```

For more information:
• about using kubectl, see Accessing a Cluster Using Kubectl on page 890
• about the drain command, see drain in the Kubernetes documentation

Recommended: Leverage pod disruption budgets as appropriate for your application to ensure that there's a sufficient number of replica pods running throughout the drain operation.

b. On the Node Pool page, display the Nodes tab and click the worker node’s name in the Node Name field.
c. On the Instances page, select Terminate from the More Actions menu.

The worker node is terminated and a new worker node is started in its place, running the Kubernetes version you specified.
8. Repeat the previous step for each remaining worker node in the node pool, until all worker nodes in the node pool are running the Kubernetes version you specified.

**Performing an Out-of-Place Worker Node Upgrade by Replacing an Existing Node Pool with a New Node Pool**

You can 'upgrade' the version of Kubernetes running on worker nodes in a node pool by replacing the original node pool with a new node pool that has new worker nodes running the appropriate Kubernetes version. Having drained existing worker nodes in the original node pool to prevent new pods starting and to delete existing pods, you can then delete the original node pool. When new worker nodes are started in the new node pool, they run the more recent Kubernetes version you specified.

To perform an 'out-of-place' upgrade of a node pool in a cluster, by creating a new node pool to 'upgrade' the Kubernetes version on worker nodes:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Kubernetes Clusters.
2. Choose a Compartment you have permission to work in.
3. On the Cluster List page, click the name of the cluster where you want to change the Kubernetes version running on worker nodes.
4. On the Cluster page, display the Node Pools tab, and then click Add Node Pool to create a new node pool and specify the required Kubernetes version for its worker nodes.

   The Kubernetes version you specify must be compatible with the version that is running on the control plane nodes.
5. If there are labels attached to worker nodes in the original node pool and those labels are used by selectors (for example, to determine the nodes on which to run pods), then use the `kubectl label nodes` command to attach the same labels to the new worker nodes in the new node pool. See Assigning Pods to Nodes in the Kubernetes documentation.
6. For the first worker node in the original node pool, prevent new pods from starting and delete existing pods by entering:

   ```
   kubectl drain <node_name>
   ```

   For more information:
   - about using kubectl, see Accessing a Cluster Using Kubectl on page 890
   - about the drain command, see drain in the Kubernetes documentation

   **Recommended**: Leverage pod disruption budgets as appropriate for your application to ensure that there's a sufficient number of replica pods running throughout the drain operation.
7. Repeat the previous step for each remaining worker node in the node pool, until all the worker nodes have been drained from the original node pool.

   When you have drained all the worker nodes from the original node pool and pods are running on worker nodes in the new node pool, you can delete the original node pool.
8. On the Cluster page, display the Node Pools tab, and then select Delete Node Pool from the Actions menu beside the original node pool.

   The original node pool and all its worker nodes are deleted.

**Configuring DNS Servers for Kubernetes Clusters**

**Configuring Built-in DNS Servers (kube-dns, CoreDNS)**

Clusters created by Container Engine for Kubernetes include a DNS server as a built-in Kubernetes service that is launched automatically. The kubelet process on each worker node directs individual containers to the DNS server to translate DNS names to IP addresses.
Prior to Kubernetes version 1.14, Container Engine for Kubernetes created clusters with kube-dns as the DNS server. However, from Kubernetes version 1.14 onwards, Container Engine for Kubernetes creates clusters with CoreDNS as the DNS server. CoreDNS is a general-purpose authoritative DNS server that is modular and pluggable.

Default CoreDNS behavior is controlled by a configuration file referred to as a Corefile. The Corefile is a Kubernetes ConfigMap, with a Corefile section that defines CoreDNS behavior. You cannot modify the Corefile directly. If you need to customize CoreDNS behavior, you create and apply your own ConfigMap to override settings in the Corefile (as described in this topic). Note that if you do customize CoreDNS default behavior, the customizations are periodically deleted during internal updates to the cluster.

When you upgrade a cluster created by Container Engine for Kubernetes from an earlier version to Kubernetes 1.14 or later, the cluster's kube-dns server is automatically replaced with the CoreDNS server. Note that if you customized kube-dns behavior using the original kube-dns ConfigMap, those customizations are not carried forward to the CoreDNS ConfigMap. You will have to create and apply a new ConfigMap containing the customizations to override settings in the CoreDNS Corefile.

For more information about CoreDNS customization and Kubernetes, see the Kubernetes documentation and the CoreDNS documentation.

To create a ConfigMap to override the settings in the CoreDNS Corefile:

1. Define a ConfigMap in a yaml file, in the format:

   ```yaml
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: coredns-custom
     namespace: kube-system
   data:
     <customization-options>
   ```

   For example:

   ```yaml
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: coredns-custom
     namespace: kube-system
   data:
     example.server: | # All custom server files must have a "server" file extension.
                      # Change example.com to the domain you wish to forward.
               example.com {
                      # Change 1.1.1.1 to your customer DNS resolver.
               forward 1.1.1.1
        }
   ```

   For more information about the ConfigMap options to use to customize CoreDNS behavior, see the Kubernetes documentation and the CoreDNS documentation.

2. Create the ConfigMap by entering:

   ```bash
   kubectl apply -f <filename>.yaml
   ```

3. Verify the customizations have been applied by entering:

   ```bash
   kubectl get configmaps --namespace=kube-system coredns-custom -o yaml
   ```

4. Force CoreDNS to reload the ConfigMap by entering:

   ```bash
   kubectl delete pod --namespace kube-system -l k8s-app=kube-dns
   ```
Configuring ExternalDNS to use Oracle Cloud Infrastructure DNS

ExternalDNS is an add-on to Kubernetes that can create DNS records for services in DNS providers external to Kubernetes. It sets up DNS records in an external DNS provider to make Kubernetes services discoverable via that DNS provider, and enables you to control DNS records dynamically. See ExternalDNS for more information.

Having deployed ExternalDNS on a cluster, you can expose a service running on the cluster by adding the external-dns.alpha.kubernetes.io/hostname annotation to the service. ExternalDNS creates a DNS record for the service in the external DNS provider you've configured for the cluster.

ExternalDNS is not itself a DNS server like CoreDNS, but a way to configure other external DNS providers. Oracle Cloud Infrastructure DNS is one such external DNS provider. See Overview of the DNS Service on page 1674.

For convenience, instructions are included below to set up ExternalDNS on a cluster and configure it to use Oracle Cloud Infrastructure DNS. These instructions are a summary based on the Setting up ExternalDNS for Oracle Cloud Infrastructure (OCI) tutorial, which is available on GitHub.

To set up ExternalDNS on a cluster and configure it to use Oracle Cloud Infrastructure DNS:

1. Create a new DNS zone in Oracle Cloud Infrastructure DNS to contain the DNS records that ExternalDNS will create for the cluster. See Creating a Zone on page 1677.
2. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.
3. Create a Kubernetes secret containing the Oracle Cloud Infrastructure user authentication details for ExternalDNS to use when connecting to the Oracle Cloud Infrastructure API to insert and update DNS records in the DNS zone you just created.

   a. In a text editor, create a credentials file containing the Oracle Cloud Infrastructure user credentials to use to access the DNS zone:

   ```
   auth:
     region: <region-identifier>
     tenancy: <tenancy-ocid>
     user: <user-ocid>
     key: |
       -----BEGIN RSA PRIVATE KEY-----
       <private-key>
       -----END RSA PRIVATE KEY-----
     fingerprint: <fingerprint>
     # Omit if there is not a password for the key
     passphrase: <passphrase>
     compartment: <compartment-ocid>
   ```

   where:
   * `<region-identifier>` identifies the user's region. For example, us-phoenix-1
   * `<tenancy-ocid>` is the OCID of the user's tenancy. For example, ocid1.tenancy.oc1..aaaaaaaap...keq (abbreviated for readability).
   * `<user-ocid>` is the OCID of the user. For example, ocid1.user.oc1..aaaaa...zutq (abbreviated for readability).
   * `<private-key>` is an RSA key, starting with -----BEGIN RSA PRIVATE KEY----- and ending with -----END RSA PRIVATE KEY-----
   * `<passphrase>` optionally provides the passphrase for the key, if one exists
   * `<compartment-ocid>` is the OCID of the compartment to which the DNS zone belongs

For example:

```
auth:
  region: us-phoenix-1
```
b. Save the credentials file with a name of your choosing (for example, `oci-creds.yaml`).

c. Create a Kubernetes secret from the credentials file you just created, by entering:

```
kubectl create secret generic <secret-name> --from-file=<credential-filename>
```

For example:

```
kubectl create secret generic external-dns-config --from-file=oci-creds.yaml
```

4. Deploy ExternalDNS on the cluster.

a. In a text editor, create a configuration file (for example, called `external-dns-deployment.yaml`) to create the ExternalDNS deployment, and specify the name of the Kubernetes secret you just created. For example:

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: external-dns
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: external-dns
rules:
- apiGroups: ["" ]
  resources: ["services","endpoints","pods"]
  verbs: ["get","watch","list"]
- apiGroups: ["extensions","networking.k8s.io"]
  resources: ["ingresses"]
  verbs: ["get","watch","list"]
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["list"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: external-dns-viewer
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: external-dns
subjects:
- kind: ServiceAccount
  name: external-dns
  namespace: default
---
apiVersion: apps/v1
kind: Deployment
```
metadata:
    name: external-dns
spec:
    strategy:
        type: Recreate
    selector:
        matchLabels:
            app: external-dns
    template:
        metadata:
            labels:
                app: external-dns
        spec:
            serviceAccountName: external-dns
            containers:
                - name: external-dns
                    image: k8s.gcr.io/external-dns/external-dns:v0.7.3
                    args:
                        - --source=service
                        - --source=ingress
                        - --provider=oci
                        - --policy=upsert-only # prevent ExternalDNS from deleting any
                        records, omit to enable full synchronization
                        - --txt-owner-id=my-identifier
                    volumeMounts:
                        - name: config
                            mountPath: /etc/kubernetes/
                - name: config
                    secretName: external-dns-config

b. Save and close the configuration file.
c. Apply the configuration file to deploy ExternalDNS by entering:

```
kubectl apply -f <filename>
```

where `<filename>` is the name of the file you created earlier. For example:

```
kubectl apply -f external-dns-deployment.yaml
```

The output from the above command confirms the deployment:

```
serviceaccount/external-dns created
clusterrole.rbac.authorization.k8s.io/external-dns created
clusterrolebinding.rbac.authorization.k8s.io/external-dns-viewer created
deployment.apps/external-dns created
```

5. Verify that ExternalDNS has been deployed successfully and can insert records in the DNS zone you created earlier in Oracle Cloud Infrastructure by creating an nginx deployment and an nginx service:

a. In a text editor, create a configuration file (for example, called `nginx-externaldns.yaml`) to create an nginx deployment and an nginx service that includes the `external-dns.alpha.kubernetes.io/hostname` annotation. For example:

```
apiVersion: v1
kind: Service
metadata:
    name: nginx
    annotations:
        external-dns.alpha.kubernetes.io/hostname: example.com
spec:
```
Creating Load Balancers to Distribute Traffic Between Cluster Nodes

When you create a deployment, you can optionally create a load balancer service in the same compartment as the cluster to distribute traffic between the nodes assigned to the deployment. The key fields in the configuration of a load balancer service are the type of service being created and the ports that the load balancer will listen to.

Note:

Load balancer services you create appear in the Console. However, do not use the Console (or the Oracle Cloud Infrastructure CLI or API) to modify load balancer services. Any modifications you make will either be reverted by Container Engine for Kubernetes or will conflict with its operation and possibly result in service interruption.
Creating Load Balancers to Distribute HTTP Traffic

Consider the following configuration file, nginx_lb.yaml. It defines a deployment (kind: Deployment) for the nginx app, followed by a service definition with a type of LoadBalancer (type: LoadBalancer) that balances http traffic on port 80 for the nginx app.

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-nginx
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.7.9
        ports:
        - containerPort: 80
---
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: nginx
```

The first part of the configuration file defines an Nginx deployment, requesting that it be hosted on 3 pods running the nginx:1.7.9 image, and accept traffic to the containers on port 80.

The second part of the configuration file defines the Nginx service, which uses type LoadBalancer to balance Nginx traffic on port 80 amongst the available pods.

To create the deployment and service defined in nginx_lb.yaml while connected to your Kubernetes cluster, enter the command:

```
kubectl apply -f nginx_lb.yaml
```

This command outputs the following upon successful creation of the deployment and the load balancer:

```
deployment "my-nginx" created
service "my-nginx-svc" created
```

The load balancer may take a few minutes to go from a pending state to being fully operational. You can view the current state of your cluster by entering:

```
kubectl get all
```
The output from the above command shows the current state:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>po/my-nginx-431080787-0m4m8</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>3m</td>
</tr>
<tr>
<td>po/my-nginx-431080787-hqqcr</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>3m</td>
</tr>
<tr>
<td>po/my-nginx-431080787-n8125</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>3m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>CLUSTER-IP</th>
<th>EXTERNAL-IP</th>
<th>PORT(S)</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>svc/kubernetes</td>
<td>203.0.113.1</td>
<td>&lt;NONE&gt;</td>
<td>443/TCP</td>
<td>3d</td>
</tr>
<tr>
<td>svc/my-nginx-svc</td>
<td>203.0.113.7</td>
<td>192.0.2.22</td>
<td>80:30269/TCP</td>
<td>3m</td>
</tr>
</tbody>
</table>

The output shows that the **my-nginx** deployment is running on 3 pods (the po/my-nginx entries), that the load balancer is running (svc/my-nginx-svc) and has an external IP (192.0.2.22) that clients can use to connect to the app that's deployed on the pods.

**Creating Load Balancers with SSL Support to Distribute HTTPS Traffic**

You can create a load balancer with SSL termination, allowing https traffic to an app to be distributed among the nodes in a cluster. This example provides a walkthrough of the configuration and creation of a load balancer with SSL support.

Consider the following configuration file, nginx-demo-svc-ssl.yaml, which defines an Nginx deployment and exposes it via a load balancer that serves http on port 80, and https on port 443. This sample creates an Oracle Cloud Infrastructure load balancer, by defining a service with a type of LoadBalancer (type: LoadBalancer).

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx
        ports:
        - containerPort: 80
---
kind: Service
apiVersion: v1
metadata:
  name: nginx-service
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-ssl-ports: "443"
    service.beta.kubernetes.io/oci-load-balancer-tls-secret: ssl-certificate-secret
spec:
  selector:
```
The Load Balancer's annotations are of particular importance. The ports on which to support https traffic are defined by the value of `service.beta.kubernetes.io/oci-load-balancer-ssl-ports`. You can declare multiple SSL ports by using a comma-separated list for the annotation's value. For example, you could set the annotation's value to "443, 3000" to support SSL on ports 443 and 3000.

The required TLS secret, `ssl-certificate-secret`, needs to be created in Kubernetes. This example creates and uses a self-signed certificate. However, in a production environment, the most common scenario is to use a public certificate that's been signed by a certificate authority.

The following command creates a self-signed certificate, `tls.crt`, with its corresponding key, `tls.key`:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out tls.crt -subj "/CN=nginxsvc/O=nginxsvc"
```

Now that you created the certificate, you need to store both it and its key as a secret in Kubernetes. The name of the secret must match the name from the `service.beta.kubernetes.io/oci-load-balancer-tls-secret` annotation of the load balancer's definition. Use the following command to create a TLS secret in Kubernetes, whose key and certificate values are set by `--key` and `--cert`, respectively.

```
kubectl create secret tls ssl-certificate-secret --key tls.key --cert tls.crt
```

You must create the Kubernetes secret before you can create the service, since the service references the secret in its definition. Create the service using the following command:

```
kubectl create -f manifests/demo/nginx-demo-svc-ssl.yaml
```

Watch the service and wait for a public IP address (EXTERNAL-IP) to be assigned to the Nginx service (nginx-service) by entering:

```
kubectl get svc --watch
```

The output from the above command shows the load balancer IP to use to connect to the service.
The load balancer is now running, which means the service can now be accessed as follows:

- using http, by entering:
  
  ```
  curl http://198.51.100.1
  ```

- using https, by entering:
  
  ```
  curl --insecure https://198.51.100.1
  ```

The "--insecure" flag is used to access the service using https due to the use of self-signed certificates in this example. Do not use this flag in a production environment where the public certificate was signed by a certificate authority.

**Note**: When a cluster is deleted, a load balancer that's dynamically created when a service is created will not be removed. Before deleting a cluster, delete the service, which in turn will result in the cloud provider removing the load balancer. The syntax for this command is:

```
kubectl delete svc SERVICE_NAME
```

For example, to delete the service from the previous example, enter:

```
kubectl delete svc nginx-service
```

### Updating the TLS Certificates of Existing Load Balancers

To update the TLS certificate of an existing load balancer:

1. Obtain a new TLS certificate. In a production environment, the most common scenario is to use a public certificate that's been signed by a certificate authority.
2. Create a new Kubernetes secret. For example, by entering:

```
kubectl create secret tls new-ssl-certificate-secret --key new-tls.key --cert new-tls.crt
```

3. Modify the service definition to reference the new Kubernetes secret by changing the `service.beta.kubernetes.io/oci-load-balancer-tls-secret` annotation in the service configuration. For example:

```json
apiVersion: v1
kind: Service
metadata:
  name: nginx-service
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-ssl-ports: "443"
    service.beta.kubernetes.io/oci-load-balancer-tls-secret: new-ssl-certificate-secret
spec:
  selector:
    app: nginx
  type: LoadBalancer
  ports:
  - name: http
    port: 80
    targetPort: 80
  - name: https
    port: 443
    targetPort: 80
```
4. Update the service. For example, by entering:

```bash
kubectl apply -f new-nginx-demo-svc-ssl.yaml
```

## Creating Internal Load Balancers in Public and Private Subnets

You can create Oracle Cloud Infrastructure load balancers to control access to services running on a cluster:

- When you create a `custom` cluster, you select an existing VCN that contains the network resources to be used by the new cluster. If you want to use load balancers to control traffic into the VCN, you select existing public or private subnets in that VCN to host the load balancers.
- When you create a `quick` cluster, the VCN that's automatically created contains a public regional subnet to host a load balancer. If you want to host load balancers in private subnets, you can add private subnets to the VCN later.

Alternatively, you can create an internal load balancer service (often referred to simply as an 'internal load balancer') in a cluster to enable other programs running in the same VCN as the cluster to access services in the cluster. An internal load balancer is an Oracle Cloud Infrastructure private load balancer. A private load balancer has a private IP address assigned by the Load Balancing service, which serves as the entry point for incoming traffic. For more information about Oracle Cloud Infrastructure private load balancers, see Private Load Balancer on page 2481.

You can host internal load balancers in public subnets and private subnets.

To create an internal load balancer hosted on a public subnet, add the following annotation in the metadata section of the manifest file:

```yaml
service.beta.kubernetes.io/oci-load-balancer-internal: "true"
```

To create an internal load balancer hosted on a private subnet, add both following annotations in the metadata section of the manifest file:

```yaml
service.beta.kubernetes.io/oci-load-balancer-internal: "true"

service.beta.kubernetes.io/oci-load-balancer-subnet1: "ocid1.subnet.oc1..aaaaaa....vdfw"
```

where `ocid1.subnet.oc1..aaaaaa....vdfw` is the OCID of the private subnet.

For example:

```yaml
apiVersion: v1
class: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-internal: "true"
    service.beta.kubernetes.io/oci-load-balancer-subnet1: "ocid1.subnet.oc1..aaaaaa....vdfw"
spec:
  type: LoadBalancer
  ports:
  - port: 8100
    selector:
      app: nginx
```
Specifying Alternative Load Balancer Shapes

The shape of an Oracle Cloud Infrastructure load balancer specifies its maximum total bandwidth (that is, ingress plus egress). By default, load balancers are created with a shape of 100Mbps. Other shapes are available, including 400Mbps and 8000Mbps.

To specify an alternative shape for a load balancer, add the following annotation in the metadata section of the manifest file:

```
service.beta.kubernetes.io/oci-load-balancer-shape: <value>
```

where `<value>` is the bandwidth of the shape (for example, 100Mbps, 400Mbps, 8000Mbps).

For example:

```
apiVersion: v1
class: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-shape: 400Mbps
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: nginx
```

**Note:** Sufficient load balancer quota must be available in the region for the shape you specify. Enter the following `kubectl` command to confirm that load balancer creation did not fail due to lack of quota:

```
kubectl describe service <service-name>
```

Specifying Flexible Load Balancer Shapes

The shape of an Oracle Cloud Infrastructure load balancer specifies its maximum total bandwidth (that is, ingress plus egress). As described in Specifying Alternative Load Balancer Shapes on page 943, you can specify different load balancer shapes.

In addition, you can also specify a flexible shape for an Oracle Cloud Infrastructure load balancer, by defining a minimum and a maximum bandwidth for the load balancer.

To specify a flexible shape for a load balancer, add the following annotations in the metadata section of the manifest file:

```
service.beta.kubernetes.io/oci-load-balancer-shape: "flexible"
service.beta.kubernetes.io/oci-load-balancer-shape-flex-min: <min-value>
service.beta.kubernetes.io/oci-load-balancer-shape-flex-max: <max-value>
```

where:

- `<min-value>` is the minimum bandwidth for the load balancer, in Mbps (for example, 10)
- `<max-value>` is the maximum bandwidth for the load balancer, in Mbps (for example, 100)

Note that you do not include a unit of measurement when specifying bandwidth values for flexible load balancer shapes (unlike for pre-defined shapes). For example, specify the minimum bandwidth as 10 rather than as 10Mbps.
For example:

```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-shape: "flexible"
    service.beta.kubernetes.io/oci-load-balancer-shape-flex-min: 10
    service.beta.kubernetes.io/oci-load-balancer-shape-flex-max: 100
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: nginx
```

### Specifying Load Balancer Connection Timeout

You can specify the maximum idle time (in seconds) allowed between two successive receive or two successive send operations between the client and backend servers.

To explicitly specify a maximum idle time, add the following annotation in the metadata section of the manifest file:

```yaml
service.beta.kubernetes.io/oci-load-balancer-connection-idle-timeout: <value>
```

where `value` is the number of seconds.

For example:

```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-connection-idle-timeout: 100
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: nginx
```

Note that if you don't explicitly specify a maximum idle time, a default value is used. The default value depends on the type of listener:

- for TCP listeners, the default maximum idle time is 300 seconds
- for HTTP listeners, the default maximum idle time is 60 seconds

### Specifying Load Balancer Security List Management Options

You can use the security list management feature in Kubernetes to manage security list rules. This feature is useful if you are new to Kubernetes, or for basic deployments.
Note:
You might encounter scalability and other issues if you use the Kubernetes security list management feature in complex deployments, and with tools like Shepherd and Terraform. For these reasons, Oracle does not recommend using the Kubernetes security list management feature in production environments.

To specify how the Kubernetes security list management feature manages security lists, add the following annotation in the metadata section of the manifest file:

```
service.beta.kubernetes.io/oci-load-balancer-security-list-management-mode: <value>
```

where `<value>` is one of:

- **"All"**: All required security list rules for load balancer services are managed.
- **"Frontend"**: Only security list rules for ingress to load balancer services are managed. You have to set up a rule that allows inbound traffic to the appropriate ports for node port ranges, the kube-proxy health port, and the health check port ranges.
- **"None"**: No security list management is enabled. You have to set up a rule that allows inbound traffic to the appropriate ports for node port ranges, the kube-proxy health port, and the health check port ranges. Additionally, you have to set up rules to allow inbound traffic to load balancers.

For example:

```
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-security-list-management-mode: "Frontend"
spec:
  type: LoadBalancer
  ports:
  - port: 80
    selector:
      app: nginx
```

Note that if you specify an invalid value for `oci-load-balancer-security-list-management-mode`, the value "All" is used instead.

### Specifying Load Balancer Listener Protocol

You can define the type of traffic accepted by the load balancer listener by specifying the protocol on which the listener accepts connection requests.

To explicitly specify the load balancer listener protocol, add the following annotation in the metadata section of the manifest file:

```
service.beta.kubernetes.io/oci-load-balancer-backend-protocol: <value>
```

where `<value>` is the protocol that defines the type of traffic accepted by the listener. For example, "HTTP". To get a list of valid protocols, use the `ListProtocols` operation.
For example:

```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    service.beta.kubernetes.io/oci-load-balancer-backend-protocol: "HTTP"
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: nginx
```

Note that if you don't explicitly specify a protocol, "TCP" is used as the default value.

### Specifying Load Balancer Health Check Parameters

An Oracle Cloud Infrastructure load balancer applies a health check policy to continuously monitor backend servers. A health check is a test to confirm backend server availability, and can be a request or a connection attempt. If a server fails the health check, the load balancer takes the server temporarily out of rotation. If the server subsequently passes the health check, the load balancer returns it to the rotation.

Health check policies include a number of parameters, which have default values. When you create a load balancer, you can override health check parameter default values by including annotations in the metadata section of the manifest file. Having created a load balancer, you can later add, modify, and delete those annotations. If you delete an annotation that specified a value for a health check parameter, the load balancer uses the parameter's default value instead.

To specify how many unsuccessful health check requests to attempt before a backend server is considered unhealthy, add the following annotation in the metadata section of the manifest file:

```yaml
service.beta.kubernetes.io/oci-load-balancer-health-check-retries: <value>
```

where `<value>` is the number of unsuccessful health check requests.

To specify the interval between health check requests, add the following annotation in the metadata section of the manifest file:

```yaml
service.beta.kubernetes.io/oci-load-balancer-health-check-interval: <value>
```

where `<value>` is a numeric value in milliseconds. The minimum is 1000.

To specify the maximum time to wait for a response to a health check request, add the following annotation in the metadata section of the manifest file:

```yaml
service.beta.kubernetes.io/oci-load-balancer-health-check-timeout: <value>
```

where `<value>` is a numeric value in milliseconds. A health check is successful only if the load balancer receives a response within this timeout period.

For example:

```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
```
labels:
  app: nginx
annotations:
  service.beta.kubernetes.io/oci-load-balancer-health-check-retries: 5
  service.beta.kubernetes.io/oci-load-balancer-health-check-interval: 15000
  service.beta.kubernetes.io/oci-load-balancer-health-check-timeout: 4000
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: nginx

Note that if you don’t explicitly specify health check parameter values by including annotations in the metadata section of the manifest file, the following defaults are used:

<table>
<thead>
<tr>
<th>Annotation Not Included</th>
<th>Default Value Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>service.beta.kubernetes.io/oci-load-balancer-health-check-retries</td>
<td>3</td>
</tr>
<tr>
<td>service.beta.kubernetes.io/oci-load-balancer-health-check-interval</td>
<td>10000</td>
</tr>
<tr>
<td>service.beta.kubernetes.io/oci-load-balancer-health-check-timeout</td>
<td>3000</td>
</tr>
</tbody>
</table>

For more information about Oracle Cloud Infrastructure load balancer health check policies, see Working with Health Check Policies on page 2558.

**Preventing Nodes from Handling Load Balancer Traffic**

You can exclude particular worker nodes from the list of backend servers in an Oracle Cloud Infrastructure load balancer backend set. For more information, see node.kubernetes.io/exclude-from-external-load-balers on page 900.

**Creating a Persistent Volume Claim**

Container storage via a container’s root file system is ephemeral, and can disappear upon container deletion and creation. To provide a durable location to prevent data from being lost, you can create and use persistent volumes to store data outside of containers.

A persistent volume offers persistent storage that enables your data to remain intact, regardless of whether the containers to which the storage is connected are terminated.

A persistent volume claim (PVC) is a request for storage, which is met by binding the PVC to a persistent volume (PV). A PVC provides an abstraction layer to the underlying storage. For example, an administrator could create a number of static persistent volumes that can later be bound to one or more persistent volume claims. If none of the static persistent volumes match the user's PVC request, the cluster may attempt to dynamically create a new PV that matches the PVC request.

With Oracle Cloud Infrastructure as the underlying IaaS provider, you can provision persistent volume claims by attaching volumes from the Oracle Cloud Infrastructure Block Volume service. The volumes are connected to clusters created by Container Engine for Kubernetes using FlexVolume and CSI (Container Storage Interface) volume plugins deployed on the clusters.

The minimum amount of persistent storage that a PVC can request is 50 gigabytes. If the request is for less than 50 gigabytes, the request is rounded up to 50 gigabytes.

For more information about persistent volumes, persistent volume claims, and volume plugins, see the Kubernetes documentation.
Provisioning Persistent Volume Claims on the Block Volume Service

The Oracle Cloud Infrastructure Block Volume service (the Block Volume service) provides persistent, durable, and high-performance block storage for your data. You can use the CSI volume plugin or the FlexVolume volume plugin to connect clusters to volumes from the Block Volume service. Using the CSI volume plugin has several advantages:

- In future, new functionality will only be added to the CSI volume plugin, not to the FlexVolume volume plugin (although Kubernetes developers will continue to maintain the FlexVolume volume plugin).
- The CSI volume plugin does not require access to underlying operating system and root file system dependencies.

The StorageClass specified for a PVC controls which volume plugin to use to connect to Block Volume service volumes. If you don’t explicitly specify a value for storageClassName in the yaml file that defines the PVC, the cluster’s default StorageClass is used. In clusters created by Container Engine for Kubernetes, the oci StorageClass is initially set up as the default. The oci StorageClass is used by the FlexVolume volume plugin.

In the case of the CSI volume plugin, the CSI topology feature ensures that worker nodes and volumes are located in the same availability domain. In the case of the FlexVolume volume plugin, you can use the matchLabels element to select the availability domain in which a persistent volume claim is provisioned. Note that you do not use the matchLabels element with the CSI volume plugin.

Regardless of the volume plugin you choose to use, if a cluster is in a different compartment to its worker nodes, you must create an additional policy to enable access to Block Volume service volumes. This situation arises when the subnet specified for a node pool belongs to a different compartment to the cluster. To enable the worker nodes to access Block Volume service volumes, create the additional policy with both the following policy statements:

- ALLOW any-user to manage volumes in TENANCY where request.principal.type = 'cluster'
- ALLOW any-user to manage volume-attachments in TENANCY where request.principal.type = 'cluster'

Note:

In the FlexVolume examples in this topic, the PVCs request storage in availability domains in the Ashburn region using the failure-domain.beta.kubernetes.io/zone label. For more information about using this label (and the shortened versions of availability domain names to specify), see failure-domain.beta.kubernetes.io/zone on page 899.

Specifying the Volume plugin used by a Persistent Volume Claim

To explicitly specify the volume plugin to use to connect to the Block Volume service when provisioning a persistent volume claim, specify a value for storageClassName in the yaml file that defines the PVC:

- to use the CSI volume plugin, specify storageClassName: "oci-bv"
- to use the FlexVolume volume plugin, specify storageClassName: "oci"

Example 1: Dynamically Creating a Persistent Volume on the Block Volume Service for Use by the CSI Volume Plugin

In this example, the cluster administrator has not created any suitable PVs that match the PVC request. As a result, a block volume is dynamically provisioned using the CSI plugin specified by the oci-bv StorageClass's definition (provisioner: blockvolume.csi.oraclecloud.com).

You define a PVC in a file called csi-bvs-pvc.yaml. For example:

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mynginxclaim
spec:
```
Enter the following command to create the PVC from the csi-bvs-pvc.yaml file:

```bash
kubectl create -f csi-bvs-pvc.yaml
```

The output from the above command confirms the creation of the PVC:

```
persistentvolumeclaim "mynginxclaim" created
```

Verify that the PVC has been created by running `kubectl get pvc`:

```bash
kubectl get pvc
```

The output from the above command shows the current status of the PVC:

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>VOLUME</th>
<th>CAPACITY</th>
<th>ACCESSMODES</th>
<th>STORAGECLASS</th>
</tr>
</thead>
<tbody>
<tr>
<td>mynginxclaim</td>
<td>Pending</td>
<td></td>
<td></td>
<td></td>
<td>oci-bv</td>
</tr>
</tbody>
</table>

4m

The PVC has a status of `Pending` because the `oci-bv` StorageClass's definition includes `volumeBindingMode: WaitForFirstConsumer`.

You can use this PVC when creating other objects, such as pods. For example, you could create a new pod from the following pod definition, which instructs the system to use the `mynginxclaim` PVC as the nginx volume, which is mounted by the pod at /data.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
    - name: nginx
      image: nginx:latest
      ports:
        - name: http
          containerPort: 80
      volumeMounts:
        - name: data
          mountPath: /usr/share/nginx/html
  volumes:
    - name: data
      persistentVolumeClaim:
        claimName: mynginxclaim
```

Having created the new pod, you can verify that the PVC has been bound to a new persistent volume by entering:

```bash
kubectl get pvc
```

The output from the above command confirms that the PVC has been bound:
You can verify that the pod is using the new persistent volume claim by entering:

```
kubectl describe pod nginx
```

### Example 2: Dynamically Creating a Persistent Volume on the Block Volume Service for Use by the FlexVolume Volume Plugin

In this example, the cluster administrator has not created any suitable PVs that match the PVC request. As a result, a block volume is dynamically provisioned using the FlexVolume volume plugin specified by the `oci` StorageClass's definition (`provisioner: oracle.com/oci`).

You define a PVC in a file called `flex-bvs-pvc.yaml`. For example:

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mynginxclaim
spec:
  storageClassName: "oci"
  selector:
    matchLabels:      
    failure-domain.beta.kubernetes.io/zone: "US-ASHBURN-AD-1"
  accessModes:
    - ReadWriteOnce
  resources:
    requests:      
    storage: 50Gi
```

Note that the `flex-bvs-pvc.yaml` file includes the `matchLabels` element, which is only applicable in the case of the FlexVolume volume plugin.

Enter the following command to create the PVC from the `flex-bvs-pvc.yaml` file:

```
kubectl create -f flex-bvs-pvc.yaml
```

The output from the above command confirms the creation of the PVC:

```
persistentvolumeclaim "mynginxclaim" created
```

Verify that the PVC has been created and bound to a new persistent volume by entering:

```
kubectl get pvc
```

The output from the above command shows the current status of the PVC:

```
NAME               STATUS    VOLUME                               CAPACITY
ACCESSMODES   STORAGECLASS   AGE
mynginxclaim       Bound     ocid1.volume.oc1.iad.<unique_ID> 50Gi
RWO             oci-bv        4m
```

The PVC already has a status of `Bound` because the `oci` StorageClass’s definition includes `volumeBindingMode: Immediate`. 
You can use this PVC when creating other objects, such as pods. For example, the following pod definition instructs the system to use the mynginxclaim PVC as the nginx volume, which is mounted by the pod at /data.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
  - name: nginx
    image: nginx:latest
    ports:
    - name: http
      containerPort: 80
    volumeMounts:
    - name: data
      mountPath: /usr/share/nginx/html
  volumes:
  - name: data
    persistentVolumeClaim:
      claimName: mynginxclaim
```

Having created the new pod, you can verify that it is running and using the new persistent volume claim by entering:

```bash
kubectl describe pod nginx
```

**Example 3: Creating a Persistent Volume from a Backup on the Block Volume Service for Use by the FlexVolume Volume Plugin**

In this example, the cluster administrator has created a block volume backup for you to use when provisioning a new persistent volume claim. The block volume backup comes with data ready for use by other objects such as pods.

You define a PVC in a file called flex-pvcfrombackup.yaml file. You use the `volume.beta.kubernetes.io/oci-volume-source` annotation element to specify the source of the block volume to use when provisioning a new persistent volume claim using the FlexVolume volume plugin. You can specify the OCID of either a block volume or a block volume backup as the value of the annotation. In this example, you specify the OCID of the block volume backup created by the cluster administrator. For example:

```yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: myvolume
  annotations:
    volume.beta.kubernetes.io/oci-volume-source: ocidi.volumebackup.ocl.iad.abuw...
spec:
  selector:
    matchLabels:
      failure-domain.beta.kubernetes.io/zone: US-ASHBURN-AD-1
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 50Gi
```

Note that the flex-pvcfrombackup.yaml file includes the `matchLabels` element, which is only applicable in the case of the FlexVolume volume plugin.

Enter the following command to create the PVC from the flex-pvcfrombackup.yaml file:

```bash
kubectl create -f flex-pvcfrombackup.yaml
```
The output from the above command confirms the creation of the PVC:

```
persistentvolumeclaim "myvolume" created
```

Verify that the PVC has been created and bound to a new persistent volume created from the volume backup by entering:

```
kubectl get pvc
```

The output from the above command shows the current status of the PVC:

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>VOLUME</th>
<th>CAPACITY</th>
<th>ACCESSMODES</th>
<th>STORAGECLASS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>myvolume</td>
<td>Bound</td>
<td>ocid1.volume.oc1.iad.&lt;unique_ID&gt;</td>
<td>50Gi</td>
<td>RWO</td>
<td>oci</td>
<td>4m</td>
</tr>
</tbody>
</table>

You can use the new persistent volume created from the volume backup when defining other objects, such as pods. For example, the following pod definition instructs the system to use the myvolume PVC as the nginx volume, which is mounted by the pod at /data.

```
apiVersion: v1
group: apps
kind: StatefulSet
metadata:
  name: nginx
spec:
  replicas: 1
  serviceName: nginx
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:latest
          ports:
            - containerPort: 80
          volumeMounts:
            - name: data
              mountPath: /data
          volumes:
            - name: data
              persistentVolumeClaim:
                claimName: myvolume
```

Having created the new pod, you can verify that it is running and using the new persistent volume claim by entering:

```
kubectl describe pod nginx
```

Adding OCI Service Broker for Kubernetes to Clusters

Service brokers offer a catalog of backing services to workloads running on cloud native platforms. The Open Service Broker API is a commonly-used standard for interactions between service brokers and platforms. The Open Service Broker API specification describes a simple set of API endpoints that platforms use to provision, gain access to, and manage service offerings. For more information about the Open Service Broker API, see resources available online including those at openservicebrokerapi.org.

OCI Service Broker for Kubernetes is an implementation of the Open Service Broker API. OCI Service Broker for Kubernetes is specifically for interacting with Oracle Cloud Infrastructure services from Kubernetes clusters. It includes service broker adapters to bind to the following Oracle Cloud Infrastructure services:

- Object Storage
- Autonomous Transaction Processing
- Autonomous Data Warehouse
- Streaming
You can add OCI Service Broker for Kubernetes to clusters you've created with Oracle Cloud Infrastructure Container Engine for Kubernetes to interact with the Oracle Cloud Infrastructure services listed above. Having added OCI Service Broker for Kubernetes to a cluster, you don't have to manually provision and de-provision the Oracle Cloud Infrastructure services each time you deploy or un-deploy an application on the cluster. Instead, you interact with the Oracle Cloud Infrastructure services by using kubectl to call the Open Service Broker APIs implemented by OCI Service Broker for Kubernetes.

OCI Service Broker for Kubernetes is available as a Helm chart, a Docker container, and as source code from Github. For more information about OCI Service Broker for Kubernetes, see the OCI Service Broker for Kubernetes documentation in the Github repository.

**Adding OCI Service Broker for Kubernetes to a Cluster**

To add OCI Service Broker for Kubernetes to a cluster, follow the detailed instructions in the Github repository. For convenience, here's a high-level summary of the steps involved:

1. **Install OCI Service Broker for Kubernetes.** During this step, you will typically:
   - Install the Service Catalog.
   - Install the svcat tool.
   - Deploy OCI Service Broker for Kubernetes.
   - Grant RBAC permissions and roles.
   - Register OCI Service Broker for Kubernetes.
   
   For more information about installation, see the OCI Service Broker for Kubernetes documentation in the Github repository.

2. **Secure OCI Service Broker for Kubernetes.** During this step, you will typically:
   - Restrict access to Service Catalog resources using RBAC permissions and roles.
   - Configure TLS for OCI Service Broker for Kubernetes.
   - Set up an Oracle Cloud Infrastructure user for use by OCI Service Broker for Kubernetes.
   - Set up appropriate policies to control access to resources (according to the Oracle Cloud Infrastructure services to be used).
   - Limit access to the OCI Service Broker for Kubernetes endpoint using NetworkPolicy.
   - Stand up an etcd cluster for Service Catalog and OCI Service Broker for Kubernetes.
   - Protect sensitive values by creating secrets.
   
   The security configuration to choose will depend on your particular requirements. For more information, see the OCI Service Broker for Kubernetes documentation in the Github repository.

3. **Provision and bind to the required Oracle Cloud Infrastructure services.** During this step, you will typically:
   - Provide service provision request parameters.
   - Provide service binding request parameters.
   - Provide service binding response credentials.
   
   The details to provide will depend on the Oracle Cloud Infrastructure service to bind to. For more information, see the OCI Service Broker for Kubernetes documentation in the Github repository.

**Example: Setting Up an Ingress Controller on a Cluster**

You can set up different open source ingress controllers on clusters you have created with Container Engine for Kubernetes.

This topic explains how to set up an example ingress controller along with corresponding access control on an existing cluster. Having set up the ingress controller, this topic describes how to use the ingress controller with an example hello-world backend, and how to verify the ingress controller is working as expected.
Example Components

The example includes an ingress controller and a hello-world backend.

Ingress Controller Components

The ingress controller comprises:

- An ingress controller deployment called `nginx-ingress-controller`. The deployment deploys an image that contains the binary for the ingress controller and Nginx. The binary manipulates and reloads the `/etc/nginx/nginx.conf` configuration file when an ingress is created in Kubernetes. Nginx upstreams point to services that match specified selectors.
- An ingress controller service called `ingress-nginx`. The service exposes the ingress controller deployment as a LoadBalancer type service. Because Container Engine for Kubernetes uses an Oracle Cloud Infrastructure integration/cloud-provider, a load balancer will be dynamically created with the correct nodes configured as a backend set.

Backend Components

The hello-world backend comprises:

- A backend deployment called `docker-hello-world`. The deployment handles default routes for health checks and 404 responses. This is done by using a stock hello-world image that serves the minimum required routes for a default backend.
- A backend service called `docker-hello-world-svc`. The service exposes the backend deployment for consumption by the ingress controller deployment.

Setting Up the Example Ingress Controller

In this section, you create the access rules for ingress. You then create the example ingress controller components, and confirm they are running.

Creating the Access Rules for the Ingress Controller

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.
2. If your Oracle Cloud Infrastructure user is a tenancy administrator, skip the next step and go straight to Creating the Service Account, and the Ingress Controller on page 955.
3. If your Oracle Cloud Infrastructure user is not a tenancy administrator, in a terminal window, grant the user the Kubernetes RBAC cluster-admin clusterrole on the cluster by entering:

```
kubectl create clusterrolebinding <my-cluster-admin-binding> --clusterrole=cluster-admin --user=<user-OCID>
```

where:

- `<my-cluster-admin-binding>` is a string of your choice to be used as the name for the binding between the user and the Kubernetes RBAC cluster-admin clusterrole. For example, `jdoe_clst_adm`
- `<user-OCID>` is the user's OCID (obtained from the Console). For example, `ocid1.user.oc1..aaaaa...zutq` (abbreviated for readability).

For example:

```
kubectl create clusterrolebinding jdoe_clst_adm --clusterrole=cluster-admin --user=ocid1.user.oc1..aaaaa...zutq
```
Creating the Service Account, and the Ingress Controller

1. Run the following command to create the `nginx-ingress-controller` ingress controller deployment, along with the Kubernetes RBAC roles and bindings:

   ```bash
   kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/nginx-0.30.0/deploy/static/mandatory.yaml
   ```

2. Create and save the file `cloud-generic.yaml` containing the following code to define the `ingress-nginx` ingress controller service as a load balancer service:

   ```yaml
   kind: Service
   apiVersion: v1
   metadata:
     name: ingress-nginx
     namespace: ingress-nginx
     labels:
       app.kubernetes.io/name: ingress-nginx
       app.kubernetes.io/part-of: ingress-nginx
   spec:
     type: LoadBalancer
     selector:
       app.kubernetes.io/name: ingress-nginx
       app.kubernetes.io/part-of: ingress-nginx
     ports:
       - name: http
         port: 80
         targetPort: http
       - name: https
         port: 443
         targetPort: https
   ```

3. Using the file you just saved, create the `ingress-nginx` ingress controller service by running the following command:

   ```bash
   kubectl apply -f cloud-generic.yaml
   ```

Verifying the `ingress-nginx` Ingress Controller Service is Running as a Load Balancer Service

1. View the list of running services by entering:

   ```bash
   kubectl get svc -n ingress-nginx
   ```

The output from the above command shows the services that are running:

```
NAME            TYPE           CLUSTER-IP     EXTERNAL-IP    PORT(S)
AGE
```
The EXTERNAL-IP for the ingress-nginx ingress controller service is shown as <pending> until the load balancer has been fully created in Oracle Cloud Infrastructure.

2. Repeat the kubectl get svc command until an EXTERNAL-IP is shown for the ingress-nginx ingress controller service:

```
kubectl get svc -n ingress-nginx
```

The output from the above command shows the EXTERNAL-IP for the ingress-nginx ingress controller service:

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>CLUSTER-IP</th>
<th>EXTERNAL-IP</th>
<th>PORT(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ingress-nginx</td>
<td>LoadBalancer</td>
<td>10.96.229.38</td>
<td>129.146.214.219</td>
<td>80:30756/TCP</td>
</tr>
</tbody>
</table>

### Creating the TLS Secret

A TLS secret is used for SSL termination on the ingress controller.

1. Output a new key to a file. For example, by entering:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out tls.crt -subj "/CN=nginxsvc/O=nginxsvc"
```

To generate the secret for this example, a self-signed certificate is used. While this is okay for testing, for production, use a certificate signed by a Certificate Authority.

**Note:**

Under Windows, you may need to replace "/CN=nginxsvc/O=nginxsvc" with "//CN=nginxsvc\O=nginxsvc". For example, this is necessary if you run the openssl command from a Git Bash shell.

2. Create the TLS secret by entering:

```
kubectl create secret tls tls-secret --key tls.key --cert tls.crt
```

### Setting Up the Example Backend

In this section, you define a hello-world backend service and deployment.

### Creating the docker-hello-world Service Definition

1. Create the file hello-world-ingress.yaml containing the following code. This code uses a publicly available hello-world image from Docker Hub. You can substitute another image of your choice that can be run in a similar manner.

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: docker-hello-world
  labels:
    app: docker-hello-world
spec:
```

Container Engine for Kubernetes

```yaml
selector:
  matchLabels:
    app: docker-hello-world
replicas: 3

template:
  metadata:
    labels:
      app: docker-hello-world
  spec:
    containers:
      - name: docker-hello-world
        image: scottsbaldwin/docker-hello-world:latest
        ports:
          - containerPort: 80
---

apiVersion: v1
kind: Service
metadata:
  name: docker-hello-world-svc
spec:
  selector:
    app: docker-hello-world
  ports:
    - port: 8088
      targetPort: 80
  type: ClusterIP

```

Note the docker-hello-world service's type is ClusterIP, rather than LoadBalancer, because this service will be proxied by the ingress-nginx ingress controller service. The docker-hello-world service does not need public access directly to it. Instead, the public access will be routed from the load balancer to the ingress controller, and from the ingress controller to the upstream service.

2. Create the new hello-world deployment and service on nodes in the cluster by running the following command:

```
kubectl create -f hello-world-ingress.yaml
```

### Using the Example Ingress Controller to Access the Example Backend

In this section you create an ingress to access the backend using the ingress controller.

#### Creating the Ingress Resource

1. Create the file `ingress.yaml` and populate it with this code:

```yaml
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: hello-world-ing
  annotations:
    kubernetes.io/ingress.class: "nginx"
spec:
  tls:
    - secretName: tls-secret
  rules:
    - http:
        paths:
          - backend:
              serviceName: docker-hello-world-svc
              servicePort: 8088
```

Oracle Cloud Infrastructure User Guide
2. Create the resource by entering:

```
kubectl create -f ingress.yaml
```

## Verifying that the Example Components are Working as Expected

In this section, you confirm that all of the example components have been successfully created and are operating as expected. The `docker-hello-world-svc` service should be running as a ClusterIP service, and the `ingress-nginx` service should be running as a LoadBalancer service. Requests sent to the ingress controller should be routed to nodes in the cluster.

### Obtaining the External IP Address of the Load Balancer

To confirm the `ingress-nginx` service is running as a LoadBalancer service, obtain its external IP address by entering:

```
kubectl get svc --all-namespaces
```

The output from the above command shows the services that are running:

<table>
<thead>
<tr>
<th>NAMESPACE</th>
<th>NAME</th>
<th>TYPE</th>
<th>CLUSTER-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>docker-hello-world-svc</td>
<td>ClusterIP</td>
<td>10.96.83.247</td>
</tr>
<tr>
<td></td>
<td>8088/TCP</td>
<td>16s</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>kubernetes</td>
<td>ClusterIP</td>
<td>10.96.0.1</td>
</tr>
<tr>
<td></td>
<td>443/TCP</td>
<td>1h</td>
<td></td>
</tr>
<tr>
<td>ingress-nginx</td>
<td>ingress-nginx</td>
<td>LoadBalancer</td>
<td>10.96.229.38</td>
</tr>
<tr>
<td>129.146.214.219</td>
<td>80:30756/TCP,443:30118/TCP</td>
<td>5m</td>
<td></td>
</tr>
<tr>
<td>kube-system</td>
<td>kube-dns</td>
<td>ClusterIP</td>
<td>10.96.5.5</td>
</tr>
<tr>
<td></td>
<td>53/UDP,53/TCP</td>
<td>1h</td>
<td></td>
</tr>
</tbody>
</table>

### Sending cURL Requests to the Load Balancer

1. Use the external IP address of the `ingress-nginx` service (for example, 129.146.214.219) to curl an http request by entering:

```
curl -I http://129.146.214.219
```

Example output from the above command:

```
HTTP/1.1 301 Moved Permanently
Via: 1.1 10.68.69.10 (McAfee Web Gateway 7.6.2.10.0.23236)
Date: Thu, 07 Sep 2017 15:20:16 GMT
Server: nginx/1.13.2
Location: https://129.146.214.219/
Content-Type: text/html
Content-Length: 185
Proxy-Connection: Keep-Alive
```
Strict-Transport-Security: max-age=15724800; includeSubDomains;

The output shows a 301 redirect and a Location header that suggest that http traffic is being redirected to https.

2. Either cURL against the https url or add the `-L` option to automatically follow the location header. The `-k` option instructs cURL to not verify the SSL certificates. For example, by entering:

```
curl -ikL http://129.146.214.219
```

Example output from the above command:

```
HTTP/1.1 301 Moved Permanently
Via: 1.1 10.68.69.10 (McAfee Web Gateway 7.6.2.10.0.23236)
Date: Thu, 07 Sep 2017 15:22:29 GMT
Server: nginx/1.13.2
Location: https://129.146.214.219/
Content-Type: text/html
Content-Length: 185
Proxy-Connection: Keep-Alive
Strict-Transport-Security: max-age=15724800; includeSubDomains;

HTTP/1.1 200 Connection established
HTTP/1.1 200 OK
Server: nginx/1.13.2
Date: Thu, 07 Sep 2017 15:22:30 GMT
Content-Type: text/html
Content-Length: 71
Connection: keep alive
Last-Modified: Thu, 07 Sep 2017 15:17:24 GMT
ETag: "59b16304-47"
Accept-Ranges: bytes
Strict-Transport-Security: max-age=15724800; includeSubDomains;

<h1>Hello webhook world from: docker-hello-world-1732906117-0ztkm</h1>
```

The last line of the output shows the HTML that is returned from the pod whose hostname is `docker-hello-world-1732906117-0ztkm`.

3. Issue the cURL request several times to see the hostname in the HTML output change, demonstrating that load balancing is occurring:

```
$ curl -k https://129.146.214.219
<h1>Hello webhook world from: docker-hello-world-1732906117-6115l</h1>

$ curl -k https://129.146.214.219
<h1>Hello webhook world from: docker-hello-world-1732906117-7r89v</h1>

$ curl -k https://129.146.214.219
<h1>Hello webhook world from: docker-hello-world-1732906117-0ztkm</h1>
```
Inspecting nginx.conf

The nginx-ingress-controller ingress controller deployment manipulates the nginx.conf file in the pod within which it is running.

1. Find the name of the pod running the nginx-ingress-controller ingress controller deployment by entering:

   ```bash
   kubectl get po -n ingress-nginx
   ```

   The output from the above command shows the name of the pod running the nginx-ingress-controller ingress controller:

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>nginx-ingress-controller-110676328-h86xg</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
</tr>
<tr>
<td>1h</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Use the name of the pod running the nginx-ingress-controller ingress controller deployment to show the contents of nginx.conf by entering the following kubectl exec command:

   ```bash
   kubectl exec -n ingress-nginx -it nginx-ingress-controller-110676328-h86xg -- cat /etc/nginx/nginx.conf
   ```

3. Look for `proxy_pass` in the output. There will be one for the default backend and another that looks similar to:

   ```text
   proxy_pass http://upstream_balancer;
   ```

   This shows that Nginx is proxying requests to an upstream called `upstream_balancer`.

4. Locate the upstream definition in the output. It will look similar to:

   ```text
   upstream upstream_balancer {
       server 0.0.0.1:1234; # placeholder
       balancer_by_lua_block {
           tcp_udpBalancer.balance()
       }
   }
   ```

   The upstream is proxying via Lua.

Example: Installing Calico and Setting Up Network Policies

The Kubernetes networking model assumes containers (pods) have unique and routable IP addresses within a cluster. In the Kubernetes networking model, containers communicate with each other using those IP addresses, regardless of whether the containers are deployed on the same node in a cluster or on a different node. The Container Networking Interface (CNI) is the API that enables containers to communicate with the network using IP addresses.

By default, pods accept traffic from any source. To enhance cluster security, pods can be 'isolated' by selecting them in a network policy (the Kubernetes NetworkPolicy resource). A network policy is a specification of how groups of pods are allowed to communicate with each other and other network endpoints. NetworkPolicy resources use labels to select pods and to define rules that specify what traffic is allowed to the selected pods. If a NetworkPolicy in a cluster namespace selects a particular pod, that pod will reject any connections that are not allowed by any NetworkPolicy. Other pods in the namespace that are not selected by a NetworkPolicy will continue to accept all traffic. For more information about network policies, see the Kubernetes documentation.

Network policies are implemented by the CNI network provider. Simply creating the NetworkPolicy resource without a CNI network provider to implement it will have no effect. Note that not all CNI network providers implement the NetworkPolicy resource.
Clusters you create with Container Engine for Kubernetes have flannel installed as the default CNI network provider. Flannel is a simple overlay virtual network that satisfies the requirements of the Kubernetes networking model by attaching IP addresses to containers. For more information about flannel, see the flannel documentation.

Although flannel satisfies the requirements of the Kubernetes networking model, it does not support NetworkPolicy resources. If you want to enhance the security of clusters you create with Container Engine for Kubernetes by implementing network policies, you have to install and configure a network provider that does support NetworkPolicy resources. One such provider is Calico (refer to the Kubernetes documentation for a list of other network providers). Calico is an open source networking and network security solution for containers, virtual machines, and native host-based workloads. For more information about Calico, see the Calico documentation.

You can manually install Calico alongside flannel in clusters you have created using Container Engine for Kubernetes.

### Note:
- Only the use of open source Calico is supported. Use of Calico Enterprise is not supported.
- If you install Calico on a cluster that has existing node pools in which pods are already running, you will have to recreate the pods when the Calico installation is complete. For example, by running the `kubectl rollout restart` command. If you install Calico on a cluster before creating any node pools in the cluster (recommended), you can be sure that there will be no pods to recreate.

### Installing Calico manually

Having created a cluster using Container Engine for Kubernetes (using either the Console or the API), you can subsequently install Calico on the cluster (alongside flannel) to support network policies.

For convenience, Calico installation instructions are included below, based on Calico version 3.10. Note that Calico installation instructions vary between Calico versions. For information about installing different versions of Calico, always refer to the Calico documentation for installing Calico for network policy enforcement only.

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.

2. In a terminal window, download the Calico policy-only manifest for the Kubernetes API datastore by entering:

   ```
curl https://docs.projectcalico.org/v3.10/manifests/calico-policy-only.yaml -o calico.yaml
   
   Note that the url differs, according to the version of Calico that you want to install. Refer to the Calico documentation for instructions to install a particular version of Calico.

3. The calico.yaml file includes multiple references to the pod CIDR block value. In the downloaded calico.yaml file, the pod CIDR block value is initially set to 192.168.0.0/16. If the pod CIDR block value of the cluster created by Container Engine for Kubernetes is 192.168.0.0/16, skip this step. However, if the pod CIDR block value of the cluster created by Container Engine for Kubernetes is a different value (such as the default value of
10.244.0.0/16), you have to change the initial value in the calico.yaml file. The steps below show one way to do that:

a. Set the value of an environment variable to the pod CIDR block value. For example, by entering a command like:

```bash
echo $POD_CIDR
```

b. Replace the default value 192.168.0.0/16 in the calico.yaml file with the actual pod CIDR block value of the cluster created by Container Engine for Kubernetes. For example, by entering a command like:

```bash
sed -i -e "s?192.168.0.0/16?$POD_CIDR?g" calico.yaml
```

4. The calico.yaml file defines a deployment named calico-typha, which has a replica count of 1 by default. You might want to consider changing this default replica count for large clusters or production environments. Calico recommends:

- At least one replica for every 200 nodes, up to a maximum of 20.
- A minimum of three replicas in production environments to reduce the impact of rolling upgrades and failures (the number of replicas should always be less than the number of nodes, otherwise rolling upgrades will stall).

To change the replica count, open the calico.yaml file in a text editor and change the value of the `replicas` setting:

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: calico-typha
...
spec:
...
  replicas: <number-of-replicas>
```

Note that the way to set the replica count differs, according to the Calico version you've installed. Refer to the Calico documentation to find out how to set the replica count for the version you've installed.

5. Install and configure Calico by entering the following command:

```bash
kubectl apply -f calico.yaml
```

### Setting up Network Policies

Having installed Calico on a cluster you've created with Container Engine for Kubernetes, you can create Kubernetes NetworkPolicy resources to isolate pods as required.

For NetworkPolicy examples and how to use them, see the Calico documentation and specifically:

- Kubernetes policy, demo
- Kubernetes policy, basic tutorial
- Kubernetes policy, advanced tutorial

Note that the examples vary, according to the Calico version you've installed.

### Frequently Asked Questions About Container Engine for Kubernetes

This topic provides answers to some frequently asked questions about Container Engine for Kubernetes.
Does Container Engine for Kubernetes Support Alpha and Beta Features in Kubernetes?

Periodically, Kubernetes releases new features. New Kubernetes features are introduced in the following stages, as described in the Kubernetes documentation and summarized below:

- **Alpha stage**: An Alpha feature is disabled by default, might contain bugs, and might change or be dropped at any time. The feature is recommended for short-lived testing clusters only.
- **Beta stage**: A Beta feature is usually enabled by default, has been well-tested, and will not be dropped. However, details of the feature might change in incompatible ways, and is recommended for non-business-critical use only.
- **General Availability stage**: A Generally Available (or Stable) feature is always enabled, and will appear in released software for many subsequent versions.

Container Engine for Kubernetes supports the use of Kubernetes Beta features that are enabled by default in Kubernetes. Container Engine for Kubernetes does not support Alpha features, nor Beta features that are disabled by default.

For more information about Kubernetes Alpha and Beta features, see the Kubernetes documentation.

Container Engine for Kubernetes Metrics

You can monitor the health, capacity, and performance of Kubernetes clusters managed by Container Engine for Kubernetes using metrics, alarms, and notifications.

This topic describes the metrics emitted by Container Engine for Kubernetes in the `oci_oke` metric namespace.

Resources: clusters, worker nodes

Overview of the Container Engine for Kubernetes Service Metrics

Container Engine for Kubernetes metrics help you monitor Kubernetes clusters, along with node pools and individual worker nodes. You can use metrics data to diagnose and troubleshoot cluster and node pool issues.

To view a default set of metrics charts in the Console, navigate to the cluster you're interested in, and then click Metrics. You also can use the Monitoring service to create custom queries.

Prerequisites

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: `oci_oke`

The metrics listed in the following tables are automatically available for any Kubernetes clusters you create. You do not need to enable monitoring on the resource to get these metrics.

Container Engine for Kubernetes metrics include the following dimensions:

**RESOURCEID**

- The OCID of the resource to which the metric applies.

**RESOURCEDisplayNAME**

- The name of the resource to which the metric applies.

**RESPONSECODE**

- The response code sent from the Kubernetes API server.
RESPONSEGROUP

The response code group, based on the response code's first digit (for example, 2xx, 3xx, 4xx, 5xx).

CLUSTERID

The OCID of the cluster to which the metric applies.

NODEPOOLID

The OCID of the node pool to which the metric applies.

NODESTATE

The state of the compute instance hosting the worker node. For example, ACTIVE, CREATING, DELETING, DELETED, FAILED, UPDATING, INACTIVE.

NODECONDITION

The condition of the worker node, as indicated by the Kubernetes API server. For example, Ready, MemoryPressure, PIDPressure, DiskPressure, NetworkUnavailable.

AVAILABILITYDOMAIN

The availability domain where the compute instance resides.

FAULTDOMAIN

The fault domain where the compute instance resides.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Server Request Count</td>
<td>API Server Requests</td>
<td>count</td>
<td>Number of requests received by the Kubernetes API Server.</td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceDisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>responseCode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>responseGroup</td>
</tr>
<tr>
<td>API Server Response Count</td>
<td>API Server Response Count</td>
<td>count</td>
<td>Number of different non-200 responses (that is, error responses) sent from the Kubernetes API server.</td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceDisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>responseCode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>responseGroup</td>
</tr>
<tr>
<td>Unschedulable Pods</td>
<td>Unschedulable Pods</td>
<td>count</td>
<td>Number of pods that the Kubernetes scheduler is unable to schedule. Not available in clusters running versions of Kubernetes prior to version 1.15.x.</td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceDisplayName</td>
</tr>
</tbody>
</table>
## Container Engine for Kubernetes

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeState</td>
<td>Node State</td>
<td>count</td>
<td>Number of compute nodes in different states.</td>
<td>resourceId, clusterId, nodepoolId, resourceDisplayName, nodeState, nodeCondition, availabilityDomain, faultDomain</td>
</tr>
<tr>
<td>KubernetesNodeCondition</td>
<td>Kubernetes Node Condition</td>
<td>count</td>
<td>Number of worker nodes in different conditions, as indicated by the Kubernetes API server.</td>
<td>resourceId, clusterId, nodepoolId, resourceDisplayName, nodeCondition</td>
</tr>
</tbody>
</table>

### Using the Console

#### To view default metric charts for a single cluster

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.

2. Select the region you are using with Container Engine for Kubernetes.

3. Select the compartment containing the cluster for which you want to view metrics.

   The **Clusters** page shows all the clusters in the compartment you selected.

4. Click the name of the cluster for which you want to view metrics.

5. Under **Resources**, click **Metrics**.

   The **Metrics** tab displays a chart for each metric for the cluster that is emitted by the Container Engine for Kubernetes metric namespace. To see metrics for a node pool in the cluster, display the **Node Pools** tab, click the name of the node pool, and display the **Metrics** tab. To see metrics for a worker node in the node pool, display the **Nodes** tab and click the **View Metrics** link beside the name of the worker node. For more information about the emitted metrics, see **Available Metrics: oci_oke** on page 963.

   For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**Not seeing the cluster metrics data you expect?**

If you don't see the metrics data for a cluster that you expect, see the following possible causes and resolutions.
## Container Engine for Kubernetes

### Problem

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>How to check</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I know the Kubernetes API server returned some error responses but the API Server Response Count chart doesn't show them.</td>
<td>The responses might have been returned outside the time period covered by the API Server Response Count chart.</td>
<td>Confirm the Start Time and End Time cover the period when the responses were returned.</td>
<td>Adjust the Start Time and End Time as necessary.</td>
</tr>
<tr>
<td>I know the Kubernetes API server returned some error responses but the API Server Response Count chart doesn't show them, even though the responses were returned between the Start Time and End Time.</td>
<td>Although the responses were returned between the Start Time and End Time, the x-axis (window of data display) might be excluding the responses.</td>
<td>Confirm the x-axis (window of data display) covers the period when the responses were returned.</td>
<td>Adjust the x-axis (window of data display) as necessary.</td>
</tr>
<tr>
<td>I want to see data in the charts as a continuous line over time, but the line has gaps in it.</td>
<td>This is expected behavior. If there is no metrics data to show in the selected interval, the data line is discontinuous.</td>
<td>Increase the Interval (for example, from 1 minute to 5 minutes, or from 1 minute to 1 hour).</td>
<td>Adjust the Interval as necessary.</td>
</tr>
</tbody>
</table>

### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)
Chapter
13

Data Transfer

This chapter explains how to migrate data to Oracle Cloud Infrastructure using Disk-Based Data Import and Data Transfer Appliance.

Overview of Data Transfer Service

Oracle offers offline data transfer solutions that let you migrate data to Oracle Cloud Infrastructure. You can also export data currently residing in Oracle Cloud Infrastructure to your data center offline. Moving data over the public internet is not always feasible because of high network costs, unreliable network connectivity, long transfer times, and security concerns. Our transfer solutions address these pain points, are easy to use, and provide faster data upload compared to over-the-wire data transfer.

Note:

To simplify this Data Transfer documentation, we generically refer to Object Storage to mean that you can transfer data into a bucket in either the Object Storage tier or Archive Storage tier.

DISK-BASED DATA TRANSFER

You send your data as files on encrypted commodity disk to an Oracle transfer site. Operators at the Oracle transfer site upload the files into your designated Object Storage bucket in your tenancy.

This transfer solution requires you to source and purchase the disk used to transfer data to Oracle Cloud Infrastructure. The disk is shipped back to you after the data is successfully uploaded.

See Data Import - Disk on page 970 for details.

APPLIANCE-BASED DATA TRANSFER

You send your data as files on secure, high-capacity, Oracle-supplied storage appliances to an Oracle transfer site. Operators at the Oracle transfer site upload the data into your designated Object Storage bucket in your tenancy.

This solution supports data transfer when you are migrating a large volume of data and when using a transfer disk is not a practical alternative. You do not need to write any code or purchase any hardware. Oracle supplies the transfer appliance and software required to manage the transfer.

See Data Import - Appliance on page 1015 for details.

APPLIANCE-BASED DATA EXPORT

You export your data from your Oracle Cloud Infrastructure Object Storage bucket to your data center using an Oracle-provided appliance.

This solution is useful if you have media content or processed datasets you need to share with a customer or business partner.

See Appliance Data Export on page 1082 for details.

Supported Regions

Data transfer and export are supported in the following regions:
• US East (Ashburn)
• US West (Phoenix)
• US DoD East (Ashburn)
• US DoD North (Chicago)
• US DoD West (Phoenix)
• Germany Central (Frankfurt)
• UK South (London)
• Japan East (Tokyo)
• Japan Central (Osaka)

Limits on Data Transfer Service Resources

When you sign up for Oracle Cloud Infrastructure, a set of service limits is configured for your tenancy. The service limit is the quota or allowance set on a resource. Verify that your service limits are set appropriately before you begin the data transfer process.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Tagging Resources

Apply tags to your resources to help organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Automation for Objects Using the Events Service

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

Events for objects are handled differently than other resources. Objects do not emit events by default. Use the Console, CLI, or API to enable a bucket to emit events for object state changes. You can enable events for object state changes during or after bucket creation.

Notifications

You can set up different types of notifications to alert you when any change happens to during your data transfer. See Notifications Overview on page 3350.

Note:

To fully utilize notifications, setup events that trigger the notifications. See Overview of Events on page 1784 for more information.

You can also set up notifications for appliance-based import and export jobs using a CLI command. The notifications run from the CLI provides a more convenient process than using the Notifications and Events services. Instructions for setting these CLI-based notifications are in the Preparation topics for appliance-based import and export.

Inputting Text into Data Transfer

You must use only ASCII text for all inputs to Data Transfer. This requirement applies to the browser-based Console and CLIs.

What's Next

Now you are ready to prepare for your data transfer or export. See the following pages for more information on each of the data transfer or export methods:

• Data Import - Disk on page 970
Data Import - Disk

Disk-Based Data Import is one of Oracle's offline data transfer solutions that lets you migrate data to Oracle Cloud Infrastructure. You send your data as files on an encrypted disk to an Oracle transfer site. Operators at the Oracle transfer site upload the files into the designated Object Storage bucket in your tenancy. You are then free to move the uploaded data to other Oracle Cloud Infrastructure services as needed.

Note:
Oracle does not certify or test disks you intend to use for disk import jobs. Calculate your disk capacity requirements and disk I/O to determine what USB 2.0/3.0 disk works best for your data transfer needs.

Disk-Based Data Import Concepts

IMPORT DISK
An import disk is a user-supplied storage device that is specially prepared to copy and upload data to Oracle Cloud Infrastructure. You copy your data to the import disk and ship it in a parcel to Oracle to upload your data.

Disk-Based Data Import supports external USB 2.0/3.0 hard disk drives.

Note:
Pin-code protected devices and physical-key protected devices are currently not supported.

TRANSFER DISK
A transfer disk is the logical representation of an import disk that has been prepared to copy and upload data to Oracle Cloud Infrastructure.

Note:
The terms transfer disk and import disk both represent the disk being used to move your data to Oracle Cloud Infrastructure. Transfer disk is used in the context of configuring the disk within the transfer job and transfer package. Import disk is used when physically handling the disk, such as connecting it to the Data Host or mailing it to Oracle.

TRANSFER JOB
A transfer job is the logical representation of a data migration to Oracle Cloud Infrastructure. A transfer job consists of one or more transfer packages that each contain a single transfer disk.

DATA TRANSFER UTILITY
The Data Transfer Utility is the command line software that Oracle provides for you to prepare the transfer disk for your data and for shipment to Oracle. In addition, you can use this software to manage transfer jobs and packages.

Note:
You can only run Data Transfer Utility tasks for a supported Linux machine. Windows-based machines are not supported in disk-based transfer jobs.
DATA HOST

The host computer on your site that stores the data you intend to copy to the disk for migration to Oracle Cloud Infrastructure.

Note:

Only Linux machines can be used as Data Hosts.

TRANSFER PACKAGE

A transfer package is the logical representation of the parcel containing the transfer disk that you ship to Oracle to upload to Oracle Cloud Infrastructure.

BUCKET

The logical container in Oracle Cloud Infrastructure Object Storage where Oracle operators upload your data. A bucket is associated with a single compartment in your tenancy whose policies determine what actions a user can perform.

DATA TRANSFER ADMINISTRATOR

A new or existing IAM user that has the authorization and permissions to create and manage transfer jobs.

DATA TRANSFER UPLOAD USER

A temporary IAM user that grants Oracle personnel the authorization and permissions to upload the data from your transfer disk to your designated Oracle Cloud Infrastructure Object Storage bucket. Delete this temporary user after your data is uploaded to Oracle Cloud Infrastructure.

Roles and Responsibilities

Depending on your organization, the responsibilities of using and managing the data transfer may span multiple roles. Use the following set of roles as a guideline for how you can assign the various tasks associated with the data transfer.

- **Project Sponsor**: Responsible for the overall success of the data transfer. Project Sponsors usually have complete access to their organization's Oracle Cloud Infrastructure tenancy. They coordinate with the other roles in the organization to complete the implementation of data transfer project. The Project Sponsor is also responsible for signing legal documentation and setting up notifications for the data import.

- **Infrastructure Engineer**: Responsible for integrating the transfer appliance into the organization's IT infrastructure from where the data is being transferred. Tasks associated with this role include connecting the transfer appliance to power, placing it within the network, and setting the IP address through a serial console menu using the provided USB-to-Serial adapter.

- **Data Administrator**: Responsible for identifying and preparing the data to be transferred to Oracle Cloud Infrastructure. This person usually has access to, and expertise with, the data being migrated.

These roles correspond to the various phases of the data transfer described in the following section. A specific role can be responsible for one or more phases.

Task Flow for Disk-Based Data Import

Here is a high-level overview of the tasks involved in transferring data to Oracle Cloud Infrastructure using Data Transfer Disk. Complete one phase before proceeding to the next one. Use the roles previously described to distribute the tasks across individuals or groups within your organization.
Secure Disk Data Transfer to Oracle Cloud Infrastructure

This section highlights the security details of the Data Transfer Service process.

- The Data Transfer Utility uses the standard Linux dm-crypt and LUKS utilities to encrypt block devices.
- The dm-crypt software generates a master AES-256 bit encryption key that is used for all data written to or read from the disk. That key is protected by an encryption passphrase that the user must know to access the encrypted data.
- When the data transfer administrator uses the Data Transfer Utility to create a disk, Oracle Cloud Infrastructure creates a strong encryption passphrase that is displayed to the user and passed to dm-crypt. The passphrase is displayed to standard output only once and cannot be retrieved again. Copy this passphrase to a durable, secure location for future reference.
• For extra security, you can also encrypt your own data with your own encryption keys. Before copying your data to the transfer disk, you can encrypt your data with a tool and encryption key of your choosing. After the data has been uploaded, you would need to use the same tool and encryption key to access the data.
• All network communication between the Data Transfer Utility and Oracle Cloud Infrastructure is encrypted in-transit using Transport Layer Security (TLS).
• After copying your data to a transfer disk, generate a manifest file using the Data Transfer Utility. The manifest contains an index of all of the copied files and generated data integrity hashes. The Data Transfer Utility copies the config_upload_user configuration file and referenced IAM credentials to the encrypted transfer disk. This configuration file describes the temporary IAM data transfer upload user. Oracle uses the credentials and entries defined in the config_upload_user file when processing the transfer disk and uploading files to Oracle Cloud Infrastructure Object Storage.

| Note: |
| Data Transfer Service Does Not Support Passphrases on Private Keys |
| While we recommend encrypting a private key with a passphrase when generating API signing keys, Data Transfer does not support passphrases on the key file required for the config_upload_user. If you use a passphrase, Oracle personnel cannot upload your data. |

Oracle cannot upload data from a transfer disk without the correct credentials defined in this configuration file. See Installing the Data Transfer Utility on page 974 for more information about the required configuration files.

• When you disconnect or lock a transfer disk using the Data Transfer Utility, the original encryption passphrase is required to once again access the disk. If the encryption passphrase is not known or lost, you cannot access the data on the transfer disk. To reuse a transfer disk, you must reformat the disk. Reformatting a disk removes all the data.
• Oracle retrieves the encryption passphrase for a transfer disk from Oracle Cloud Infrastructure. Oracle uses the passphrase to decrypt, mount the transfer disk, and upload the data to the designated bucket in the tenancy.
• After processing a transfer package, Oracle returns the transfer disk attached to the transfer package using the return shipping label you provide.
• To protect your data, we make the data on the disk unrecoverable before shipping the transfer disk back to you. To comply with customs regulations, we wipe the disk completely before shipping it back to international shipping addresses.

Ways to Manage Disk Data Transfers

We provide two ways to manage disk-based data transfers:

• The Data Transfer Utility is a full-featured command line tool for disk-based data transfers only (appliance-based data transfers use a different command line tool). For more information and installation instructions, see Installing the Data Transfer Utility on page 974.
• The Console is an easy-to-use, partial-featured browser-based interface. For more information, see Signing In to the Console on page 41.

| Note: |
| You can perform many data transfer tasks using either the Console or the Data Transfer Utility. However, there are some tasks you can only perform using the Data Transfer Utility (for example, creating and locking the transfer disk). describes the management tasks in detail and guides you to the appropriate management interface to use for each task. |

What's Next

You are now ready to begin preparation for the Disk-Based Data Import. See Preparing for Disk Data Transfers on page 974 for more information.
Preparing for Disk Data Transfers

This topic describes the tasks associated with preparing for the Disk-Based Data Import. The Project Sponsor role typically performs these tasks. See Roles and Responsibilities on page 971.

Import Disk Requirements

You are responsible for performing following tasks in order:

• Purchasing the required number of hard drives to migrate your data to Oracle Cloud Infrastructure. Use USB 2.0/3.0 external hard disk drives (HDD) with a single partitioned file system containing your data.

  Note:
  Oracle does not certify or test disks you intend to use for disk import jobs. Calculate your disk capacity requirements and disk I/O to determine what USB 2.0/3.0 disk works best for your data transfer needs.

• Copying the data to the HDDs following the procedures described in this import disk documentation.

• Shipping the disks to the specified Oracle data transfer site.

After the data is copied successfully to Oracle Cloud Infrastructure Object Storage, the hard drives are shipped back to you in the same encrypted state that they were received.

Installing the Data Transfer Utility

This topic describes how to install and configure the Data Transfer Utility for use in disk-based data transfers. In addition, this topic describes the syntax for the Data Transfer Utility commands.

Important:

With this release, the Data Transfer Utility only supports disk-based data transfers. Use of the Data Transfer Utility for appliance-based transfers has been replaced with the Oracle Cloud Infrastructure command line interface (CLI).

The Data Transfer Utility is licensed under the Universal Permissive License 1.0 and the Apache License 2.0. Third-party content is separately licensed as described in the code.

Note:

The Data Transfer Utility must be run as the root user.

Prerequisites

To install and use the Data Transfer Utility, obtain the following:

• An Oracle Cloud Infrastructure account.

• The required Oracle Cloud Infrastructure users and groups with the required IAM policies.

  See Creating the Required IAM Users, Groups, and Policies on page 980 for details.
• A Data Host machine with the following installed:
  • Oracle Linux 6 or greater, Ubuntu 14.04 or greater, or SUSE 11 or greater. All Linux operating systems must have the ability to create an EXT file system.

  Note:
  Windows-based machines are not supported in disk-based transfer jobs.

  • Java 1.8 or Java 1.11
  • hdparm 9.0 or later
  • Cryptsetup 1.2.0 or greater
  • Firewall access: If you have a restrictive firewall in the environment where you are using the Data Transfer Utility, you may need to open your firewall configuration to the following IP address ranges: 140.91.0.0/16. You also need to open access to the object storage IP address ranges: 134.70.0.0/17.

Installation
Download and install the Data Transfer Utility installer that corresponds to your Data Host's operating system.

To install the Data Transfer Utility on Debian or Ubuntu
1. Download the installation .deb file.
2. Issue the apt install command as the root user that has write permissions to the /opt directory.

   ```
   sudo apt install ./dts-X.Y.Z.x86_64.deb
   ```

   X.Y.Z represents the version numbers that match the installer you downloaded.

3. Confirm that the Data Transfer Utility installed successfully.

   ```
   sudo dts --version
   ```

   Your Data Transfer Utility version number is returned.

To install the Data Transfer Utility on Oracle Linux or Red Hat Linux
1. Download the installation .rpm file.
2. Issue the yum install command as the root user that has write permissions to the /opt directory.

   ```
   sudo yum localinstall ./dts-X.Y.Z.x86_64.rpm
   ```

   X.Y.Z represents the version numbers that match the installer you downloaded.

3. Confirm that the Data Transfer Utility installed successfully.

   ```
   sudo dts --version
   ```

   Your Data Transfer Utility version number is returned.

Configuration
Before using the Data Transfer Utility, you must create a base Oracle Cloud Infrastructure directory and two configuration files with the required credentials. One configuration file is for the data transfer administrator, the IAM user with the authorization and permissions to create and manage transfer jobs. The other configuration file is for the data transfer upload user, the temporary IAM user that Oracle uses to upload your data on your behalf.

Base Data Transfer Directory
Create a base Oracle Cloud Infrastructure directory:

```bash
mkdir /root/.oci/
```
Configuration File for the Data Transfer Administrator

Create a data transfer administrator configuration file /root/.oci/config with the following structure:

```ini
[DEFAULT]
user=<The OCID for the data transfer administrator>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user’s private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>
```

For example:

```ini
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..<unique_ID>.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1
```

For the data transfer administrator, you can create a single configuration file that contains different profile sections with the credentials for multiple users. Then use the `##profile` option to specify which profile to use in the command. Here is an example of a data transfer administrator configuration file with different profile sections:

```ini
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..<unique_ID>.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1

[PROFILE1]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..<unique_ID>.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-ashburn-1
```

By default, the `DEFAULT` profile is used for all Data Transfer Utility commands. For example:

```
dts job create --compartment-id <compartment_id> --bucket <bucket_name> --display-name <display_name> --device-type <disk>
```

Instead, you can issue any Data Transfer Utility command with the `--profile` option to specify a different data transfer administrator profile. For example:

```
dts job create --compartment-id <compartment_id> --bucket <bucket_name> --display-name <display_name> --device-type <disk> --profile <profile_name>
```

Using the example configuration file above, the `<profile_name>` would be `profile1`.

Configuration File for the Data Transfer Upload User

Create a data transfer upload user /root/.oci/config_upload_user configuration file with the following structure:

```ini
[DEFAULT]
user=<The OCID for the data transfer upload user>
```
fingerprint=<The fingerprint of the above user's public key>  
key_file=<The _absolute_ path to the above user's private key file on the host machine>  
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>  
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>

For example:

```
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..<unique_ID>.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1
```

**Important:**

Creating an upload user configuration file with multiple profiles is *not* supported.

**Configuration File Entries**

The following table lists the basic entries that are required for each configuration file and where to get the information for each entry.

**Note:**

Data Transfer Service does not support passphrases on the key files for both data transfer administrator and data transfer upload user.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description and Where to Get the Value</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>OCID of the data transfer administrator or the data transfer upload user, depending on which profile you are creating. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>fingerprint</td>
<td>Fingerprint for the key pair being used. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>key_file</td>
<td>Full path and filename of the private key.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Important:** The key pair must be in PEM format. For instructions on generating a key pair in PEM format, see Required Keys and OCIDs on page 4179.
### Entry

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description and Where to Get the Value</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenancy</td>
<td>OCID of your tenancy. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>region</td>
<td>An Oracle Cloud Infrastructure region. See Regions and Availability Domains on page 180. Data transfer is supported in US East (Ashburn), US West (Phoenix), Germany Central (Frankfurt), and UK South (London).</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You can verify the data transfer upload user credentials using the following command:

```
dts job verify-upload-user-credentials --bucket <bucket_name>
```

### Configuration File Location

The location of the configuration files is `~/oci/config`.

### Using the Data Transfer Utility

This section provides an overview of the syntax for the Data Transfer Utility.

**Important:**

The Data Transfer Utility must be run as the root user.

You can specify Data Transfer Utility command options using the following commands:

- `--option <value>`
- `--option=<value>`

### Syntax

The basic Data Transfer Utility syntax is:

```
dts <resource> <action> <options>
```

This syntax is applied to the following:

- `dts` is the shortened utility command name
- `job` is an example of a `<resource>`
- `create` is an example of an `<action>`
- Other utility strings are `<options>`

The following examples show typical Data Transfer Utility commands to create a transfer job:

```
dts job create --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name "mycompany transfer1" --bucket mybucket --device-type disk
```
Or:

```bash
dts job create --compartment-id=compartment-id 
  ocid.compartment.oc1..exampleuniqueID --display-name="mycompany transfer1"
  --bucket=mybucket --device-type=disk
```

**Note:**
In the previous examples, provide a friendly name for the transfer job using the `--display-name` option. Avoid entering confidential information.

### Finding Out the Installed Version of the Data Transfer Utility

You can get the installed version of the Data Transfer Utility using `--version` or `-v`. For example:

```bash
dts --version
0.6.183
```

### Accessing Data Transfer Utility Help

All Data Transfer Utility help commands have an associated help component you can access from the command line. To view the help, enter any command followed by the `--help` or `-h` option. For example:

```bash
dts job --help
```

**Usage:** `job [COMMAND]`
Transfer disk or appliance job operations — `{job <action> [options]}`

**Commands:**
- `create job` Creates a new transfer disk or appliance job.
- `show details` Shows the transfer disk or appliance job details.
- `update details` Updates the transfer disk or appliance job details.
- `delete` Deletes the transfer disk or appliance job.
- `close` Closes the transfer disk or appliance job.
- `list` Lists all transfer disk or appliance jobs.
- `verify-upload-user-credentials` Verifies the transfer disk or appliance upload user credentials.

When you run the help option (`--help` or `-h`) for a specified command, all the subordinate commands and options for that level of the Data Transfer Utility are displayed. If you want to access the Data Transfer Utility help for a specific subordinate command, include it in the Data Transfer Utility string, for example:

```bash
dts job create --help
```

**Usage:** `job create --bucket=<bucket> --compartment-id=<compartmentId>
  [--defined-tags=<definedTags>] --device-type=<deviceType>
  --display-name=<displayName>
  [--freeform-tags=<freeformTags>] [--profile=<profile>]`

Creates a new transfer disk or appliance job.

- `--bucket=<bucket>` Upload bucket for the job.
- `--compartment-id=<compartmentId>` Compartment OCID.
- `--defined-tags=<definedTags>` Defined tags for the new transfer job in JSON format.
- `--device-type=<deviceType>` Device type for the job: DISK or APPLIANCE.
- `--display-name=<displayName>` Display name for the job.
Creating the Required IAM Users, Groups, and Policies

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization.

To use Oracle Cloud Infrastructure, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in.

Access to resources is provided to groups using policies and then inherited by the users that are assigned to those groups. Data transfer requires the creation of two distinct groups:

- **Data transfer administrators** who can create and manage transfer jobs.
- **Data transfer upload users** who can upload data to Object Storage. For your data security, the permissions for upload users allow Oracle personnel to upload standard and multi-part objects on your behalf and inspect bucket and object metadata. The permissions do not allow Oracle personnel to inspect the actual data.

The Data Administrator is responsible for generating the required RSA keys needed for the temporary upload users. These keys should never be shared between users.

For details on creating groups, see Managing Groups on page 2419.

An administrator creates these groups with the following policies:

- **The data transfer administrator group** requires an authorization policy that includes the following:

  ```
  Allow group <group_name> to manage data-transfer-jobs in compartment <compartment_name>
  Allow group <group_name> to manage objects in compartment <compartment_name>
  Allow group <group_name> to manage buckets in compartment <compartment_name>
  ```

  Alternatively, you can consolidate the `manage buckets` and `manage objects` policies into the following:

  ```
  Allow group <group_name> to manage object-family in compartment <compartment_name>
  ```

- **The data transfer upload user group** requires an authorization policy that includes the following:

  ```
  Allow group <group_name> to manage buckets in compartment <compartment_name> where all
  { request.permission='BUCKET_READ', target.bucket.name='<bucket_name>' }
  ```

  ```
  Allow group <group_name> to manage objects in compartment <compartment_name> where all
  { target.bucket.name='<bucket_name>', any
  { request.permission='OBJECT_CREATE', request.permission='OBJECT_OVERWRITE', request.permission='OBJECT_INSPECT' }}
  ```

To enable notifications, add the following policies:

- **Allow group <group name> to manage ons-topics in tenancy**
- **Allow group <group name> to manage ons-subscriptions in tenancy**
- **Allow group <group name> to manage cloudevents-rules in tenancy**
- **Allow group <group name> to inspect compartments in tenancy**

See Notifications Overview on page 3350 and Overview of Events on page 1784 for more information.
The Oracle Cloud Infrastructure administrator then adds a user to each of the data transfer groups created. For details on creating users, see Managing Users on page 2414.

**Important:**
For security reasons, we recommend that you create a unique IAM data transfer upload user for each transfer job and then delete that user once your data is uploaded to Oracle Cloud Infrastructure.

### Creating Object Storage Buckets

The Object Storage service is used to upload your data to Oracle Cloud Infrastructure. Object Storage stores objects in a container called a bucket within a *compartment* in your tenancy. For details on creating the bucket to store uploaded data, see Managing Buckets on page 3398.

### Configuring Firewall Settings

Ensure that your local environment's firewall can communicate with the Data Transfer Service running on the IP address ranges: 140.91.0.0/16. You also need to open access to the Object Storage IP address ranges: 134.70.0.0/17.

### Creating Transfer Jobs

This section describes how to create a transfer job as part of the preparation for the data transfer. See Transfer Jobs on page 999 for complete details on all tasks related to transfer jobs.

**Tip:**
You can use the Console or the Data Transfer Utility to create a transfer job.

A transfer job represents the collection of files that you want to transfer and signals the intention to upload those files to Oracle Cloud Infrastructure. A transfer job combines at least one transfer disk with a transfer package. Identify which compartment and Object Storage bucket that Oracle is to upload your data to. Create the transfer job in the same compartment as the upload bucket and supply a human-readable name for the transfer job.

**Note:**
It is recommended that you create a compartment for each transfer job to minimize the required access your tenancy.

Creating a transfer job returns a job ID that you specify in other transfer tasks. For example:

```
ocid1.datatransferjob.region1.phx..exampleuniqueID
```

**To create a transfer job using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Select the designated compartment you are to use for data transfers from the list.
   A list of transfer jobs that have already been created is displayed.
3. Click Create Transfer Job.
   The Create Transfer Job dialog appears.
4. Enter a Job Name. Avoid entering confidential information. Then, select the Upload Bucket from the list.
5. Select Disk for the Transfer Device Type.
6. Click Create Transfer Job.

**To create a transfer job using the Data Transfer Utility**

```
dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name>
```

<display_name> is the name of the transfer job. Avoid entering confidential information.
For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocidd.compartment.oc1..exampleuniqueID --display-name MyDiskImportJob
```

```
Transfer Job : 
ID : ocidd.datatransferjob.oc1..exampleuniqueID
CompartmentId : ocidd.compartment.oc1..exampleuniqueID
UploadBucket : MyBucket1
Name : MyDiskImportJob
Label : JZM9PAVWH
CreationDate : 2019/06/04 17:07:05 EDT
Status : PREPARING
freeformTags : *** none ***
definedTags : *** none ***
Packages :
[1] :
Label : PBNZOX9RU
TransferSiteShippingAddress : Oracle Data Transfer Service;
Job:JZM9PAVWH Package:PBNZOX9RU ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
DeliveryVendor : FedEx
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]
UnattachedDevices : [*** none ***]
Appliances : [*** none ***]
```

When you use the `dts job describe` command to display the details of a job, tagging details are also included in the output if you specified tags.

Optional, you can specify one or more defined or free-form tags when you create a transfer job. For more information about tagging, see Resource Tags on page 211.

**Defined Tags**

To specify defined tags when creating a job:

```
dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --defined-tags '{ "<tag_namespace>": { "<tag_key>": "<value>" }}'
```

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocidd.compartment.oc1..exampleuniqueID --display-name MyDiskImportJob --defined-tags '{"Operations": {"CostCenter": "01"}}'
```

```
Transfer Job :
ID : ocidd.datatransferjob.oc1..exampleuniqueID
CompartmentId : ocidd.compartment.oc1..exampleuniqueID
UploadBucket : MyBucket1
Name : MyDiskImportJob
Label : JZM9PAVWH
CreationDate : 2019/06/04 17:07:05 EDT
Status : PREPARING
freeformTags : *** none ***
definedTags :
  Operations :
    CostCenter : 01
Packages :
[1] :
  Label : PBNZOX9RU
```
TransferSiteShippingAddress : Oracle Data Transfer Service;
Job:JZM9PAVWH Package:PBNZOX9RU ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
DeliveryVendor : FedEx
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]
UnattachedDevices : [*** none ***]
Appliances : [*** none ***]

When you use the to display the details of a job, tagging details are also included in the output if you specified tags.

Note:
Users create tag namespaces and tag keys with the required permissions. These items must exist before you can specify them when creating a job. See Working with Defined Tags on page 3914 for details.

Freeform Tags
To specify freeform tags when creating a job:

dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --freeform-tags '{ "<tag_key>"":"<value>" }'

For example:

oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyDiskImportJob --defined-tags '{"Operations": {"CostCenter": "01"}}'

Transfer Job :
ID : ocid1.datatransferjob.oc1..exampleuniqueID
CompartmentId : ocid.compartment.oc1..exampleuniqueID
UploadBucket : MyBucket1
Name : MyDiskImportJob
Label : JZM9PAVWH
CreationDate : 2019/06/04 17:07:05 EDT
Status : PREPARING
freeformTags :
Pittsburg_Team : brochures
definedTags : [*** none ***]
Packages :
[1] :
Label : PBNZOX9RU
TransferSiteShippingAddress : Oracle Data Transfer Service;
Job:JZM9PAVWH Package:PBNZOX9RU ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
DeliveryVendor : FedEx
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]
UnattachedDevices : [*** none ***]
Appliances : [*** none ***]

When you use the to display the details of a job, tagging details are also included in the output if you specified tags.

Multiple Tags
To specify multiple tags, comma separate the JSON-formatted key/value pairs:

```
dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type disk --freeform-tags '{ "<tag_key>":"<value>" }', '{ "<tag_key>":"<value>" }'
```

**Getting Transfer Job IDs**

Each transfer job you create has a unique ID within Oracle Cloud Infrastructure. For example:

```
ocid1.datatransferjob.region1.phx..<unique_ID>
```

You will need to forward this transfer job ID to the Data Administrator.

*To get the transfer job ID using the Console*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list.
   
The transfer jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the transfer job whose details you want to view.
   
   Alternatively, you can click the **Actions** icon (⋮), and then click **View Details**.
   
The Details page for that transfer job appears.
4. Find the **OCID** field in the Details page and click **Show** to display it or **Copy** to copy it to your computer.

*To get the transfer job ID using the CLI*

```
dts job list --compartment-id <compartment_id>
```

For example:

```
dts job list --compartment-id ocid.compartment.oc1..exampleuniqueID
```

**Transfer Job List**:

```
[1] :
   ID : ocid1.datatransferjob.oc1..exampleuniqueID
   Name : MyDiskImportJob
   Label : JVWK5YWPU
   BucketName : MyBucket1
   CreationDate : 2020/06/01 17:33:16 EDT
   Status : INITIATED
   FreeformTags : *** none ***
   DefinedTags :
   Financials :
      key1 : nondefault
```

The ID for each transfer job is returned:

```
ID : ocid1.datatransferjob.oc1..exampleuniqueID
```

**Tip:**

When you create a transfer job using the `dts job create` CLI, the transfer job ID is displayed in the CLI's return.
Creating Upload Configuration Files

The Project Sponsor is responsible for creating or obtaining configuration files that allow the uploading of user data to the transfer appliance. Send these configuration files to the Data Administrator where they can be placed in the Data Host. The `config` file is for the data transfer administrator, the IAM user with the authorization and permissions to create and manage transfer jobs. The `config_upload_user` file is for the data transfer upload user, the temporary IAM user that Oracle uses to upload your data on your behalf.

Create a base Oracle Cloud Infrastructure directory and two configuration files with the required credentials.

Creating the Data Transfer Directory

Create an Oracle Cloud Infrastructure directory (`.oci`) on the same Data Host where the CLI is installed. For example:

```bash
mkdir /root/.oci/
```

The two configuration files (`config` and `config_upload_user`) are placed in this directory.

Creating the Data Transfer Administrator Configuration File

Create the data transfer administrator configuration file `/root/.oci/config` with the following structure:

```
[DEFAULT]
user=<The OCID for the data transfer administrator>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user's private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>
```

For example:

```
[DEFAULT]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..exampleuniqueID
region=us-phoenix-1
```

For the data transfer administrator, you can create a single configuration file that contains different profile sections with the credentials for multiple users. Then use the `##profile` option to specify which profile to use in the command.

Here is an example of a data transfer administrator configuration file with different profile sections:

```
[DEFAULT]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..exampleuniqueID
region=us-phoenix-1

[PROFILE1]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..exampleuniqueID
region=us-ashburn-1
```

By default, the `DEFAULT` profile is used for all CLI commands. For example:

```bash
oci dts job create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket MyBucket --display-name MyDisplay --device-type disk
```

Instead, you can issue any CLI command with the `--profile` option to specify a different data transfer administrator profile. For example:

```bash
oci dts job create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket MyBucket --display-name MyDisplay --device-type disk --profile MyProfile
```

Using the example configuration file above, the `<profile_name>` would be `profile1`.

If you created two separate configuration files, use the following command to specify the configuration file to use:

```bash
oci dts job create --compartment-id <compartment_id> --bucket <bucket_name> --display-name <display_name>
```

### Creating the Data Transfer Upload User Configuration File

The `config_upload_user` configuration file is for the data transfer upload user, the temporary IAM user that Oracle uses to upload your data on your behalf. Create this configuration file with the following structure:

```ini
[DEFAULT]
user=<The OCID for the data transfer upload user>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user’s private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>
```

### Adding Object Storage Endpoints

Include the line `endpoint=<url>` for the Object Storage API endpoint in the upload user configuration file.

For example:

```ini
endpoint=https://objectstorage.us-phoenix-1.oraclecloud.com
```

Click here to view a list of endpoints.

A complete configuration including the Object Storage endpoint might look like this:

```ini
[DEFAULT]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..exampleuniqueID
region=us-phoenix-1
endpoint=https://objectstorage.us-phoenix-1.oraclecloud.com
```

**Important:**

Creating an upload user configuration file with multiple profiles is not supported.
### Configuration File Entries

The following table lists the basic entries that are required for each configuration file and where to get the information for each entry.

**Note:**
Data Transfer Service does not support passphrases on the key files for both data transfer administrator and data transfer upload user.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description and Where to Get the Value</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>OCID of the data transfer administrator or the data transfer upload user, depending on which profile you are creating. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>fingerprint</td>
<td>Fingerprint for the key pair being used. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>key_file</td>
<td>Full path and filename of the private key. <strong>Important:</strong> The key pair must be in PEM format. For instructions on generating a key pair in PEM format, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>tenancy</td>
<td>OCID of your tenancy. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>region</td>
<td>An Oracle Cloud Infrastructure region. See <strong>Regions and Availability Domains</strong> on page 180.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Data transfer is supported in US East (Ashburn), US West (Phoenix), Germany Central (Frankfurt), and UK South (London).

You can verify the data transfer upload user credentials using the following command:

```
dts job verify-upload-user-credentials --bucket <bucket_name>
```
Creating Transfer Packages

A transfer package is the virtual representation of the physical disk package that you are shipping to Oracle for upload to Oracle Cloud Infrastructure. See Transfer Packages on page 1012 for complete details on all tasks related to transfer packages.

Creating a transfer package requires the job ID returned from when you created the transfer job. For example:

```
ocid1.datatransferjob.region1.phx..exampleuniqueID```

To create a transfer package using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job for which you want to create a transfer package.
3. Click the Actions icon ( chặn ), and then click View Details.

   Alternatively, click the hyperlinked name of the transfer job.

   A list of transfer packages that have already been created is displayed.
4. Click Create Transfer Package.

   The Create Transfer Package dialog appears.
5. Select a Vendor from the list.
6. Click Create Transfer Package.

   The Data Transfer Package dialog appears displaying information such as the shipping address, the shipping vendor, and the shipping status.

To create a transfer package using the Data Transfer Utility

At the command prompt on the Data Host, run dts package create to create a transfer package.

```
dts package create --job-id <job_id>```

The following information is returned:

```
Transfer Package :
Label :
TransferSiteShippingAddress :
DeliveryVendor :
DeliveryTrackingNumber :
ReturnDeliveryTrackingNumber :
Status :
Devices :
```

Getting Transfer Package Labels

To get the transfer package label using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job for which you want to see the details.
3. Click the Actions icon ( chặn ), and then click View Details.

   Alternatively, click the hyperlinked name of the transfer job.
4. Click Transfer Packages under Resources.

   A list of transfer packages associated with the transfer job is displayed.
To get the transfer package label using the Data Transfer Utility

```
dts job show --job-id <job_id>
```

For example:

```
dts job show --job-id ocid1.datatransferjob.oc1..exampleuniqueID
```

Transfer Job :

<table>
<thead>
<tr>
<th>ID</th>
<th>ocid1.datatransferjob.oc1..exampleuniqueID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompartmentId</td>
<td>ocid.compartment.oc1..exampleuniqueID</td>
</tr>
<tr>
<td>UploadBucket</td>
<td>MyBucket1</td>
</tr>
<tr>
<td>Name</td>
<td>MyDiskImportJob</td>
</tr>
<tr>
<td>Label</td>
<td>JZM9PAVWH</td>
</tr>
<tr>
<td>CreationDate</td>
<td>2019/06/04 17:07:05 EDT</td>
</tr>
<tr>
<td>Status</td>
<td>PREPARING</td>
</tr>
<tr>
<td>freeformTags</td>
<td>*** none ***</td>
</tr>
<tr>
<td>definedTags</td>
<td>*** none ***</td>
</tr>
<tr>
<td>Packages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[1] :</td>
</tr>
<tr>
<td>Label</td>
<td>PBNZOX9RU</td>
</tr>
<tr>
<td>TransferSiteShippingAddress</td>
<td>Oracle Data Transfer Service;</td>
</tr>
<tr>
<td>Job:JZM9PAVWH</td>
<td>Package:PBNZOX9RU ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA</td>
</tr>
<tr>
<td>DeliveryVendor</td>
<td>FedEx</td>
</tr>
<tr>
<td>DeliveryTrackingNumber</td>
<td>*** none ***</td>
</tr>
<tr>
<td>ReturnDeliveryTrackingNumber</td>
<td>*** none ***</td>
</tr>
<tr>
<td>Status</td>
<td>PREPARING</td>
</tr>
<tr>
<td>Devices</td>
<td>[*** none ***]</td>
</tr>
<tr>
<td>UnattachedDevices</td>
<td>[*** none ***]</td>
</tr>
<tr>
<td>Appliances</td>
<td>[*** none ***]</td>
</tr>
</tbody>
</table>

The transfer package label is displayed as part of the job details.

Getting Shipping Labels

You can find the shipping address in the transfer package details. Use this information to get a shipping label for the transfer package that is used to send the disk to Oracle.

After getting the shipping labels from the Console or Data Transfer Utility, go to the supported carrier you are using (UPS, FedEx, or DHL) and manually create both the SHIP TO ORACLE and RETURN TO CUSTOMER labels. See Shipping Import Disks on page 995 and Monitoring the Import Disk Shipment and Data Transfer on page 997 for information.

To get the shipping address for a transfer package using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job for which you want to see the details.
3. Click the Actions icon ( ), and then click View Details.
   Alternatively, click the hyperlinked name of the transfer job.
   A list of transfer packages that have already been created is displayed.
4. Find the transfer package for which you want to see the details.
5. Click the Actions icon ( ), and then click View Details.
   Alternatively, click the hyperlinked name of the transfer job.
**Data Transfer**

To get the shipping address for a transfer package using the Data Transfer Utility

```
dts package show --job-id <job_id> --package-label <package_label>
```

For example:

```
dts package show --job-id ocid1.datatransferjob.oc1..exampleuniqueID --package-label PWA8067MI
```

Transfer Package:
```
Label : PWA8067MI
TransferSiteShippingAddress : Oracle Data Transfer Service;
Job:JZM9PAVWH Package:PWA8067MI ; 21111 Ridgetop Circle; Dock B; Sterling,
VA 20166; USA
DeliveryVendor : *** none ***
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]
```

**Notifying the Data Administrator**

When you have completed all the tasks in this topic, provide the Data Administrator of the following:

- IAM login credentials
- Data Transfer Utility configuration files
- Transfer job ID
- Package label

**What’s Next**

You are now ready to configure your system for the data transfer. See Configuring Import Disk Data Transfers on page 990.

### Configuring Import Disk Data Transfers

This topic describes the tasks associated with configuring the Disk-Based Data Import. The Infrastructure Engineer role typically performs these tasks. See Roles and Responsibilities on page 971.

Configuration for the Disk-Based Data Import consists of the following tasks:

- Attaching the import disk to the Data Host. Remove all partitions and any file systems. To prevent the accidental deletion of data, the Data Transfer Utility does not work with disks that already have partitions or file systems. Disks are visible to the host as block devices and must provide a valid response to the `hdparm -i <device>` Linux command.
- Sending the block device path to the Data Administrator.

**What’s Next**

You are now ready to load your data to the transfer disk. See Copying the Data to the Import Disk on page 990.

### Copying the Data to the Import Disk
This topic describes the tasks associated with running the data transfer from the Data Host to the import disk. The Data Administrator role typically performs these tasks. See Roles and Responsibilities on page 971.

**Information Prerequisites**

Before performing any disk copying tasks, you must obtain the following information:

- Disk block device path. The Infrastructure Engineer typically provides this information.
- IAM login information, Data Transfer Utility configuration files, transfer job ID, and package label. The Project Sponsor typically provides this information.

**Creating the Transfer Disk**

The transfer disk is the logical representation of the physical import disk that has been configured for use for receiving data as part of the disk-based data transfer. See Transfer Disks on page 1008 for complete details on all tasks related to transfer disks.

**Note:**
You can only use the Data Transfer Utility to create a transfer disk.

When you create a transfer disk for use with the disk on which you are copying your files, the Data Transfer Utility:

- Sets up the disk for encryption using the passphrase
- Creates a file system on the disk
- Mounts the file system at `/mnt/orcdts_<label>`

For example:

```
/mnt/orcdts_DJZNWK3ET
```

When you register a transfer disk, Oracle Cloud Infrastructure generates a strong encryption passphrase that is used to encrypt the contents on the disk. The encryption passphrase is displayed to standard output to the data transfer administrator user and cannot be retrieved again. Create a local, secure copy of the encryption passphrase, so you can reference the passphrase again.

Creating a transfer disk requires the job ID returned from when you created the transfer job and the path to the attached disk (for example, `/dev/sdb`).

**To create a transfer disk using the Data Transfer Utility**

At the command prompt on the host, run `dts disk create` to create a transfer disk.

```
dts disk create --job-id <job_id> --block-device <block_device>
```

**Copying Files to the Disk**

You can only copy regular files to the disk. You cannot copy special files, such as symbolic links, device special, sockets, and pipes, directly to the disk. See the following section for instructions on how to prepare special files.

**Important:**

- Individual files being copied to the disk cannot exceed 9.76 TB.
- Do not fill up the disk to 100% capacity. There must be space available to generate metadata and for the manifest file to perform the upload to Object Storage. At least 1 GB of free disk space is needed for this area.

Attach the disk to the Data Host and copy files to the mount point created by `disk` through the Data Transfer Utility.

**Note:**

Only Linux machines can be used as Data Hosts.
**Note:**

Copy all Files Before Disconnecting the Disk

Do not disconnect the disk until you copy all files from the Data Host and generate the manifest file. If you accidentally disconnect the disk before copying all files, you must unlock the disk using the encryption passphrase. The encryption passphrase was generated and displayed when you created the transfer disk. If the generated encryption passphrase is not available, you must delete the transfer disk from the transfer job and re-create the transfer disk. All data previously copied to that disk is lost.

**Copying Special Files**

To transfer special files, create a tar archive of these files and copy the tar archive to the Data Transfer Appliance. We recommend copying many small files using a tar archive. Copying a single compressed archive file should also take less time than running copy commands such as `cp -r` or `rsync`.

Here are some examples of creating a tar archive and getting it onto the Data Transfer Appliance:

- Running a simple tar command:

  ```
tar -cvzf /mnt/nfs-dts-1/filesystem.tgz filesystem/
  ```

- Running a command to create a file with md5sum hashes for each file in addition to the tar archive:

  ```
tar cvzf /mnt/nfs-dts-1/filesystem.tgz filesystem/ | xargs -I '{}' sh -c "test -f '{}' && md5sum '{}"" | tee tarzip_md5
  ```

The tar archive file `filesystem.tgz` has a base64 md5sum once it is uploaded to OCI Object Storage. Store the `tarzip_md5` file where you can retrieve it. After the compressed tar archive file is downloaded from Object Storage and unpacked, you can compare the individual files against the hashes in the file.

**Generating the Manifest File**

**Note:**

You can only use the Data Transfer Utility to generate a manifest file. The amount of time to generate the manifest file depends on the size of the upload files, disk speed, and available processing power.

After copying your data to a transfer disk, generate a manifest file using the Data Transfer Utility. The manifest contains an index of all of the copied files and generated data integrity hashes. The Data Transfer Utility copies the `config_upload_user` configuration file and referenced IAM credentials to the encrypted transfer disk. This configuration file describes the temporary IAM data transfer upload user. Oracle uses the credentials and entries defined in the `config_upload_user` file when processing the transfer disk and uploading files to Oracle Cloud Infrastructure Object Storage.

**Note:**

Data Transfer Service Does Not Support Passphrases on Private Keys

While we recommend encrypting a private key with a passphrase when generating API signing keys, Data Transfer does not support passphrases on the key file required for the `config_upload_user`. If you use a passphrase, Oracle personnel cannot upload your data.

Oracle cannot upload data from a transfer disk without the correct credentials defined in this configuration file. See [Installing the Data Transfer Utility](#) on page 974 for more information about the required configuration files.
To create a manifest file using the Data Transfer Utility

At the command prompt on the Data Host, run `dts disk manifest` to create a manifest file.

```
dts disk manifest --job-id <job_id> --disk-label <disk_label>[--object-name-prefix <object_name_prefix>]
```

**Note:**

Do You Need to Regenerate the Manifest File?

If you add, remove, or modify any files on the disk after generating the manifest file, you must regenerate the file. If the manifest file does not match the contents of the target bucket, Oracle cannot upload the data.

Locking the Transfer Disk

**Note:**

You can only use the Data Transfer Utility to lock a transfer disk.

Locking a transfer disk safely unmounts the disk and removes the encryption passphrase from the Data Host.

To lock a transfer disk using the Data Transfer Utility

At the command prompt on the Data Host, run `dts disk lock` to lock a transfer disk.

```
dts disk lock --job-id <job_id> --disk-label <disk_label> --block-device <block_device>
```

Unlocking the Transfer Disk

**Note:**

You can only use the Data Transfer Utility to unlock a transfer disk.

When unlocking the transfer disk, you are prompted for the encryption passphrase that was generated when you created the transfer disk.

To unlock a transfer disk using the Data Transfer Utility

At the command prompt on the Data Host, run `dts disk unlock` to unlock a transfer disk.

```
dts disk unlock --job-id <job_id> --disk-label <disk_label> --block-device <block_device> --encryption-passphrase <encryption_passphrase>
```

Attaching the Transfer Disk to the Transfer Package

Attach a transfer disk to a transfer package after you have performed the following tasks:

1. Copied your data onto the disk
2. Generated the required manifest file
3. Run and reviewed the dry-run report
4. Locked the transfer disk in preparation for shipment

A disk can be attached to one package, detached, and then attached to another package. In some cases, you have attached a transfer disk to a transfer package, but have changed your mind about shipping that disk with the transfer package. You can also detach a transfer disk from one transfer package and attach that disk to a different transfer package.

To attach a transfer disk to a transfer package using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job associated with the transfer package that you want to attach a disk to.
3. Click the **Actions** icon ( ), and then click **View Details**.
   A list of transfer packages is displayed.
4. Find the transfer package that you want to attach a disk to.
5. Click the **Actions** icon ( ), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer package.
   A list of transfer disks is displayed.
6. Click **Attach Transfer Disks**.
   The Attach Transfer Disks dialog appears.
7. Select the **Transfer Disks** that you want to attach to the transfer package.
8. Click **Attach**.

To attach a transfer disk to a transfer package using the Data Transfer Utility

At the command prompt on the Data Host, run `dts disk attach` to attach a disk to a transfer package.

```bash
dts disk attach --job-id <job_id> --package-label <package_label> --disk-label <disk_label>
```

**Detaching the Transfer Disk from the Transfer Package**

To detach a transfer disk from a transfer package using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer package for which you want to detach a transfer disk.
3. Click the **Actions** icon ( ), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer package.
   A list of transfer disks that have already been attached is displayed.
4. Find the transfer disk that you want to detach.
5. Click the **Actions** icon ( ), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer disk.
6. Click **Detach Transfer Disk**.

To detach a transfer disk from a transfer package using the Data Transfer Utility

At the command prompt on the Data Host, run `dts disk detach` to detach a disk from a transfer package.

```bash
dts disk detach --job-id <job_id> --package-label <package_label> --disk-label <disk_label>
```

**Setting Tracking Details on the Transfer Package**

After delivering the transfer package to the shipping vendor, update the transfer package with the tracking information.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle cannot process a transfer package until you update the tracking information.</td>
</tr>
</tbody>
</table>

To update the transfer package with tracking information using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer job for which you want to see the associated transfer packages.
3. Click the Actions icon (‡), and then click View Details.
   A list of transfer packages that have already been created is displayed.
4. Find the transfer package that you want to update.
5. Click the Actions icon (‡), and then click View Details.
6. Click Edit.
7. Enter the Tracking ID and the Return Tracking ID.
8. Click Edit Transfer Package.

To update the transfer package with tracking information using the Data Transfer Utility

At the command prompt on the host, run `dts package ship` to update the transfer package tracking information.

```bash
dts package ship --job-id <job_id> --package-label <package_label> --package-vendor <vendor_name> --tracking-number <tracking_number> --return-tracking-number <return_tracking_number>
```

Notifying the Infrastructure Engineer

After completing the tasks listed in this topic, notify the Infrastructure Engineer of the following:

- Disconnect the physical disk from the Data Host
- Package the disk for shipment

What’s Next

You are now ready to ship your disk with the copied data to Oracle. See Shipping Import Disks on page 995.

Shipping Import Disks

![Flowchart](flowchart.png)

This topic describes the tasks associated with shipping the import disk containing the copied data to Oracle. The Infrastructure Engineer role typically performs these tasks. See Roles and Responsibilities on page 971.

Disconnecting the Transfer Disk from the Data Host

Do not disconnect the import disk until you copy all files from the Data Host and generate the manifest file. See Copying the Data to the Import Disk on page 990 for more information.

Printing Shipping Labels

You should receive the shipping labels electronically from the Project Sponsor. Print them on the appropriate labels for shipping the import disk. See Getting Shipping Labels on page 989 for more information.

Packaging and Shipping the Import Disk

General

Include the required return shipping label in the box when packaging the import disk for shipment.

**Note:**

If you do not include the return shipping label inside the box, Oracle cannot process the transfer package.

Ensure that the transfer job and transfer package label are clearly readable on the outside of the box containing the import disk.
**Important:**

If you are shipping transfer disks to London or Frankfurt, request that the shipping vendor requires a signature delivery.

**Listing Disk Delivery Vendors**

You can view the vendors available for delivery of your import disk to Oracle Cloud Infrastructure.

**Note:**

Available vendors for transfer disk delivery to Oracle Cloud Infrastructure can vary over time. Have the latest version of the Data Transfer Utility installed to view the current list.

**Note:**

You can only use the Data Transfer Utility to lock an transfer disk.

To list the vendors available for delivering the transfer disk to Oracle Cloud Infrastructure

At the command prompt on the Data Host, run `dts package list-delivery-vendors` to list the available delivery vendors.

```
dts package list-delivery-vendors

Delivery Vendors :
[1] : FedEx
[3] : UPS
```

**Shipping Import Disks Internationally**

Create a commercial invoice when shipping transfer disks internationally. To ensure that packages are not held up in customs, follow these guidelines when creating the commercial invoice:

- Show a unique reference number.
- Show the "bill-to party" as follows:
  - For shipments to the European Union (Frankfurt) location:
    ORACLE Deutschland B.V. & Co. KG Riesstrasse 25 Munich, 80992 GERMANY
  - For shipments to the United States location:
    Oracle America, Inc. 500 Oracle Parkway REDWOOD CITY CA 94065 UNITED STATES
- Show the "ship-to party" as the address provided in the transfer package details. See Getting Shipping Labels on page 989 for details.
- State that "The value shown includes the value of software and data recorded onto the hard drive unit."
- State that the "Goods are free of charge - no payment required."
- State that the type of export is "Temporary."
- Ensure that the commodity code shows the correct HS code for a hard drive unit as specified in the source country's HS code list.
- State the description as the manufacture's description of the hard drive unit and include the words "Hard Disk Drive."
- Ensure that the invoice is signed and includes the printed name of the signer.
What's Next

Now you can track your transfer disk shipment and review post transfer logs and summaries. See Monitoring the Import Disk Shipment and Data Transfer on page 997.

Monitoring the Import Disk Shipment and Data Transfer

This topic describes the monitoring tasks to do after sending the import disk with the copied data to Oracle for data transfer to Oracle Cloud Infrastructure. The Project Sponsor role typically performs these tasks. See Roles and Responsibilities on page 971.

Tracking the Import Disk Shipment

When Oracle has processed the transfer (import) disk associated with a transfer package, the status of the transfer package changes to Processed. When Oracle has shipped the disk, the status of the transfer package changes to Returned.

To check the status of a transfer package using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Choose the data transfer package for which you want to display the details.
3. Click the Actions icon ( ), and then click View Details.
4. Look at the Status.

To check the status of a transfer package using the Data Transfer Utility

At the command prompt on the Data Host, run dts package show to show the status of a transfer package.

\[ dts \text{ package show \ --job-id <job_id> \ --package-label <package_label>} \]

For example:

\[ dts \text{ package show \ --job-id ocid1.datatransferjob.oci1..exampleuniqueID \ --package-label PWA8067MI} \]

Transfer Package :
Label : PWA8067MI
TransferSiteShippingAddress : Oracle Data Transfer Service; Job:JZM9PAVWH Package:PWA8067MI ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
DeliveryVendor : *** none ***
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]

Reviewing the Upload Summary

Oracle creates upload summary log files for each uploaded import disk. These logs are placed in the bucket where the data was uploaded to Oracle Cloud Infrastructure. The upload summary file compares the import disk's manifest file to the contents of the target Oracle Cloud Infrastructure Object Storage bucket after file upload.

The top of the log report summarizes the overall file processing status:

P - Present: The file is present in both the disk and the target bucket
M - Missing: The file is present in the disk but not the target bucket. It was likely uploaded and then deleted by another user before the summary was generated.
C - Name Collision: The file is present in the manifest but a file with the same name but different contents is present in the target bucket.
U - Unreadable: The file is not readable from the disk
N - Name Too Long: The file name on disk is too long and could not be uploaded

Complete file upload details follow the summary.

Viewing Data Transfer Metrics

After the import disk with your copied data is received by Oracle and the data transfer begins, you can view the metrics associated with the transfer job in the Transfer Appliance Details page in chart or table format.

Tip:
Set up your notifications to alert you when the data transfer from the import disk to Oracle Cloud Infrastructure is occurring. When the state changes from ORACLE_RECEIVED to PROCESSING, you can start viewing data transfer metrics.

Select **Metrics** under **Resources** to display each of these measures:

- **Import Files Uploaded** - Total number of files uploaded for import.
- **Import Bytes Uploaded** - Total number of bytes uploaded for import.
- **Import Files Remaining** - Total number of files remaining for import upload.
- **Import Bytes Remaining** - Total number of bytes remaining for import upload.
- **Import Files in Error** - Total number of files in error for import.
- **Import Upload Verification Progress** - Progress of verification of files that have already been uploaded for import.

Select the **Start Time** and **End Time** for these measures, either by manually entering the days and times in their respective fields, or by selecting the Calendar feature and picking the times that way. As an alternative to selecting a start and end time, you can also select from a list of standard times (last hour, last 6 hours, and so forth) from the **Quick Selects** list for the period measured. The time period you specify applies to all the measures.

Specify the **Interval** (for example, 5 minutes, 1 hour) that each measure is recorded from the list.

Specify the **Statistic** being recorded (for example, Sum, Mean) for each measure from the list.

Tip:
Mean is the most useful statistic for data transfer as it reflects an absolute value of the metric.

Choose additional actions from the **Options** list, including viewing the query in the **Metrics Explorer**, capturing the URL for the measure, and switching between chart and table view.

Click **Reset Charts** to delete any existing information in the charts and begin recording new metrics.

See **Monitoring Overview** on page 2660 for general information on monitoring your Oracle Cloud Infrastructure services.
**Closing the Transfer Job**

Typically, you would close a transfer job when no further transfer job activity is required or possible. Closing a transfer job requires that the status of all associated transfer packages be returned, canceled, or deleted. In addition, the status of the associated transfer disk must be complete, in error, missing, canceled, or deleted.

*To close a transfer job using the Console*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the data transfer package for which you want to display the details.
3. Click the **Actions** icon (.), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer job.
4. Click **Close Transfer Job**.

*To close a transfer job using the Data Transfer Utility*

At the command prompt on the host, run `dts job close` to close a transfer job.

```
dts job close --job-id <job_id>
```

**What's Next**

You have completed the process of setting up, running, and monitoring the import disk-based data transfer. After the disk contents is successfully migrated to Oracle Cloud Infrastructure, your physical disk is erased and returned to you.

If you determine that another disk-based data transfer is required, repeat the procedure from the beginning.

**Disk Import Reference**

This topic provides complete task details for certain components associated with Disk-Based Data Imports. Use this topic as a reference to learn and use commands associated with components included in the Disk-Based Data Import procedure.

**Transfer Jobs**

A transfer job represents the collection of files that you want to transfer and signals the intention to upload those files to Oracle Cloud Infrastructure. A transfer job combines at least one transfer disk with a transfer package. Identify which compartment and Object Storage bucket to which Oracle will upload your data.

**Tip:**

Create a compartment for each transfer job to minimize the required access your tenancy.

*Creating Transfer Jobs*

Create the transfer job in the same compartment as the upload bucket and supply a human-readable name for the transfer job.

Creating a transfer job returns a job ID that you specify in other transfer tasks. For example:

```
ocid1.datatransferjob.region1.phx..<unique_ID>
```

*To create a transfer job using the Console*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the designated compartment you are to use for data transfers from the list.
   A list of transfer jobs that have already been created is displayed.
3. Click **Create Transfer Job**.
   
   The Create Transfer Job dialog appears.

4. Enter a **Job Name**. Avoid entering confidential information. Then, select the **Upload Bucket** from the list.

5. Select **Disk** for the **Transfer Device Type**.

6. Click **Create Transfer Job**.

To create a transfer job using the Data Transfer Utility

```
dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name>
```

<display_name> is the name of the transfer job. Avoid entering confidential information.

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyDiskImportJob
```

Transfer Job:

<table>
<thead>
<tr>
<th>ID</th>
<th>ocid1.datatransferjob.oc1..exampleuniqueID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompartmentId</td>
<td>ocid.compartment.oc1..exampleuniqueID</td>
</tr>
<tr>
<td>UploadBucket</td>
<td>MyBucket1</td>
</tr>
<tr>
<td>Name</td>
<td>MyDiskImportJob</td>
</tr>
<tr>
<td>Label</td>
<td>JZM9PAVWH</td>
</tr>
<tr>
<td>CreationDate</td>
<td>2019/06/04 17:07:05 EDT</td>
</tr>
<tr>
<td>Status</td>
<td>PREPARING</td>
</tr>
<tr>
<td>freeformTags</td>
<td>*** none ***</td>
</tr>
<tr>
<td>definedTags</td>
<td>*** none ***</td>
</tr>
<tr>
<td>Packages</td>
<td></td>
</tr>
<tr>
<td>[1]</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>PBNZOX9RU</td>
</tr>
<tr>
<td>TransferSiteShippingAddress</td>
<td>Oracle Data Transfer Service;</td>
</tr>
<tr>
<td>Job:JZM9PAVWH Package:PBNZOX9RU</td>
<td>21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA</td>
</tr>
<tr>
<td>DeliveryVendor</td>
<td>FedEx</td>
</tr>
<tr>
<td>DeliveryTrackingNumber</td>
<td>*** none ***</td>
</tr>
<tr>
<td>ReturnDeliveryTrackingNumber</td>
<td>*** none ***</td>
</tr>
<tr>
<td>Status</td>
<td>PREPARING</td>
</tr>
<tr>
<td>Devices</td>
<td>[*** none ***]</td>
</tr>
<tr>
<td>UnattachedDevices</td>
<td>[*** none ***]</td>
</tr>
<tr>
<td>Appliances</td>
<td>[*** none ***]</td>
</tr>
</tbody>
</table>

When you use the `oci dts job create` command to display the details of a job, tagging details are also included in the output if you specified tags.

Optionally, you can specify one or more defined or free-form tags when you create a transfer job. For more information about tagging, see **Resource Tags** on page 211.

**Defined Tags**

To specify defined tags when creating a job:

```
dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --defined-tags '{ "<tag_namespace>": { ";<tag_key>": "<value>" } }'
```

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyDiskImportJob --defined-tags '{"Operations": {"CostCenter": "01"}}'
```

Transfer Job:
To specify freeform tags when creating a job:

```bash
dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --freeform-tags '{ "<tag_key>":"<value>" }'
```

For example:

```bash
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyDiskImportJob --defined-tags '{"Operations": {"CostCenter": "01"}}'
```

Transfer Job:
- ID: ocid1.datatransferjob.oc1..exampleuniqueID
- CompartmentId: ocid.compartment.oc1..exampleuniqueID
- UploadBucket: MyBucket1
- Name: MyDiskImportJob
- Label: JZM9PAVWH
- CreationDate: 2019/06/04 17:07:05 EDT
- Status: PREPARING
- freeformTags: Pittsburg_Team: brochures
- definedTags: *** none ***
- Packages:
  - [1]:
    - Label: PBNZOX9RU
    - TransferSiteShippingAddress: Oracle Data Transfer Service; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
    - DeliveryVendor: FedEx
    - DeliveryTrackingNumber: *** none ***
    - ReturnDeliveryTrackingNumber: *** none ***
    - Status: PREPARING
    - Devices: [*** none ***]
    - UnattachedDevices: [*** none ***]
    - Appliances: [*** none ***]

When you use the `dts job show` command to display the details of a job, tagging details are also included in the output if you specified tags.

**Note:**

Users create tag namespaces and tag keys with the required permissions. These items must exist before you can specify them when creating a job. See Working with Defined Tags on page 3914 for details.
TransferSiteShippingAddress : Oracle Data Transfer Service;  
Job:JZM9PAVWH Package:PBNZOX9RU ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA  
DeliveryVendor : FedEx  
DeliveryTrackingNumber : *** none ***  
ReturnDeliveryTrackingNumber : *** none ***  
Status : PREPARING  
Devices : [*** none ***]  
UnattachedDevices : [*** none ***]  
Appliances : [*** none ***]  

When you use the to display the details of a job, tagging details are also included in the output if you specified tags.

Multiple Tags

To specify multiple tags, comma separate the JSON-formatted key/value pairs:

dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type disk --freeform-tags '{ "<tag_key>":"<value>" }', '{ "<tag_key>":"<value>" }'

Listing Transfer Jobs

To display the list of transfer jobs using the Console

Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.

To display the list of transfer jobs using the Data Transfer Utility

dts job list --compartment-id <compartment_id>

For example:

dts job list --compartment-id ocid.compartment.oc1..exampleuniqueID

Transfer Job List :  
[1] :  
ID : ocid1.datatransferjob.oc1..exampleuniqueID  
Name : MyDiskImportJob  
Label : JVWK5YWPU  
BucketName : MyBucket1  
CreationDate : 2020/06/01 17:33:16 EDT  
Status : INITIATED  
FreeformTags : *** none ***  
DefinedTags :  
Financials :  
key1 : nondefault

When you use the Data Transfer Utility to list jobs, tagging details are also included in the output if you specified tags.

Displaying Transfer Job Details

To display the details of a transfer job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job for which you want to display the details.
3. Click the Actions icon ( ), and then click View Details.
To display the details of a transfer job using the Data Transfer Utility

dts job show --job-id <job_id>

For example:

dts job show --job-id ocid1.datatransferjob.oc1..exampleuniqueID

Transfer Job :
| ID                | ocid1.datatransferjob.oc1..exampleuniqueID |
| CompartmentId     | ocid.compartment.oc1..exampleuniqueID      |
| UploadBucket      | MyBucket1                                  |
| Name              | MyDiskImportJob                            |
| Label             | JZM9PAVWH                                  |
| CreationDate      | 2019/06/04 17:07:05 EDT                    |
| Status            | PREPARING                                  |
| freeformTags      | *** none ***                               |
| definedTags       | *** none ***                               |
| Packages          | [1]                                           |
| Label             | PBNZOX9RU                                   |
| TransferSiteShippingAddress | Oracle Data Transfer Service; |
| Job:JZM9PAVWH Package:PBNZOX9RU | 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA |
| DeliveryVendor     | FedEx                                      |
| DeliveryTrackingNumber | *** none ***                               |
| ReturnDeliveryTrackingNumber | *** none ***                               |
| Status             | PREPARING                                  |
| Devices            | [*** none ***]                              |
| UnattachedDevices  | [*** none ***]                              |
| Appliances         | [*** none ***]                              |

When you use the Data Transfer Utility to display the details of a job, tagging details are also included in the output if you specified tags.

Editing Transfer Jobs
To edit the name of a transfer job using the Console

Note:
You can only change the name of a transfer job using the Console. If you want to change other attributes of the transfer job, use the Data Transfer Utility instead.

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the data transfer job that you want to edit.
3. Click the Actions icon (.), and then click Edit.
4. Edit the name of the transfer job. Avoid entering confidential information.
5. Click Save.

To edit the name of a transfer job using the Data Transfer Utility

dts job update --job-id <job_id> --display-name <display_name>

<display_name> is the new name of the transfer job. Avoid entering confidential information.

For example:
To edit the tags associated with a transfer job using the Data Transfer Utility

The Data Transfer Utility replaces any existing tags with the new key/value pairs you specify.

To edit defined tags, provide the replacement key value pairs:

dts job update --job-id <job_id> --defined-tags '{ "<tag_namespace>" : { "<tag_key>" : "<value>" }}'

For example:

dts job update --job-id ocid1.datatransferjob.oc1..exampleuniqueID --
defined-tags '{"Operations" : {"CostCenter" : "42"}}'

To edit free-form tags, provide the replacement key/value pairs:

dts job update --job-id <job_id> --freeform-tags '{ "<tag_key>" : "<value>", }'

For example:

dts job update --job-id ocid1.datatransferjob.oc1..exampleuniqueID --
freeform-tags '{"Chicago_Team" : "marketing_videos"}'}
To delete the tags associated with a transfer job using the Data Transfer Utility

The Data Transfer Utility replaces any existing tags with the new key/value pairs you specify. If you want to delete some of the tags, you would specify new tag string that does not contain the key/value pair you want to delete.

Partial tag deletion is handled in the same way as you edit tags:

- To edit free-form tags, provide the replacement key/value pairs:

  ```
  dts job update --job-id <job_id> --freeform-tags '{ "<tag_key>" : "<value>" }'
  ```

- To edit defined tags, provide the replacement key value pairs:

  ```
  dts job update --job-id <job_id> --defined-tags '{ "<tag_namespace>" : {
  "<tag_key>" : "<value>" }}'
  ```

To delete all free-form tags:

```
 dts job update --job-id <job_id> --freeform-tags '{}'
```  

To delete all defined tags:

```
 dts job update --job-id <job_id> --defined-tags '{}'
```  

Moving Transfer Jobs Between Compartments

**Note:**

You can only use the Console to move disk-based data transfer jobs between compartments.

To move a transfer job to a different compartment using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Select the Compartment from the list.

   The transfer jobs in that compartment are displayed.
3. Click the link under Transfer Jobs for the transfer job that you want to move.

   The Details page for that transfer job appears.
   
   Alternatively, you can click the Actions icon (⋮), and then click Move Resource.
4. Click Move Resource in the Details page.

   The Move Resource to a Different Compartment dialog appears.
5. Choose the compartment you want to which you want to move the transfer job from the list.
6. Click Move Resource.

You are returned to the Details page for that transfer job.
To move a transfer job to a different compartment using the Data Transfer Utility

```
dts job move --job-id <job_id> compartment-id <compartment_id> <options>
```

<compartment_id> is the compartment to which the data transfer job is being moved.

<options> are:

- `--if-match`: The tag that must be matched for the task to occur for that entity. If set, the update is only successful if the object's tag matches the tag specified in the request.
- `--from-json`: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The `--generate-full-command-json-input` option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. `compartment-id` -> `compartmentId`), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions.

To confirm the transfer, display the list of transfer jobs in the new compartment. See Listing Transfer Jobs on page 1002 for more information.

**Verifying Upload User Credentials**

```
Note:
You can only use the CLI command to verify upload user credentials.
```

You can verify the current upload user credentials to see if there are any problems or updates required. If any configuration file is incorrect or invalid, the upload fails.

**To verify the upload user credentials of a transfer job using the CLI**

```
dts job verify-upload-user-credentials --bucket <bucket>
```

<bucket> is the upload bucket for the transfer job.

For example:

```
dts job verify-upload-user-credentials --bucket MyBucket1
```

created object BulkDataTransferTestObject in bucket MyBucket1
overwrote object BulkDataTransferTestObject in bucket MyBucket1
inspected object BulkDataTransferTestObject in bucket MyBucket1
read object BulkDataTransferTestObject in bucket MyBucket1

Depending on your user configuration, you may get an error message returned similar to the following:

```
ERROR : key_file /root/.oci/oci_api_key.pem is not a valid file
```

If a user credential issue is identified, fix it and rerun the `verify-upload-user-credentials` CLI to ensure that all problems are addressed. Then you can proceed with transfer job activities.

**Deleting Transfer Jobs**

Typically, you would delete a transfer job early in the transfer process and before you create any transfer packages or their associated disks. For example, you initiated the data transfer by creating a transfer job, but changed your mind. If you want to delete a transfer job later in the transfer process, you must first delete all transfer packages and their associated disks from the transfer job.
To delete a transfer job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the data transfer job that you want to delete.
3. Click the Actions icon ( ), and then click Delete.
   Alternatively, you can delete a transfer job from the View Details page.
4. Confirm the deletion when prompted.

To delete a transfer job using the Data Transfer Utility

```
dts job delete --job-id <job_id>
```

For example:

```
dts job delete --job-id ocid1.datatransferjob.oc1..exampleuniqueID
```

Confirm the deletion when prompted. The transfer job is deleted with no further action or return. To confirm the deletion, display the list of transfer jobs in the compartment. See Listing Transfer Jobs on page 1002 for more information.

Closing Transfer Jobs

Typically, you would close a transfer job when no further transfer job activity is required or possible. Closing a transfer job requires that the status of all associated transfer packages be returned, canceled, or deleted. In addition, the status of all associated transfer disks must be complete, in error, missing, canceled, or deleted.

To close a transfer job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the data transfer package for which you want to display the details.
3. Click the Actions icon ( ), and then click View Details.
   Alternatively, click the hyperlinked name of the transfer job.
4. Click Close Transfer Job.

To close a transfer job using the Data Transfer Utility

```
dts job close --job-id <job_id>
```

For example:

```
dts job close --job-id ocid1.datatransferjob.oc1..exampleuniqueID
```

Transfer Job:

<table>
<thead>
<tr>
<th>ID</th>
<th>ocid1.datatransferjob.oc1..exampleuniqueID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompartmentId</td>
<td>ocid.compartment.oc1..exampleuniqueID</td>
</tr>
<tr>
<td>UploadBucket</td>
<td>MyBucket1</td>
</tr>
<tr>
<td>Name</td>
<td>MyDiskImportJob</td>
</tr>
<tr>
<td>Label</td>
<td>JZM9PAVWH</td>
</tr>
<tr>
<td>CreationDate</td>
<td>2019/06/04 17:07:05 EDT</td>
</tr>
<tr>
<td>Status</td>
<td>CLOSED</td>
</tr>
<tr>
<td>freeformTags</td>
<td>*** none ***</td>
</tr>
<tr>
<td>definedTags</td>
<td>*** none ***</td>
</tr>
<tr>
<td>Packages</td>
<td>[*** none ***]</td>
</tr>
<tr>
<td>UnattachedDevices</td>
<td>[*** none ***]</td>
</tr>
<tr>
<td>Appliances</td>
<td>[*** none ***]</td>
</tr>
</tbody>
</table>
Transfer Disks

The section describes the creation and management transfer disks.

**Important:**

Before creating a transfer disk from an attached disk, remove all partitions and any file systems. To prevent the accidental deletion of data, the Data Transfer Utility does not work with disks that already have partitions or file systems. Disks are visible to the Data Host as block devices and must provide a valid response to the `hdparm -I <device>` Linux command.

Creating Transfer Disks

**Note:**

You can only use the Data Transfer Utility to create a transfer disk.

When you create a transfer disk, the Data Transfer Utility:

- Sets up the disk for encryption using the passphrase
- Creates a file system on the disk
- Mounts the file system at `/mnt/orcdts_<label>`

For example:

```
/mnt/orcdts_DJZNWK3ET
```

When you register a transfer disk, Oracle Cloud Infrastructure generates a strong encryption passphrase that is used to encrypt the transfer disk. This passphrase is displayed in the return when you run the command. Create a local, secure copy of the encryption passphrase so you can reference the passphrase again. You cannot retrieve the passphrase after it is shown here. This passphrase is used to encrypt this disk and normally will not be needed again. However, if the system is restarted before all files are copied to the filesystem and the disk is then finalized through this CLI, you will need to provide the passphrase.

Creating a transfer disk requires the job ID returned from when you created the transfer job and the path to the attached disk (for example `/dev/sdb`).

**To create a transfer disk using the Data Transfer Utility**

```
dts disk create --job-id <job_id> --block-device <block_device>
```

When the run the disk create command, the CLI displays information regarding the creation of the disk, and prompts you to continue in several places. When the disk is created the following disk information is displayed:

```
dts disk create --job-id ocid1.datatransferjob.oci1..exampleuniqueID -- block-device /dev/sdb
...
Transfer Disk :
  Label:             : DNKZQ1XKC
  SerialNumber:      : VB6fc3b4a1-5d90f001
  Status             : PREPARING
  EncryptionPassphrase : passphrase
```

**Important:**

Record the passphrase in a secure, local location.
**Displaying Transfer Disk Details**

**Note:**
You can only use the Data Transfer Utility to display details for a specified transfer disk.

To display the details of a disk using the Data Transfer Utility

```bash
dts disk show --job-id <job_id> --disk-label <disk_label>
```

For example:

```bash
dts disk show --job-id ocid1.datatransferjob.oci1..exampleuniqueID --disk-label DNKZQ1XKC
```

Transfer Disk:
- **Label:** DNKZQ1XKC
- **SerialNumber:** VB6fc3b4a1-5d90f001
- **UploadStatusLogUrl:** JVPWPV6U/DNKZQ1XKC/upload_summary.txt
- **Status:** PREPARING

The path syntax for the upload status log URL is `<transfer_job_label>/<disk_label>/upload_summary.txt`.

**Deleting Transfer Disks**

**Note:**
You can only use the Data Transfer Utility to delete a transfer disk.

Typically, you would delete a transfer disk during the disk preparation process. You created, attached, and copied data to the transfer disk, but have changed your mind about shipping the disk. If you want to reuse the disk, remove all file systems and create the disk again.

To delete a transfer disk using the Data Transfer Utility

```bash
dts disk delete --job-id <job_id> --disk-label <disk_label>
```

For example:

```bash
dts disk delete --job-id ocid1.datatransferjob.oci1..exampleuniqueID --disk-label DNKZQ1XKC
```

Deleted Disk: DNKZQ1XKC

**Canceling Transfer Disks**

**Note:**
You can only use the Data Transfer Utility to cancel a transfer disk.

If you shipped a disk to Oracle, but have changed your mind about uploading the files, you can cancel the transfer disk.

Oracle cannot process canceled transfer disks. Oracle returns canceled transfer disks to the sender.

To cancel a transfer disk using the Data Transfer Utility

```bash
dts disk cancel --job-id <job_id> --disk-label <disk_label>
```
For example:

dts disk cancel --job-id ocid1.datatransferjob.oci1..exampleuniqueID --disk-label DNKZQ1XKC

Canceled Disk: DNKZQ1XKC

Locking Transfer Disks

**Note:**

You can only use the Data Transfer Utility to lock a transfer disk.

Locking a transfer disk safely unmounts the disk and removes the encryption passphrase from the Data Host.

**To lock a transfer disk using the Data Transfer Utility**

dts disk lock --job-id <job_id> --disk-label <disk_label> --block-device <block_device>

For example:

dts disk lock --job-id ocid1.datatransferjob.oci1..exampleuniqueID --disk-label DNKZQ1XKC --block-device /dev/sdb

Copying upload user credentials.
created object BulkDataTransferTestObject in bucket MyBucket1
overwrote object BulkDataTransferTestObject in MyBucket1
inspected object BulkDataTransferTestObject in bucket MyBucket1
read object BulkDataTransferTestObject in bucket MyBucket1
Scanning filesystem to validate manifest. If special files are encountered, they will be listed below.
validated manifest
/dev/sdb DNKZQ1XKC is encrypted and locked
Locked disk.

Unlocking Transfer Disks

If you need to unlock the transfer disk, you are prompted for the encryption passphrase that was generated when you created the transfer disk.

**To unlock a transfer disk using the Data Transfer Utility**

dts disk unlock --job-id <job_id> --disk-label <disk_label> --block-device <block_device> --encryption-passphrase <encryption_passphrase>

For example:

dts disk unlock --job-id ocid1.datatransferjob.oci1..exampleuniqueID --disk-label DNKZQ1XKC --block-device /dev/sdb --encryption-passphrase passphrase

Encryption passphrase ('q' to quit):
enabled cleartext read/write on device
Unlocked and mounted disk.

Attaching Transfer Disks to Transfer Packages

Attach a transfer disk to a transfer package after you have done the following tasks in order:

- Copied your data onto the disk
- Generated the required manifest file
• Run and reviewed the dry-run report
• Locked the transfer disk in preparation for shipment

**Note:**
You can only attach a single disk to each transfer package.

**To attach a transfer disk to a transfer package using the Console**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer job associated with the transfer package having the disk attached.
3. Click the **Actions** icon (🔍), and then click **View Details**.
   A list of transfer packages is displayed.
4. Find the transfer package that you want to attach a disk to.
5. Click the **Actions** icon (🔍), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer package.
   The transfer disk is displayed.
6. Click **Attach Transfer Disks**.
   The Attach Transfer Disks dialog appears.
7. Select the **Transfer Disks** that you want to attach to the transfer package.
8. Click **Attach**.

**To attach a transfer disk to a transfer package using the Data Transfer Utility**

```bash
dts disk attach --job-id <job_id> --package-label <package_label> --disk-label <disk_label>
```

For example:

```bash
dts attach --job-id ocid1.datatransferjob.oc1..exampleuniqueID --package-label PWA8O67MI --disk-label DNKZQ1XKC
```

Attached disk: DNKZQ1XKC to package: PWA8O67MI

See **Transfer Packages** on page 1012 for more information, including how to obtain the package label.

**Detaching Transfer Disks from Transfer Packages**

**To detach a transfer disk to a transfer package using the Console**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer package for which you want to detach a transfer disk.
3. Click the **Actions** icon (🔍), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer package.
   The attached transfer disk is displayed.
4. Click the **Actions** icon (🔍), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer disk.
5. Click **Detach Transfer Disk**.
To detach a transfer disk to a transfer package using the Data Transfer Utility

```
dts disk detach --job-id <job_id> --package-label <package_label> --disk-label <disk_label>
```

For example:

```
dts detach --job-id ocid1.datatransferjob.oc1..exampleuniqueID --package-label PWA8O67MI --disk-label DNKZQ1XKC
```

Detached disk: DNKZQ1XKC from package: PWA8O67MI

**Querying Transfer Disks**

You can query the transfer disk for information regarding the physical transfer disk such as the loops, sizes, and mountpoints.

**Note:**

You can only use the Data Transfer Utility to query the transfer disk.

To query the transfer disk using the Data Transfer Utility

```
dts disk query
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>SIZE</th>
<th>UUID</th>
<th>LABEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>loop0</td>
<td>loop</td>
<td>140.7M</td>
<td></td>
<td>/</td>
</tr>
<tr>
<td>snap/gnome-3-26-1604/92</td>
<td>loop</td>
<td>4.2M</td>
<td></td>
<td>/</td>
</tr>
<tr>
<td>loop1</td>
<td>loop</td>
<td>4.2M</td>
<td></td>
<td>/</td>
</tr>
<tr>
<td>snap/gnome-calculator/501</td>
<td>disk</td>
<td>40.8G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sda1</td>
<td>part</td>
<td>12G</td>
<td>xxxxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxxxxx</td>
<td>/</td>
</tr>
<tr>
<td>sr0</td>
<td>rom</td>
<td>56.9M</td>
<td>2020-02-18-17-20-05-35</td>
<td>VBox_GAs_6.1.4 /</td>
</tr>
<tr>
<td>media/user/VBox_GAs_6.1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Transfer Packages**

A transfer package is the virtual representation of the physical disk package that you are shipping to Oracle for upload to Oracle Cloud Infrastructure.

**Creating Transfer Packages**

Creating a transfer package requires the job ID returned from when you created the transfer job. For example:

```
ocid1.datatransferjob.region1.phx..exampleuniqueID
```

To create a transfer package using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer job for which you want to create a transfer package.
3. Click the **Actions** icon (★), and then click **View Details**.
   Alternatively, click the hyperlinked name of the transfer job.
   A list of transfer packages that have already been created is displayed.
4. Click **Create Transfer Package**.
   The Create Transfer Package dialog appears.
5. Select a **Vendor** from the list.
6. Click **Create Transfer Package**.
The Data Transfer Package dialog appears displaying information such as the shipping address, the shipping vendor, and the shipping status.

To create a transfer package using the Data Transfer Utility

```
dts package create --job-id <job_id>
```

For example:
```
dts package create --job-id ocid1.datatransferjob.oci1..exampleuniqueID
```

Transfer Package :
Label : PWA8067MI
TransferSiteShippingAddress : Oracle Data Transfer Service; Job:JZM9PAVWH Package:PWA8067MI ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
DeliveryVendor : *** none ***
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]

Displaying Transfer Package Details

To display the details of a transfer package using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job for which you want to see the details.
3. Click the Actions icon ( ), and then click View Details.
   Alternatively, click the hyperlinked name of the transfer job.
   A list of transfer packages that have already been created is displayed.

To display the details of a transfer package using the Data Transfer Utility

```
dts package show --job-id <job_id> --package-label <package_label>
```

For example:
```
dts package show --job-id ocid1.datatransferjob.oci1..exampleuniqueID --package-label PWA8067MI
```

Transfer Package :
Label : PWA8067MI
TransferSiteShippingAddress : Oracle Data Transfer Service; Job:JZM9PAVWH Package:PWA8067MI ; 21111 Ridgetop Circle; Dock B; Sterling, VA 20166; USA
DeliveryVendor : *** none ***
DeliveryTrackingNumber : *** none ***
ReturnDeliveryTrackingNumber : *** none ***
Status : PREPARING
Devices : [*** none ***]

Editing Transfer Packages

Edit the transfer package and supply the tracking information when you ship the package.

To edit a transfer package using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job for which you want to see the associated transfer packages.
3. Click the **Actions** icon (⋮), and then click **View Details**.
4. Find the transfer package that you want to edit.
5. Click the **Actions** icon (⋮), and then click **View Details**.
6. Click **Edit**.

   Change the vendor and supply the tracking information as needed.
7. Click **Edit Transfer Package**.

**Deleting Transfer Packages**

Typically, you would delete a transfer package early in the transfer process and before you create its associated transfer disk. You initiated the transfer job and package, but have changed your mind. If you delete a transfer package later in the transfer process, you must first detach the associated transfer disk. You cannot delete a transfer package once the package has been shipped to Oracle.

To delete a transfer package using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer job for which you want to see the associated transfer packages.
3. Click the **Actions** icon (⋮), and then click **View Details**.
4. Find the transfer package that you want to edit.
5. Click the **Actions** icon (⋮), and then click **View Details**.
6. Click **Edit**.

   Change the vendor and supply the tracking information as needed.
7. Click **Edit Transfer Package**.

**To delete a transfer package using the Data Transfer Utility**

    dts package delete --job-id <job_id> --package-label <package_label>

For example:

    dts package delete --job-id ocid1.datatransferjob.oc1..exampleuniqueID --package-label PWA8067MI

    Deleted package with label: PWA8067MI

**Canceling Transfer Packages**

If you shipped a transfer package, but have changed your mind about uploading the data, you can cancel a transfer package. Before canceling a transfer package, you must first cancel the transfer disk associated with that transfer package. Oracle cannot process canceled transfer packages. Oracle returns canceled transfer packages to the sender.

To cancel a transfer package using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Find the transfer job for which you want to see associated transfer packages.
3. Click the **Actions** icon (⋮), and then click **View Details**.
4. Find the transfer package that you want to cancel.
5. Click the **Actions** icon (⋮), and then click **View Details**.
6. Click **Cancel Transfer Package**.
To cancel a transfer package using the Data Transfer Utility

dts package cancel --job-id <job_id> --package-label <package_label>

For example:

dts package cancel --job-id ocid1.datatransferjob.oci1..exampleuniqueID --package-label PWA8067MI

Canceled package with label: PWA8067MI

Data Import - Appliance

Appliance-Based Data Import is one of Oracle's offline data transfer solutions that lets you migrate petabyte-scale datasets to Oracle Cloud Infrastructure. You send your data as files on one or more secure, high-capacity, Oracle-supplied Data Transfer Appliances to an Oracle transfer site. Operators at the Oracle transfer site upload the files into the designated Object Storage bucket in your tenancy. You are then free to move the uploaded data to other Oracle Cloud Infrastructure services as needed.

Note:
Appliance-Based Data Import is not available for free trial or Pay As You Go accounts.

Appliance-Based Data Import Concepts

TRANSFER JOB

A transfer job is the logical representation of a data migration to Oracle Cloud Infrastructure. A transfer job is associated with one or more import appliances.

DATA TRANSFER APPLIANCE

The Data Transfer Appliance (import appliance) is a high-storage capacity device that is specially prepared to copy and upload data to Oracle Cloud Infrastructure. You request an import appliance from Oracle, copy your data onto it, and then ship it back to Oracle for upload.

COMMAND LINE INTERFACE

The command line interface (CLI) is a small footprint tool that you can use on its own or with the Console to complete Oracle Cloud Infrastructure tasks, including Appliance-Based Data Import jobs.

Note:
You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

HOST

A physical computer at the customer site on which one or more of the logical hosts (Control, Data, Terminal Emulation) is running. Depending on your computing environment, you can have any of the following:

- A separate physical host for each logical host
- All three logical hosts consolidated onto a single physical host
- Two logical hosts on one physical host and the third logical host on a separate physical host

All physical hosts must be on network used for the data transfer.
**CONTROL HOST**

The logical representation of the host computer at your site from which you perform Data Transfer Service tasks. Depending on your needs, you may use one or more separate hosts (Control and Data) to run your Appliance-Based Data Import job.

**Note:**
You can only run Oracle Cloud Infrastructure CLI commands from a Linux-based Control Host machine. You can run Console tasks from a browser running on a Windows machine.

**DATA HOST**

The logical representation of the host computer on your site that stores the data you intend to copy to Oracle Cloud Infrastructure.

**Note:**
Only Linux machines can be used as Data Hosts.

**TERMINAL EMULATION HOST**

The logical representation of the host computer that uses terminal emulation software to communicate with, and allow you to command, the import appliance.

**BUCKET**

The logical container in Oracle Cloud Infrastructure Object Storage where Oracle operators upload your data. A bucket is associated with a single compartment in your tenancy whose policies that determine what actions a user can perform on a bucket and on all the objects in the bucket.

**DATA TRANSFER ADMINISTRATOR**

A new or existing IAM user that has the authorization and permissions to create and manage transfer jobs.

**DATA TRANSFER UPLOAD USER**

A temporary IAM user that grants Oracle personnel the authorization and permissions to upload the data from the import appliance to your designated Oracle Cloud Infrastructure Object Storage bucket. Delete this temporary user after your data is uploaded to Oracle Cloud Infrastructure.

**APPLIANCE MANAGEMENT SERVICE**

Software running on the import appliance that provides management functions. Users interact with this service though the Oracle Cloud Infrastructure CLI.

**Appliance Specifications**

Use NFS versions 3, 4, or 4.1 to copy your data onto the appliance. Here are some details about the appliance:

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Capacity</td>
<td>150 TB of protected usable space</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>- 10 GbE - RJ45</td>
</tr>
<tr>
<td></td>
<td>- 10 GbE - SFP+</td>
</tr>
<tr>
<td></td>
<td>You are responsible for providing all network cables. If you want to use SFP+, your transceivers must be compatible with Intel X520 NICs.</td>
</tr>
<tr>
<td>Item Description</td>
<td>Specification</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Provided Cables**     | - NEMA 5–15 type B to C13  
- C13 - 14 power  
- USB - DB9 serial |
| **Environmental**       | - Operational temperature: 50–95°F (10–35°C)  
- Operational relative humidity: 8–90% non-condensing  
- Acoustics: < 75 dB @ 73°F (23°C)  
- Operational altitude: -1,000 ft - 10,000 ft (approx. -300–3048 m) |
| **Power**               | - Consumption: 554 W  
- Voltage: 100–240 VAC  
- Frequency: 47–63 Hz  
- Conversion efficiency: 89% |
| **Weight**              | - Unit: 38 lbs (approx. 17 kg)  
- Unit + Transit Case: 64 lbs (approx. 29 kg) |
| **Height**              | 3.5" (approx. 9 cm) (2U) |
| **Width**               | 17" (approx. 43 cm) |
| **Depth**               | 24" (approx. 61 cm) |
| **Shipping Case**       | 11" x 25" x 28" (approx. 28 x 63.5 x 71 cm) |

**Import File Constraints**

All files being imported using the Data Transfer Appliance must conform to the following:

- Maximum file size - 10 TB
- Maximum file name length - 1024 characters

**Roles and Responsibilities**

Depending on your organization, the responsibilities of using and managing the data transfer may span multiple roles. Use the following set of roles as a guideline for how you can assign the various tasks associated with the data transfer.

- **Project Sponsor**: Responsible for the overall success of the data transfer. Project Sponsors usually have complete access to their organization's Oracle Cloud Infrastructure tenancy. They coordinate with the other roles in the organization to complete the implementation of data transfer project. The Project Sponsor is also responsible for signing legal documentation and setting up notifications for the data import.

- **Infrastructure Engineer**: Responsible for integrating the transfer appliance into the organization's IT infrastructure from where the data is being transferred. Tasks associated with this role include connecting the transfer appliance to power, placing it within the network, and setting the IP address through a serial console menu using the provided USB-to-Serial adapter.

- **Data Administrator**: Responsible for identifying and preparing the data to be transferred to Oracle Cloud Infrastructure. This person usually has access to, and expertise with, the data being migrated.

These roles correspond to the various phases of the data transfer described in the following section. A specific role can be responsible for one or more phases.
Task Flow for Appliance-Based Data Import

Here is a high-level overview of the tasks involved in the Appliance-Based Data Import to Oracle Cloud Infrastructure. Complete one phase before proceeding to the next one. Use the roles previously described to distribute the tasks across individuals or groups within your organization.
Secure Appliance Data Transfer to Oracle Cloud Infrastructure

This section highlights the security details of the Data Transfer Appliance process.

- Appliances are shipped from Oracle to you with a tamper-evident security tie on the transit case. A second tamper-evident security tie is included in the import appliance transit case for you to secure the case when you ship the case back to Oracle. The number on the physical security ties must match the numbers logged by Oracle in the import appliance details.
- When you configure the import appliance for the first time:
  - The import appliance generates a master AES-256 bit encryption key that is used for all data written to or read from the device. The encryption key never leaves the device.
  - The encryption key is protected by an encryption passphrase that you must know to access the encrypted data. The system securely fetches a provided encryption passphrase from Oracle Cloud Infrastructure and registers that passphrase on the import appliance.

  **Note:**
  The encryption passphrase is never stored on the import appliance

- All data is encrypted as the data is copied to an import appliance.
- For more security, you can also encrypt your own data with your own encryption keys. Before copying your data to the import appliance, you can encrypt your data with a tool and encryption key of your choosing. After the data has been uploaded, you would need to use the same tool and encryption key to access the data.
- All network communication between your appliance-based data transfer environment and Oracle Cloud Infrastructure is encrypted in-transit using Transport Layer Security (TLS).
- After copying your data to a transfer appliance, the data transfer system generates a manifest file. The manifest contains an index of all of the copied files and generated data integrity hashes. The system also encrypts and copies the `config_upload_user` configuration file to the transfer appliance. This configuration file describes the temporary IAM data transfer upload user. Oracle uses the credentials and entries defined in the `config_upload_user` file when processing the transfer appliance and uploading files to Oracle Cloud Infrastructure Object Storage.

  **Note:**
  Data Transfer Service Does Not Support Passphrases on Private Keys
  While we recommend encrypting a private key with a passphrase when generating API signing keys, the Data Transfer Service does not support passphrases on the key file required for the `config_upload_user` configuration file. If you use a passphrase, Oracle personnel cannot upload your data.

Oracle cannot upload data from a transfer appliance without the correct credentials defined in this configuration file. See Preparing Upload Configuration Files on page 1031 for more information about the required configuration files.

- Oracle erases all of your data from the import appliance after it has been processed. The erasure process follows the NIST 800-88 standards.
- Keep possession of the security tie after you have finished unpacking and connecting the import appliance. Include it when returning the import appliance to Oracle. Failure to include the security tie can result in a delay in the data migration process.

**What's Next**

You are now ready to prepare the host for the Appliance-Based Data Import. See Preparing for Appliance Data Transfers on page 1021 for more information.
Preparing for Appliance Data Transfers

This topic describes the tasks associated with preparing for the Appliance-Based Data Import job. The Project Sponsor role typically performs these tasks. See Roles and Responsibilities on page 1017.

Note:
You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

Installing and Using the Oracle Cloud Infrastructure Command Line Interface

The Oracle Cloud Infrastructure Command Line Interface (CLI) provides a set of command line-based tools for configuring and running Appliance-Based Data Import jobs. Use the Oracle Cloud Infrastructure CLI as an alternative to running commands from the Console. Sometimes you must use the CLI to complete certain tasks as there is no Console equivalent.

Minimum Required CLI Version

The minimum CLI version required for Appliance-Based Data Import is 2.12.1.

Determining CLI Versions

Access the following URL to see the currently available version of the CLI:

https://github.com/oracle/oci-cli/blob/master/CHANGELOG.rst

Enter the following command at the prompt to see the version of the CLI currently installed on your machine:

oci --version

If you have a version on your machine older than the version currently available, install the latest version.

Note:
Always update to the latest version of the CLI. The CLI is not updated automatically, and you can only access new or updated CLI features by installing the current version.

Linux Operating System Requirements

See Requirements on page 4193 for a list of the Linux operating systems that support the CLI.

Installing the CLI

Installation and configuration of the CLIs is described in detail in Command Line Interface (CLI) on page 4192.

Using the CLI

You can specify CLI options using the following commands:

• --option <value> or
• --option=<value>
The basic CLI syntax is:

```
oci dts <resource> <action> <options>
```

This syntax is applied to the following:

- `oci dts` is the shortened CLI command name
- `job` is an example of a `<resource>`
- `create` is an example of an `<action>`
- Other strings are `<options>`

The following command to create a transfer job shows a typical CLI command construct.

```
oci dts job create --compartment-id ocid1.compartment.oc1..exampleuniqueID --bucket MyBucket --display-name MyApplianceImportJob --device-type appliance
```

**Note:**
In the previous examples, provide a friendly name for the transfer job using the `##display#name` option. Avoid entering confidential information.

### Accessing Command Line Interface Help

All CLI help commands have an associated help component you can access from the command line. To view the help, enter any command followed by the `--help` or `-h` option. For example:

```
oci dts job --help
```

**NAME**

dts_job -

**DESCRIPTION**

Transfer disk or appliance job operations

**AVAILABLE COMMANDS**

- change-compartment
- close
- create
- delete
- detach-devices-details
  ...

When you run the help option (`--help` or `-h`) for a specified command, all the subordinate commands and options for that level of CLI are displayed. If you want to access the CLI help for a specific subordinate command, include it in the CLI string. For example:

```
oci dts job create --help
```

**NAME**

dts_job_create -

**DESCRIPTION**

Creates a new transfer disk or appliance job.

**USAGE**

oci dts job create [OPTIONS]

**REQUIRED PARAMETERS**
Creating the Required IAM Users, Groups, and Policies

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization.

To use Oracle Cloud Infrastructure, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in.

Access to resources is provided to groups using policies and then inherited by the users that are assigned to those groups. Data transfer requires the creation of two distinct groups:

- **Data transfer administrators** who can create and manage transfer jobs.
- **Data transfer upload users** who can upload data to Object Storage. For your data security, the permissions for upload users allow Oracle personnel to upload standard and multi-part objects on your behalf and inspect bucket and object metadata. The permissions do not allow Oracle personnel to inspect the actual data.

The Data Administrator is responsible for generating the required RSA keys needed for the temporary upload users. These keys should never be shared between users.

For details on creating groups, see Managing Groups on page 2419.

An administrator creates these groups with the following policies:

- **The data transfer administrator group** requires an authorization policy that includes the following:

  ```
  Allow group <group_name> to manage data-transfer-jobs in
  compartment <compartment_name>
  Allow group <group_name> to manage objects in
  compartment <compartment_name>
  Allow group <group_name> to manage buckets in
  compartment <compartment_name>
  ```

  Alternatively, you can consolidate the manage buckets and manage objects policies into the following:

  ```
  Allow group <group_name> to manage object-family in
  compartment <compartment_name>
  ```

- **The data transfer upload user group** requires an authorization policy that includes the following:

  ```
  Allow group <group_name> to manage buckets
  in compartment <compartment_name> where all
  { request.permission='BUCKET_READ', target.bucket.name='<bucket_name>' }
  Allow group <group_name> to manage objects
  in compartment <compartment_name> where all
  { target.bucket.name='<bucket_name>', any
  { request.permission='OBJECT_CREATE',
  request.permission='OBJECT_OVERWRITE',
  request.permission='OBJECT_INSPECT' })
  ```

  To enable notifications, add the following policies:

  ```
  Allow group <group name> to manage ons-topics in tenancy
  ```
Allow group <group name> to manage ons-subscriptions in tenancy
Allow group <group name> to manage cloudevents-rules in tenancy
Allow group <group name> to inspect compartments in tenancy

See Notifications Overview on page 3350 and Overview of Events on page 1784 for more information.

The Oracle Cloud Infrastructure administrator then adds a user to each of the data transfer groups created. For details on creating users, see Managing Users on page 2414.

**Important:**
For security reasons, we recommend that you create a unique IAM data transfer upload user for each transfer job and then delete that user once your data is uploaded to Oracle Cloud Infrastructure.

**Requesting Appliance Entitlement**

If your tenancy is not entitled to use the Data Transfer Appliance, you must request the Data Transfer Appliance Entitlement before creating an appliance-based transfer job.

**Important:**
The main buyer or administrator, who is at a VP level or higher, receives an email notification and is required to e-sign a Terms and Conditions document. After Oracle has confirmed signature of the document, you can create an appliance-based transfer job. The email for the DocuSign does not go to the requester unless they are the main buyer or administrator who is at least at a VP level.

It can take up to 24 hours before the Terms and Conditions are sent.

To request the Data Transfer Appliance Entitlement using the Console

Open the Transfer Job page and click Request at the top. Otherwise, you are prompted to request the entitlement when attempting to create your first appliance-based transfer job.

Once requested, the status of your request is visible at the top of the Transfer Job page. For example:

**Data Transfer Appliance Entitlement:** Granted

It can take a while to get the Data Transfer Appliance Entitlement approved. After Oracle receives your request, a Terms and Conditions Agreement is sent to the account owner via DocuSign to use the appliance. The entitlement request is approved once the signature is received. The Data Transfer Appliance Entitlement is a tenancy-wide entitlement that you need to request once for each tenancy.

To request the Data Transfer Appliance Entitlement using the CLI

```
oci dts appliance request-entitlement --compartment-id <compartment_id> --name <name> --email <email>
```

<name> is the name of the requester.
<email> is the email address of the requester.

For example:

```
oci dts appliance request-entitlement --compartment-id ocid.compartment.oc1..exampleuniqueID --name "John Doe" --email jdoe@mycompany.com
```

```json
{
    "data": {
        "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
        "creation-time": "2019-12-18T18:29:15+00:00",
        "defined-tags": {}
    }
}```
To show the status of a Data Transfer Appliance Entitlement request using the CLI

```
oci dts appliance show-entitlement --compartment-id <compartment_id>
```

For example:

```
oci dts appliance show-entitlement --compartment-id ocid.compartment.oc1..exampleuniqueID
```

Establishing the Data Transfer Appliance Entitlement Policy

Use the following policy to enable users in a specific group to request a Data Transfer Appliance Entitlement in your tenancy.

```
Allow group <group_name> to {DTA_ENTITLEMENT_CREATE} in tenancy
```

Appliance Entitlement Eligibility

Your request for a Data Transfer Appliance Entitlement in your tenancy may be denied if you are a free trial customer. If your request is denied, upgrade to a full account. You can also contact your Oracle Customer Support Manager or Oracle Support to determine your options for obtaining the entitlement.

Creating Object Storage Buckets

The Object Storage service is used to upload your data to Oracle Cloud Infrastructure. Object Storage stores objects in a container called a bucket within a compartment in your tenancy. For details on creating the bucket to store uploaded data, see Managing Buckets on page 3398.

Configuring Firewall Settings

Ensure that your local environment's firewall can communicate with the Data Transfer Service running on the IP address ranges: 140.91.0.0/16. You also need to open access to the Object Storage IP address ranges: 134.70.0.0/17.

Creating Transfer Jobs

This section describes how to create a transfer job as part of the preparation for the data transfer. See Transfer Jobs on page 1060 for complete details on all tasks related to transfer jobs.

A transfer job represents the collection of files that you want to transfer and signals the intention to upload those files to Oracle Cloud Infrastructure. Identify which compartment and Object Storage bucket to which Oracle is to upload
your data. Create the transfer job in the same compartment as the upload bucket and supply a human-readable name for the transfer job.

**Note:**
It is recommended that you create a compartment for each transfer job to minimize the required access your tenancy.

Creating a transfer job returns a transfer job ID that you specify in other transfer tasks. For example:

```
oci1.datatransferjob.region1.phx..<unique_ID>
```

To create a transfer job using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the designated compartment you are to use for data transfers from the list.
   - A list of transfer jobs that have already been created is displayed.
3. Click **Create Transfer Job**.
   - The Create Transfer Job dialog appears.
4. Enter a **Job Name**. Avoid entering confidential information. Then, select the **Upload Bucket** from the list.
5. Select **Appliance** for the **Transfer Device Type**.
6. Click **Create Transfer Job**.

To create a transfer job using the CLI

```
oci dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type <device_type>
```

- `<display_name>` is the name of the transfer job. Avoid entering confidential information.
- `<device_type>` should always be appliance for Appliance-Based Data Import jobs.

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyApplianceImportJob --device-type appliance
```

```json
{
    "data": {
        "attached-transfer-appliance-labels": [],
        "attached-transfer-device-labels": [],
        "attached-transfer-package-labels": [],
        "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
        "creation-time": "2019-12-18T19:43:58+00:00",
        "defined-tags": {},
        "device-type": "APPLIANCE",
        "display-name": "MyApplianceImportJob",
        "freeform-tags": {},
        "id": "oci1.datatransferjob.oc1..exampleuniqueID",
        "label": "JAKQVAGJF",
        "lifecycle-state": "INITIATED",
        "upload-bucket-name": "MyBucket1"
    },
    "etag": "2--gzip"
}
```

 Optionally, you can specify one or more defined or freeform tags when you create a transfer job. For more information about tagging, see [Resource Tags](#) on page 211.
Defined Tags

To specify defined tags when creating a job:

```
oci dts job create --bucket <bucket> --compartment-id <compartment_id>
   --display-name <display_name> --device-type appliance --defined-tags
   '{ "<tag_namespace>": { "<tag_key>":"<value>" }}'
```

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID
   --display-name MyApplianceImportJob --device-type appliance --defined-tags
   '{"Operations": {"CostCenter": "01"}}'
```

```
{
   "data": {
      "attached-transfer-appliance-labels": [],
      "attached-transfer-device-labels": [],
      "attached-transfer-package-labels": [],
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "creation-time": "2019-12-18T19:43:58+00:00",
      "defined-tags": {
         "operations": {
            "costcenter": "01"
         }
      },
      "device-type": "APPLIANCE",
      "display-name": "MyApplianceImportJob",
      "freeform-tags": {
         "Operations": {"CostCenter": "01"}
      },
      "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
      "label": "JAKQVAGJF",
      "lifecycle-state": "INITIATED",
      "upload-bucket-name": "MyBucket1"
   },
   "etag": "2--gzip"
}
```

Freeform Tags

To specify freeform tags when creating a job:

```
oci dts job create --bucket <bucket> --compartment-id <compartment_id>
   --display-name <display_name> --device-type appliance --freeform-tags
   '{ "<tag_key>":"<value>" }'
```

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID
   --display-name MyApplianceImportJob --device-type appliance --freeform-tags
   '{"Pittsburg_Team":"brochures"}'
```

```
{
   "data": {
      "attached-transfer-appliance-labels": [],
      "attached-transfer-device-labels": [],
      "attached-transfer-package-labels": [],
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "creation-time": "2019-12-18T19:43:58+00:00",
      "defined-tags": {
         "Pittsburg_Team": "brochures",
      },
      "device-type": "APPLIANCE",
      "display-name": "MyApplianceImportJob",
      "freeform-tags": {
```
"Pittsburg_Team": "brochures"},
  "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
  "label": "JAKQVAGJF",
  "lifecycle-state": "INITIATED",
  "upload-bucket-name": "MyBucket1"
},
  "etag": "2--gzip"
}

**Note:**
Users create tag namespaces and tag keys with the required permissions. These items must exist before you can specify them when creating a job. See [Working with Defined Tags](#) for details.

### Multiple Tags
To specify multiple tags, comma separate the JSON-formatted key/value pairs:

```bash
oci dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type appliance --freeform-tags '{ "<tag_key>": "<value>" }', '{ "<tag_key>": "<value>" }'
```

### Notifications
To include notifications, include the `--setup-notifications` option. See [Setting Up Transfer Job Notifications from the CLI](#) for more information on this feature.

### Getting Transfer Job IDs
Each transfer job you create has a unique ID within Oracle Cloud Infrastructure. For example:

```
ocid1.datatransferjob.oc1.phx.exampleuniqueID
```

You will need to forward this transfer job ID to the Data Administrator.

*To get the transfer job ID using the Console*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list.
   The transfer jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the transfer job whose details you want to view.
   Alternatively, you can click the **Actions** icon (●), and then click **View Details**.
   The Details page for that transfer job appears.
4. Find the **OCID** field in the Details page and click **Show** to display it or **Copy** to copy it to your computer.

*To get the transfer job ID using the CLI*

```
oci dts job list --compartment-id <compartment_id>
```

For example:

```
oci dts job list --compartment-id ocid.compartment.oc1..exampleuniqueID

{
  "data": [
    {
      "creation-time": "2019-12-18T19:43:58+00:00",
```
The ID for each transfer job is included in the return:

```
"id": "ocid.compartment.oc1..exampleuniqueID"
```

**Tip:**
When you create a transfer job using the `oci dts job create` CLI, the transfer job ID is displayed in the CLI's return. You can also run the `oci dts job show` CLI for that specific job to get the ID.

### Setting Up Transfer Job Notifications from the CLI

You can generate notifications that send messages regarding changes to a new or existing appliance-based transfer job through the CLI. Using this feature creates a topic, subscription for a list of email addresses, and a rule that notifies you on all events related to the export job's activities and changes in state. This method provides a more convenient way to generate notifications tailored to appliance-based transfer jobs.

The CLI command to set up transfer job notifications is different depending on whether you are creating a new transfer job or updating an existing transfer job. In both cases, running the CLI command prompts you to enter the email addresses of each notification subscriber as a comma separated list. Each recipient is sent an email with a link to confirm they want to receive the notifications.

You are prompted to enter those email addresses you want included in the notifications, separated by commas (","). When your list is complete, add a colon (":") followed by your own email address:

```
user1@mycompany.com,user2@mycompany.com : myemail@mycompany.com
```

For both of the notification commands, the following is returned:

```
If the commands fail to run, you can use the OCI CLI to do the setup manually:
export ROOT_COMPARTMENT_OCID=ocidv1:tenancy:oc1:exampleuniqueID
oci ons topic create --compartment-id $ROOT_COMPARTMENT_OCID --name
DTSExportTopic --description "Topic for data transfer service export jobs"
oci ons subscription create --protocol EMAIL --compartment-id
$ROOT_COMPARTMENT_OCID --topic-id $TOPIC_OCID --endpoint $EMAIL_ID
oci events rule create --display-name DTSExportRule --is-enabled
true --compartment-id $ROOT_COMPARTMENT_OCID --actions '{"actions":
[{{"actionType":"ONS","topicId":"$TOPIC_OCID","isEnabled":true}}]}' --condition
'{{"eventType":"com.oraclecloud.datatransferservice.addapplianceexportjob","com.oraclecloud.datatransferservice.updateapplianceexportjob","com.oraclecloud.datatransferservice.moveapplianceexportjob"}}'
```

Oracle Cloud Infrastructure User Guide 1029
To set up notifications when creating a transfer job using the CLI

To set up notifications when creating a transfer job, include the --setup-notifications option in the CLI:

```
oci dts job create --bucket <bucket_name> --compartment-id <compartment_id>
    --display-name <display_name> --device-type appliance ... --setup-notifications
```

To set up notifications for an existing transfer job using the CLI

To set up notifications for an existing transfer job:

```
oci dts job setup-notifications --job-id <job_id>
```

For example:

```
oci dts job setup-notifications --job-id
    ocid1.datatransferjob.oc1..exampleuniqueID

If the commands fail to run, you can use the OCI CLI to do the setup manually:
oci ons topic create --compartment-id ocid1.tenancy.oc1..exampleuniqueID
    --name MyImportJob --description "Topic for data transfer service import job
    with OCID ocid1.datatransferjob.oc1..exampleuniqueID"
oci ons subscription create --protocol EMAIL --compartment-id
    $ROOT_COMPARTMENT_OCID --topic-id $TOPIC_OCID --subscription_endpoint
    $EMAIL_ID
oci events rule create --display-name MyImportJob --is-enabled true--
    compartment-id ocid1.tenancy.oc1..exampleuniqueID --actions '{"actions":
    [{"actionType":"ONS","topicId":"$TOPIC_OCID","isEnabled":true}]}
    --condition
    '{"eventType":"com.oraclecloud.datatransferservice.*transferjob","data":
    {"resourceId":"ocid1.datatransferjob.oc1..exampleuniqueID"})' --description
    "Rule for data transfer service to send notifications for an import job
    with OCID ocid1.datatransferjob.oc1..exampleuniqueID"
Creating topic DTSImportJobTopic_2pwaqq
{
    "data": {
        "api-endpoint": "https://cell1.notification.us-phoenix-1.oraclecloud.com",
        "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
        "defined-tags": {},
        "description": "Topic for data transfer service import job with OCID
        ocid1.datatransferjob.oc1..exampleuniqueID",
        "etag": "null",
        "freeform-tags": {},
        "lifecycle-state": "ACTIVE",
        "name": "DTSImportJobTopic_2pwaqq",
        "time-created": "2020-07-15T18:26:07.179000+00:00",
        "topic-id": "ocid1.onstopic.oc1..exampleuniqueID"
    },
    "etag": "2e5a567d"
}
```

Enter email addresses to subscribe to as a comma separated list. Example:

```
jdoe@mycompany.com,rroe@mycompany.com : jsmith@mycompany.com
```

Creating subscription for jsmith@mycompany.com
Preparing Upload Configuration Files

The Project Sponsor is responsible for creating or obtaining configuration files that allow the uploading of user data to the import appliance. Send these configuration files to the Data Administrator where they can be placed in the Control Host (if there are separate Control and Data Hosts). The config file is for the data transfer administrator, the IAM user with the authorization and permissions to create and manage transfer jobs. The config_upload_user file is for the data transfer upload user, the temporary IAM user that Oracle uses to upload your data on your behalf.

Create a base Oracle Cloud Infrastructure directory and two configuration files with the required credentials.
Creating the Data Transfer Directory

Create a Oracle Cloud Infrastructure directory (.oci) on the same Control Host machine where the Oracle Cloud Infrastructure CLI is installed. For example:

```bash
mkdir /root/.oci/
```

The two configuration files (config and config_upload_user) are placed in whatever location you choose.

**Note:**
You can store the configuration files anywhere on your Control Host. The root directory is only given as an example.

Creating the Data Transfer Administrator Configuration File

The data transfer administrator configuration file contains the required credentials for working with Oracle Cloud Infrastructure. You can create this file using a setup CLI or manually using a text editor.

**Using the Setup CLI**

Run the `oci setup config` command line utility to walk through the first-time setup process. The command prompts you for the information required for the configuration file and the API public/private keys. The setup dialog generates an API key pair and creates the configuration file.

For more information about how to find the required information, see:

- Where to Get the Tenancy's OCID and User's OCID on page 4184
- Regions and Availability Domains on page 180

**Manual Setup**

If you want to set up the API public/private keys yourself and write your own configuration file, see SDK and Tool Configuration.

**Tip:**
Use the `oci setup keys` command to generate a key pair to include in the config file.

Create the data transfer administrator configuration file `/root/.oci/config` with the following structure:

```ini
[DEFAULT]
user=<The OCID for the data transfer administrator>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user's private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1, and ap-osaka-1.>
```

For example:

```ini
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..<exampleuniqueID>.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1
```
For the data transfer administrator, you can create a single configuration file that contains different profile sections with the credentials for multiple users. Then use the `--profile` option to specify which profile to use in the command. Here is an example of a data transfer administrator configuration file with different profile sections:

```ini
[DEFAULT]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..exampleuniqueID
region=us-ashburn-1

[PROFILE1]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..exampleuniqueID
region=us-ashburn-1
```

By default, the DEFAULT profile is used for all CLI commands. For example:

```bash
oci dts job create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket MyBucket --display-name MyDisplay --device-type appliance
```

Instead, you can issue any CLI command with the `--profile` option to specify a different data transfer administrator profile. For example:

```bash
oci dts job create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket MyBucket --display-name MyDisplay --device-type appliance --profile MyProfile
```

Using the example configuration file above, the `<profile_name>` would be `profile1`.

If you created two separate configuration files, use the following command to specify the configuration file to use:

```bash
oci dts job create --compartment-id <compartment_id> --bucket <bucket_name> --display-name <display_name> --config
```

Creating the Data Transfer Upload User Configuration File

The `config_upload_user` configuration file is for the data transfer upload user, the temporary IAM user that Oracle uses to upload your data on your behalf. Create this configuration file with the following structure:

```ini
[DEFAULT]
user=<The OCID for the data transfer upload user>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user's private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1, and ap-osaka-1.>
```

Adding Object Storage Endpoints

Include the line `endpoint=<url>` for the Object Storage API endpoint in the upload user configuration file.
For example:

```
endpoint=https://objectstorage.us-phoenix-1.oraclecloud.com
```

Click [here](https://example.com) to view a list of endpoints.

A complete configuration including the Object Storage endpoint might look like this:

```
[DEFAULT]
user=ocid1.user.oc1..exampleuniqueID
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
region=us-phoenix-1
endpoint=https://objectstorage.us-phoenix-1.oraclecloud.com
```

**Important:**

Creating an upload user configuration file with multiple profiles is *not* supported.

### Configuration File Entries

The following table lists the basic entries that are required for each configuration file and where to get the information for each entry.

**Note:**

Data Transfer Service does not support passphrases on the key files for both data transfer administrator and data transfer upload user.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description and Where to Get the Value</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>OCID of the data transfer administrator or the data transfer upload user, depending on which profile you are creating. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>fingerprint</td>
<td>Fingerprint for the key pair being used. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>key_file</td>
<td>Full path and filename of the private key. <strong>Important:</strong> The key pair must be in PEM format. For instructions on generating a key pair in PEM format, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
You can verify the data transfer upload user credentials using the following command:

```
oci dts job verify-upload-user-credentials --bucket <bucket_name>
```

### Requesting the Import Appliance

This section describes how to request an import appliance from Oracle for copying your data to Oracle Cloud Infrastructure. See Import Appliances on page 1069 for complete details on all tasks related to transfer jobs.

Oracle Cloud Infrastructure customers can use import appliances to migrate data for free. You are only charged for Object Storage usage once the data is successfully transferred to your designated bucket. All appliance requests still require approval from Oracle.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description and Where to Get the Value</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>tenancy</td>
<td>OCID of your tenancy. To get the value, see Required Keys and OCIDs on page 4179.</td>
<td>Yes</td>
</tr>
<tr>
<td>region</td>
<td>An Oracle Cloud Infrastructure region. See Regions and Availability Domains on page 180.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Data transfer is supported in US East (Ashburn), US West (Phoenix), Germany Central (Frankfurt), and UK South (London).</td>
<td></td>
</tr>
</tbody>
</table>

Tip:

To save time, identify the data you intend to upload and make data copy preparations before requesting the import appliance.

Creating an appliance request returns an Oracle-assigned appliance label. For example:

```
XA8XM27EH
```

**To request an appliance using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.

   Choose the transfer job that for which you want to request an import appliance.

2. Click Request Transfer Appliance under Transfer Appliances.

   The Request Transfer Appliance dialog appears.
3. Provide the shipping address details where you want the import appliance sent.

- **Company Name**: Required. Specify the name of the company that owns the data being migrated to Oracle Cloud Infrastructure.
- **Recipient Name**: Required. Specify the name of the recipient of the import appliance.
- **Recipient Phone Number**: Required. Specify the recipient's phone number.
- **Recipient Email Address**: Required. Specify the recipient's email address.
- **Care Of**: Optional intermediary party responsible for transferring the import appliance shipment from the delivery vendor to the intended recipient.
- **Address Line 1**: Required. Specify the street address to where the import appliance is sent.
- **Address Line 2**: Optional identifying address details like building, suite, unit, or floor information.
- **City/Locality**: Required. Specify the city or locality.
- **State/Province/Region**: Required. Specify the state, province, or region.
- **Zip/Postal Code**: Specify the zip code or postal code.
- **Country**: Required. Select the country.

4. Click **Request Transfer Appliance**.

*To request an appliance using the CLI*

```
oci dts appliance request --job-id <job_id> --addressee <addressee>
--care-of <care_of> --address1 <address_line1> --city-or-locality <city_or_locality>
--state-province-region <state_province_region> --country <country> --zip-postal-code <zip_postal_code>
--phone-number <phone_number> --email <email> <options>
```

*<options>* are:

- **--address2**: Optional address of the addressee (line 2).
- **--address3**: Optional address of the addressee (line 3).
- **--address4**: Optional address of the addressee (line 4).
- **--from-json**: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The **--generate-full-command-json-input** option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: [https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions](https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions).

For example:

```
oci dts appliance request --job-id ocid1.datatransferjob.oc1..exampleuniqueID --addressee MyCompany --care-of "John Doe" --address1 "123 Main Street" --city-or-locality Anytown --state-province-region NY --country USA --zip-postal-code 12345 --phone-number 8005551212 --email john.doe@mycompany.com
```

```json
{
  "data": {
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "creation-time": "2020-05-20T22:08:13+00:00",
    "customer-received-time": null,
    "customer-returned-time": null,
    "customer-shipping-address": {
      "address1": "123 Main Street",
      "address2": null,
```
When you submit an appliance request, Oracle generates a unique label (label: "XAKWEGKZ5T") to identify the import appliance and your request is sent to Oracle for approval and processing.

**Setting Up Import Appliance Request Notifications from the CLI**

You can generate notifications that send messages regarding changes to your import appliance request by using the `setup-notifications` command through the CLI. Running this command creates a topic, subscription for list of email addresses, and also a rule that notifies you on all events related to the import appliance request's activities and changes in state. This method provides a more convenient way to generate notifications tailored to import appliance requests.

Running the CLI command prompts you to enter the email addresses of each notification subscriber as a comma separated list. Each recipient is sent an email with a link to confirm they want to receive the notifications.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up notifications from the CLI affects all import appliances in your tenancy. You cannot specify notifications for individual appliances.</td>
</tr>
</tbody>
</table>

**Setting Up Notifications for a New Import Appliance Request**

To include job notifications when requesting an import appliance, include the `--setup-notifications` option in the CLI:

```
oci dts appliance request --job-id <job_id> --addressee <addressee> --address1 <address_line1> --city-or-locality <city_or_locality> --state-or-region <state_or_region> --country <country> --zip-code <zip> ... --setup-notifications
```

**Setting up Notifications for an Existing Import Appliance Request**

To set up notifications for an existing import appliance request, run the `appliance setup-notifications` CLI on the appliance:

```
oci dts appliance setup-notifications --appliance-label <appliance_label>
```

**Notifying the Data Administrator**

When you have completed all the tasks in this topic, provide the Data Administrator of the following:
Data Transfer

- IAM login credentials
- Oracle Cloud Infrastructure CLI configuration files
- Transfer job ID
- Appliance label

What’s Next

You are now ready to configure your system for the data transfer. See Configuring Appliance Data Imports on page 1038.

Configuring Appliance Data Imports

This topic describes the tasks associated with configuring the Appliance-Based Data Import. The Infrastructure Engineer role typically performs these tasks. See Roles and Responsibilities on page 1017.

Unpacking and Connecting the Import Appliance to the Network

When the shipping vendor delivers your import appliance, Oracle updates the status as Delivered and provides the date and time the appliance was received in the Transfer Appliance Details.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your import appliance arrives in a transit case with a telescoping handle and wheels. The case amenities allow for easy movement to the location where you intend to place the appliance to upload your data.</td>
</tr>
</tbody>
</table>

| Retain all packaging materials! When shipping the import appliance back to Oracle, you must package the appliance in the same manner and packaging in which the appliance was received. |

Here are the tasks involved in unpacking and getting your import appliance ready to configure.

1. Inspect the tamper-evident security tie on the transit case.

   If the appliance was tampered with during transit, the tamper-evident security tie serves to alert you.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the security tie is damaged or is missing, do not plug the appliance into your network! Immediately file a Service Request (SR).</td>
</tr>
</tbody>
</table>
2. Remove and compare the number on the security tie with the number logged by Oracle.

To see the security tie number logged by Oracle using the Console

a. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
b. Find the transfer job and import appliance associated with the removed security tie.
c. Click the **Actions** icon ( ), and then click **View Details**.
d. Look at the contents of the **Send Security Tie ID** field in the **Transfer Appliance Details** and compare that number with the number on the physical tag.

To see the security tie number logged by Oracle using the CLI

```
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```

For example:

```
oci dts appliance show --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

```json
{
  "data": {
    "delivery-security-tie-id": "exampleuniqueID",
    "label": "XAKWEGKZ5T",
    "lifecycle-state": "PROCESSING",
    "next-billing-time": null,
    "return-security-tie-id": "exampleuniqueID",
    "serial-number": "exampleuniqueserialnumber",
    "transfer-job-id": "ocid1.datatransferjob.oc1..exampleuniqueID",
    "upload-status-log-uri": "JAKQVAGJF/XAKWEGKZ5T/upload_summary.txt"
  }
}
```
Compare the value of the `delivery-security-tie-id` attribute with the number on the physical tag to ensure they match.

**Caution:**
If the number on the physical security tie does not match the number logged by Oracle, do not plug the appliance into your network! Immediately file a Service Request (SR).

**Note:**
Keep possession of the security tie after you have finished unpacking and connecting the appliance. Include it when returning the appliance to Oracle. Failure to include the security tie can result in a delay in the data migration process.

3. Open the transit case and ensure that the case contains the following items:
   - Appliance unit and power cable (two types of power cables provided: C14 and C13 to 14)
   - USB to DB-9 serial cable
   - Return shipping instructions (retain these instructions)
   - Return shipping label, label sleeve, tie-on tag, and zip tie
   - Return shipment tamper-evident security tie (use this tie to ensure secure transit case back to Oracle)

4. Compare the number on the return shipment security tie with the number logged by Oracle.

To see the security tie number logged by Oracle using the Console

a. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.  
b. Find the transfer job and import appliance associated with the return shipment security tie.  
c. Click the actions icon (⃣), and then click **View Details**.
   d. Look at the contents of the **Return Security Tie ID** field in the **Transfer Appliance Details** and compare that number with the number on the physical tag.

To see the security tie number logged by Oracle using the CLI

```bash
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```

For example:

```bash
oci dts appliance show --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

```json
{
    "data": {
        "appliance-delivery-tracking-number": null,
        "appliance-delivery-vendor": null,
        "appliance-return-delivery-tracking-number": null,
        "creation-time": "2020-05-20T22:08:13+00:00",
        "customer-received-time": null,
        "customer-returned-time": null,
        "customer-shipping-address": {
            "address1": "123 Main Street",
            "address2": null,
            "address3": null,
            "address4": null,
            "addressee": "MyCompany",
            "care-of": "John Doe",
        }...
    }
}
```
Compare the value of the `return-security-tie-id` attribute with the number on the physical tag to ensure they match.

**Caution:**
If the number on the return security tie does not match the number logged by Oracle, file a Service Request (SR). These security tie numbers must match or Oracle cannot upload data from your returned appliance.

5. Remove the import appliance from the case and place the appliance on a solid surface or in a rack.

**Caution:**
We recommend assistance lifting the appliance out of the transit case and placing the appliance in a rack or on a desk top. The total shipping weight is about 64 lbs (29.0299 kg) and appliance weight is 38 lbs (17.2365 kg).

6. Connect the appliance to your local network using one of the following:
   - 10GBase-T: Standard RJ-45
   - SFP+: The transceiver must be compatible with Intel X520 NICs.

7. Attach one of the provided power cords to the appliance and plug the other end into a grounded power source.

8. Turn on the appliance by flipping the power switch on the back of the appliance.

**Connecting the Import Appliance to the Terminal Emulation Host**

Connect the import appliance to your designated Terminal Emulation Host computer using the provided USB to DB-9 serial cable.

**Note:**
You might need to download the driver for this cable on your Terminal Emulation Host: [https://www.cablestogo.com/product/26887/5ft-usb-to-db9-male-serial-rs232-adapter-cable#support](https://www.cablestogo.com/product/26887/5ft-usb-to-db9-male-serial-rs232-adapter-cable#support)

**Setting Up Terminal Emulation**

Appliance-based transfers require you to set up your host for terminal emulation so you can communicate with the appliance through the appliance's serial console. This communication requires installing serial console terminal emulator software. We recommend using the following:

- PuTTY for Windows
- ZOC for OS X
- PuTTY or Minicom for Linux

Configure the following terminal emulator software settings:
• Baud Rate: 115200
• Emulation: VT102
• Handshaking: Disabled/off
• RTS/DTS: Disabled/off

Note:
PuTTY does not allow you to configure all of these settings individually. However, you can configure the PuTTY default settings by selecting the Serial connection type and specifying "115200" for the Serial Line baud speed. This configuration is sufficient to use PuTTY as a terminal emulator for the appliance.

Configuring the Import Appliance Networking

When the import appliance boots up, an appliance serial console configuration menu is displayed on the Terminal Emulation Host to which the appliance is connected.

Oracle Cloud Data Transfer Appliance
   - For use with minimum dts version: dts-0.4.140
   - See "Help" for determining your dts version

1) Configure Networking
2) Show Networking
3) Reset Authentication
4) Show Authentication
5) Show Status
6) Collect Appliance Diagnostic Information
7) Generate support bundle
8) Shutdown Appliance
9) Reboot Appliance
10) Help

Select a command:

Note:
It can take up to 5 minutes for the serial console menu to display. Press Enter if you do not see the serial console configuration menu after this amount of time.

The appliance supports a single active network interface on any of the 10-Gbps network ports. If only one interface is cabled and active, that interface is chosen automatically. When multiple interfaces are active, you are given the choice to select the interface to use.

To configure your import appliance networking

1. From the Terminal Emulation Host, select Configure Networking from the appliance serial console menu.
2. Provide the required networking information when prompted:

   • **IP Address**: IP address of the appliance.
   • **Subnet Mask Length**: The count of leading 1 bit in the subnet mask. For example, if the subnet mask is 255.255.255.0 then the length is 24.
   • **Default Gateway**: Default gateway for network communications.

For example:

Configure Networking:
^C to cancel

Configuring IP address, subnet mask length, gateway

Example:
### Data Transfer

- **IP Address**: 10.0.0.2
- **Subnet Mask Length**: 24
- **Gateway**: 10.0.0.1

- **Address**: 10.0.0.1
- **Subnet Mask Length**: 24
- **Gateway**: 10.0.0.1

**Configuring IP address 10.0.0.1 netmask 255.255.255.0 default gateway 10.0.0.1**

**Enabling enp0s3**

**Now trying to restart the network**

**Network configuration is complete**

**New authentication material created.**

- **Client access token**: 4iH1gw1lokPJ0

Press ENTER to return...

---

When you configure a network interface, the appliance software generates a new client access token and appliance X.509/SSL certificate. The access token is used to authorize your Control Host to communicate with the Data Transfer Appliance's Management Service. The x.509/SSL certificate is used to encrypt communications with the Data Transfer Appliance's Management Service over the network. Provide the access token and SSL certificate fingerprint values displayed here when you use the CLI commands to **initialize authentication on your host machine**.

You can change the selected interface, network information, and reset the authentication material at any time by selecting **Configure Networking** again from the appliance serial console menu.

### Notifying the Data Administrator

After completing the tasks in this topic, send the following import appliance information to the Data Administrator:

- Appliance IP address
- Access token
- SSL certificate fingerprint

### What's Next

You are now ready to load your data to the disk. See **Copying Data to the Import Appliance** on page 1043.

### Copying Data to the Import Appliance

This topic describes the tasks associated with copying data from the Data Host to the import appliance using the Control Host. The Data Administrator role typically performs these tasks. See **Roles and Responsibilities** on page 1017.

**Note:**

You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

### Information Prerequisites

Before performing any import appliance copying tasks, you must obtain the following information:
• Appliance IP address - typically is provided by the Infrastructure Engineer.
• IAM login information, Data Transfer Utility configuration files, transfer job ID, and appliance label - typically is provided by the Project Sponsor.

**Setting Up an HTTP Proxy Environment**

You might need to set up an HTTP proxy environment on the Control Host to allow access to the public internet. This proxy environment allows the Oracle Cloud Infrastructure CLI to communicate with the Data Transfer Appliance Management Service and the import appliance over a local network connection. If your environment requires internet-aware applications to use network proxies, configure the Control Host to use your environment's network proxies by setting the standard Linux environment variables on your Control Host.

Assume that your organization has a corporate internet proxy at http://www-proxy.myorg.com and that the proxy is an HTTP address at port 80. You would set the following environment variable:

```
export HTTPS_PROXY=http://www-proxy.myorg.com:80
```

If you configured a proxy on the Control Host and the appliance is directly connected to that host, the Control Host tries unsuccessfully to communicate with the appliance using a proxy. Set a `no_proxy` environment variable for the appliance. For example, if the appliance is on a local network at 10.0.0.1, you would set the following environment variable:

```
export NO_PROXY=10.0.0.1
```

**Setting Firewall Access**

If you have a restrictive firewall in the environment where you are using the Oracle Cloud Infrastructure CLI, you may need to open your firewall configuration to the following IP address ranges: 140.91.0.0/16.

**Initializing Authentication to the Import Appliance**

**Note:**

You can only use the Oracle Cloud Infrastructure CLI to initialize authentication.

Initialize authentication to allow the host machine to communicate with the import appliance. Use the values returned from the `Configure Networking` command. See Configuring the Transfer Appliance Networking for details.

**To initialize authentication using the CLI**

Perform this task using the following CLI. There is no Console equivalent.

```
oci dts physical-appliance initialize-authentication --job-id <job-id> --appliance-cert-fingerprint <fingerprint> --appliance-ip <ip_address> --appliance-label <appliance-label>
```

For example:

```
```

When prompted, supply the access token and system. For example:

```
```

Retrieving the Appliance serial id from Oracle Cloud Infrastructure.
Access token ('q' to quit):
Found an existing appliance. Is it OK to overwrite it? [y/n] y
Registering and initializing the authentication between the dts CLI and the appliance
Appliance Info:
  encryptionConfigured: false
  lockStatus: NA
  finalizeStatus: NA
  totalSpace: Unknown
  availableSpace: Unknown

The Control Host can now communicate with the import appliance.

To show details about the connected appliance using the CLI

At the command prompt on the host, run `oci dts physical-appliance show` to show the status of the connected import appliance.

```
oci dts physical-appliance show
```

For example:

```
Appliance Info:
  encryptionConfigured: false
  lockStatus: NA
  finalizeStatus: NA
  totalSpace: Unknown
  availableSpace: Unknown
```

Configuring Import Appliance Encryption

Configure the import appliance to use encryption. Oracle Cloud Infrastructure creates a strong passphrase for each appliance. The command securely collects the strong passphrase from Oracle Cloud Infrastructure and sends that passphrase to the Data Transfer service.

If your environment requires Internet-aware applications to use network proxies, ensure that you set up the required Linux environment variables. See for more information.

**Important:**

If you are working with multiple appliances at the same time, be sure the job ID and appliance label you specify in this step matches the physical appliance you are currently working with. You can get the serial number associated with the job ID and appliance label using the Console or the Oracle Cloud Infrastructure CLI. You can find the serial number of the physical appliance on the back of the device on the agency label.

**Note:**

You can only use the Oracle Cloud Infrastructure CLI to configure encryption.

To configure import appliance encryption using the CLI

At the command prompt on the host, run `oci dts physical-appliance configure-encryption` to configure import appliance encryption.

```
oci dts physical-appliance configure-encryption --job-id <job_id> --appliance-label <appliance_label>
```
Data Transfer

For example:

```
oci dts physical-appliance configure-encryption --job-id
ocid1.datatransferjob.region1.phx..exampleuniqueID --appliance-label
XA8XM27EVH
```

Moving the state of the appliance to preparing...
Passphrase being retrieved...
Configuring encryption...
Encryption configured. Getting physical transfer appliance info...

```
{
  "data": {
    "availableSpaceInBytes": "Unknown",
    "encryptionConfigured": true,
    "finalizeStatus": "NA",
    "lockStatus": "LOCKED",
    "totalSpaceInBytes": "Unknown"
  }
}
```

Unlocking the Import Appliance

You must unlock the appliance before you can write data to it. Unlocking the appliance requires the strong passphrase that is created by Oracle Cloud Infrastructure for each appliance. Unlocking can be accomplished in two different ways:

- If you provide the `--job-id` and `--appliance-label` when running the `unlock` command, the data transfer system retrieves the passphrase from Oracle Cloud Infrastructure and sends it to the appliance during the unlock operation.
- You can query Oracle Cloud Infrastructure for the passphrase and provide that passphrase when prompted during the unlock operation.

**Important:**

It can take up to 10 minutes to unlock an appliance the first time. Subsequent unlocks are not as time consuming.

**Note:**

You can only use the Oracle Cloud Infrastructure CLI to unlock the import appliance.

To unlock the appliance and send the passphrase to the appliance using the CLI

```
oci dts physical-appliance unlock --job-id <job_id> --appliance-label <label>
```

For example:

```
oci dts physical-appliance unlock --job-id
ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

Retrieving the passphrase from Oracle Cloud Infrastructure

```
{
  "data": {
    "availableSpaceInBytes": "64.00GB",
    "encryptionConfigured": true,
    "finalizeStatus": "NOT_FINALIZED",
    "lockStatus": "NOT_LOCKED",
    "totalSpaceInBytes": "64.00GB"
  }
}
```
To query Oracle Cloud Infrastructure for the passphrase to unlock the import appliance using the CLI

```bash
oci dts appliance get-passphrase --job-id <job_id> --appliance-label <label>
```

For example:

```bash
oci dts appliance get-passphrase --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
{
  "data": {
    "encryption-passphrase": "passphrase"
  }
}
```

Run `dts physical-appliance unlock` without `--job-id` and `--appliance-label` and supply the passphrase when prompted to complete the task:

```bash
oci dts physical-appliance unlock
```

Creating NFS Datasets

A dataset is a collection of files that are treated similarly. You can write up to 100 million files onto the import appliance for migration to Oracle Cloud Infrastructure. We currently support one dataset per appliance. Appliance-Based Data Import supports NFS versions 3, 4, and 4.1 to write data to the appliance. In preparation for writing data, create and configure a dataset to write to. See Datasets on page 1077 for complete details on all tasks related to datasets.

To create a dataset using the CLI

```bash
oci dts nfs-dataset create --name <dataset_name>
```

For example:

```bash
oci dts nfs-dataset create --name nfs-ds-1
```

Creating dataset with NFS export details nfs-ds-1

```json
{
  "data": {
    "datasetType": "NFS",
    "name": "nfs-ds-1",
    "nfsExportDetails": {
      "exportConfigs": null,
      "state": "INITIALIZED"
    }
  }
}
```

Configuring Export Settings on the Dataset

To configure export settings on a dataset using the CLI

```bash
oci dts nfs-dataset set-export --name <dataset_name> --rw true --world true
```

For example:

```bash
oci dts nfs-dataset set-export --name nfs-ds-1 --rw true --world true
```

Settings NFS exports to dataset nfs-ds-1

```json
{
  "data": {
    "datasetType": "NFS",
```

Oracle Cloud Infrastructure User Guide
Here is another example of creating the export to give read/write access to a subnet:

```
oci dts nfs-dataset set-export --name nfs-ds-1 --ip 10.0.0.0 --subnet-mask-length 24 --rw true --world false
```

Settings NFS exports to dataset nfs-ds-1
```
{
    "data": {
        "datasetType": "NFS",
        "name": "nfs-ds-1",
        "nfsExportDetails": {
            "exportConfigs": [
                {
                    "hostname": null,
                    "ipAddress": "10.0.0.0",
                    "readWrite": true,
                    "subnetMaskLength": "24",
                    "world": false
                }
            ],
            "state": "INITIALIZED"
        }
    }
}
```

Activating the Dataset

Activation creates the NFS export, making the dataset accessible to NFS clients.

To activate the dataset using the CLI

```
oci dts nfs-dataset activate --name <dataset_name>
```

For example:

```
oci dts nfs-dataset activate --name nfs-ds-1
```

Fetching all the datasets
Activating dataset small-files
Dataset nfs-ds-1 activated

Setting Your Data Host as an NFS Client

**Note:**

Only Linux machines can be used as Data Hosts.
Set up your Data Host as an NFS client:

- For Debian or Ubuntu, install the `nfs-common` package. For example:
  
  ```bash
  sudo apt-get install nfs-common
  ```

- For Oracle Linux or Red Hat Linux, install the `nfs-utils` package. For example:
  
  ```bash
  sudo yum install nfs-utils
  ```

### Mounting the NFS Share

**To mount the NFS share**

At the command prompt on the Data Host, create the mountpoint directory:

```bash
mkdir -p /mnt/<mountpoint>
```

For example:

```bash
mkdir -p /mnt/nfs-ds-1
```

Next, use the `mount` command to mount the NFS share.

```bash
mount -t nfs <appliance_ip>:/data/<dataset_name> <mountpoint>
```

For example:

```bash
mount -t nfs 10.0.0.1:/data/nfs-ds-1 /mnt/nfs-ds-1
```

**Note:**

The appliance IP address in this example (10.0.0.1) may be different than the one you use for your appliance.

After the NFS share is mounted, you can write data to the share.

### Copying Files to the NFS Share

You can only copy regular files to transfer appliances. You cannot copy special files, such as symbolic links, device special, sockets, and pipes, directly to the Data Transfer Appliance. See the following section for instructions on how to prepare special files.

**Important:**

- Individual files being copied to the transfer appliance cannot exceed 9.76 TB.
- Do not fill up the transfer appliance to 100% capacity. There must be space available to generate metadata and for the manifest file to perform the upload to Object Storage. At least 1 GB of free disk space is needed for this area.

### Copying Special Files

To transfer special files, create a tar archive of these files and copy the tar archive to the Data Transfer Appliance. We recommend copying many small files using a tar archive. Copying a single compressed archive file should also take less time than running copy commands such as `cp -r` or `rsync`.

Here are some examples of creating a tar archive and getting it onto the Data Transfer Appliance:

- Running a simple tar command:
  
  ```bash
tar -cvzf /mnt/nfs-dts-1/filesystem.tgz filesystem/
  ```
Running a command to create a file with md5sum hashes for each file in addition to the tar archive:

```bash
tar cvzf /mnt/nfs-dts-1/filesystem.tgz filesystem/ | xargs -I '{}' sh -c "test -f '{}' && md5sum '{}''" | tee tarzip_md5
```

The tar archive file `filesystem.tgz` has a base64 md5sum once it is uploaded to OCI Object Storage. Store the `tarzip_md5` file where you can retrieve it. After the compressed tar archive file is downloaded from Object Storage and unpacked, you can compare the individual files against the hashes in the file.

**Deactivating the Dataset**

**Note:**

Deactivating the dataset is only required if you are running appliance commands using the Data Transfer Utility. If you are using the Oracle Cloud Infrastructure CLI to run your Appliance-Based Data Import, you can skip this step and proceed to Sealing the Dataset on page 1050.

After you are done writing data, deactivate the dataset. Deactivation removes the NFS export on the dataset, disallowing any further writes.

*To deactivate the dataset using the CLI*

At the command prompt on the host, run `dts nfs-dataset deactivate` to deactivate the NFS dataset.

```bash
oci dts nfs-dataset deactivate --name <dataset_name>
```

For example:

```bash
oci dts nfs-dataset deactivate --name nfs-ds-1
```

**Sealing the Dataset**

Sealing a dataset stops all writes to the dataset. This process can take some time to complete, depending upon the number of files and total amount of data copied to the import appliance.

If you issue the `seal` command without the `--wait` option, the seal operation is triggered and runs in the background. You are returned to the command prompt and can use the `seal-status` command to monitor the sealing status. Running the `seal` command with the `--wait` option results in the seal operation being triggered and continues to provide status updates until sealing completion.

The sealing operation generates a manifest across all files in the dataset. The manifest contains an index of the copied files and generated data integrity hashes.

*To seal the dataset using the CLI*

```bash
oci dts nfs-dataset seal --name <dataset_name> [--wait]
```

For example:

```bash
oci dts nfs-dataset seal --name nfs-ds-1
```

**Seal initiated. Please use seal-status command to get progress.**

*To monitor the dataset sealing process using the CLI*

```bash
oci dts nfs-dataset seal-status --name <dataset_name>
```

For example:

```bash
oci dts nfs-dataset seal-status --name nfs-ds-1
```
Downloading the Dataset Seal Manifest

After sealing the dataset, you can optionally download the dataset’s seal manifest to a user-specified location. The manifest file contains the checksum details of all the files. The transfer site uploader consults the manifest file to determine the list of files to upload to object storage. For every uploaded file, it validates that the checksum reported by object storage matches the checksum in manifest. This validation ensures that no files got corrupted in transit.

To download the dataset seal manifest file using the CLI

```
oci dts nfs-dataset get-seal-manifest --name <dataset_name> --output-file <file_path>
```

For example:

```
oci dts nfs-dataset get-seal-manifest --name nfs-ds-1 --output-file ~/Downloads/seal-manifest
```

Finalizing the Import Appliance

```
Note:

You can only use the CLI commands to finalize the import appliance.
```

Finalizing an appliance tests and copies the following to the appliance:

- Upload user configuration credentials
- Private PEM key details
- Name of the upload bucket

The credentials, API key, and bucket are required for Oracle to be able to upload your data to Oracle Cloud Infrastructure Object Storage. When you finalize an appliance, you can no longer access the appliance for dataset operations unless you unlock the appliance. See Reopening a Dataset on page 1080 if you need to unlock an appliance that was finalized.

```
Important:

If you are working with multiple appliances at the same time, be sure the job ID and appliance label you specify in this step matches the physical appliance you are currently working with. You can get the serial number associated with the job ID and appliance label using the Console or the Oracle Cloud Infrastructure CLI. You can find the serial number of the physical appliance on the back of the device on the agency label.
```
**To finalize the import appliance**

1. Seal the dataset before finalizing the import appliance. See Sealing the Dataset on page 1050.
2. Open a command prompt on the host and run `oci dts physical-appliance finalize` to finalize an appliance.

   ```
   oci dts physical-appliance finalize --job-id <job_id> --appliance-label <appliance_label>
   
   For example:
   
   oci dts physical-appliance finalize --job-id ocid1.datatransferjob.region1.phx..exampleuniqueID --appliance-label XAKWEGKZ5T
   
   Retrieving the upload summary object name from Oracle Cloud Infrastructure
   Retrieving the upload bucket name from Oracle Cloud Infrastructure
   Validating the upload user credentials
   Create object BulkDataTransferTestObject in bucket MyBucket using upload user
   Overwrite object BulkDataTransferTestObject in bucket MyBucket using upload user
   Inspect object BulkDataTransferTestObject in bucket MyBucket using upload user
   Read bucket metadata MyBucket using upload user
   Storing the upload user configuration and credentials on the transfer appliance
   Finalizing the transfer appliance...
   
   The transfer appliance is locked after finalize. Hence the finalize status will be shown as NA. Please unlock the transfer appliance again to see the correct finalize status
   Changing the state of the transfer appliance to FINALIZED
   
   ```

   ```json
   {  
     "data": {  
       "availableSpaceInBytes": "Unknown",  
       "encryptionConfigured": true,  
       "finalizeStatus": "NA",  
       "lockStatus": "LOCKED",  
       "totalSpaceInBytes": "Unknown"  
     }  
   }
   ```

   **Note:**

   If changes are necessary after sealing a dataset or finalizing an appliance, you must reopen the dataset to modify the contents. See Reopening a Dataset on page 1080.

**What's Next**

You are now ready to ship your import appliance with the copied data to Oracle. See Shipping the Import Appliance on page 1052.

**Shipping the Import Appliance**

This topic describes the tasks associated with shipping the import appliance containing the copied data to Oracle. The Infrastructure Engineer role typically performs these tasks. See Roles and Responsibilities on page 1017.
Note:
You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

Shutting Down the Import Appliance

Shut down the import appliance before packing up and shipping the appliance back to Oracle.

To shut down the import appliance

Using the terminal emulator on the host machine, select Shutdown from the appliance serial console.

Important:
The shutdown does not power off the appliance. Wait 10 minutes after issuing the shutdown, then turn the power switch off and disconnect the power cable.

Packing and Shipping the Import Appliance to Oracle

Return the import appliance to Oracle within 30 days. If you need the appliance beyond the standard 30-day window, you can file a service request to ask for an extension of up to 60 days.

Important:
Review and follow the instructions that were provided in the transit case with the appliance.

To pack and ship the import appliance

1. Unplug the power cord from the power source and detach the other end of the cord from the appliance.
2. Disconnect the appliance from your network.
3. Remove the return shipment tamper-evident security tie from the transit case.
4. Place the appliance, power cord, and serial cable in the transit case.
5. Close and secure the transit case with the return tamper-evident security tie.
6. Loop the top of the plastic tie-on tag with return shipping label through the handle of the transit case. Remove the protective tape from the back of the tie-on tag, exposing the adhesive area on which to secure the tag onto itself. Use the provided zip tie to secure the tie-on tag to the handle.
7. Return the transit case:
   • If a return label was included with the import appliance, attach the label and arrange with the shipping vendor to drop off or pick up the appliance.
   • If a return label was not included, open a service request with Oracle to arrange for the appliance's return. See Creating a Service Request Using the Console on page 126.

The shipping vendor notifies Oracle when the appliance is shipped back to Oracle for upload to Oracle Cloud Infrastructure Object Storage.

What's Next

Now you can track your return import appliance shipment to Oracle and review post transfer logs and summaries. See Monitoring the Import Appliance and Data Transfer on page 1054.
Monitoring the Import Appliance and Data Transfer

This topic describes the monitoring tasks to do after sending the import appliance with the copied data back to Oracle for data transfer to Oracle Cloud Infrastructure. The Project Sponsor role typically performs these tasks. See Roles and Responsibilities on page 1017.

**Note:**
You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

Monitoring the Status of Your Import Appliance Return Shipment

The shipping vendor notifies Oracle when your import appliance is picked up and shipped back for upload to Oracle Cloud Infrastructure Object Storage.

**To monitor the status of your import appliance return shipment using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the transfer job and associated import appliance that you shipped back to Oracle for data upload.
3. Under Transfer Appliances, look at the Status field.

**To monitor the status of your import appliance return shipment using the CLI**

```
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```

For example:

```
oci dts appliance show --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

```json
{
"data": {
"appliance-delivery-tracking-number": null,
"appliance-delivery-vendor": null,
"appliance-return-delivery-tracking-number": null,
"creation-time": "2020-05-20T22:08:13+00:00",
"customer-received-time": null,
"customer-returned-time": null,
"customer-shipping-address": {
"address1": "123 Main Street",
"address2": null,
"address3": null,
"address4": null,
"addressee": "MyCompany",
"care-of": "John Doe",
"city-or-locality": "Anytown",
"country": "USA",
"email": "john.doe@mycompany.com",
"phone-number": "3115551212",
"state-or-region": "NY",
"zipcode": "12345"
},
"delivery-security-tie-id": "exampleuniqueID",
"label": "XAKWEGKZ5T",
"lifecycle-state": "PROCESSING",
```
The import appliance status is indicated by the `lifecycle-state` attribute.

**Import Appliance Status Values**

Here are the import appliance status values, listed in alphabetic order:

**CANCELLED**
You can change your mind about uploading your data to Oracle Cloud Infrastructure Object Storage and cancel your import appliance. Ship the appliance back to Oracle and then cancel the appliance. Oracle always uses secure wipe tools on the boot and data areas whenever an appliance is returned.

**COMPLETE**
Oracle completed your import appliance data upload. Your data is available in your designated bucket in Oracle Cloud Infrastructure Object Storage.

**CUSTOMER LOST**
You have not returned the import appliance within the required 90 days.

**DELIVERED**
Oracle received a delivery confirmation from the shipping vendor that your import appliance was delivered. When the appliance is delivered, Oracle provides the date and time it was received in the appliance details. Appliance usage tracking begins.

**ERROR**
Oracle encountered an unrecoverable error trying to process your import appliance. Oracle cannot upload your data from the appliance. To protect your data, Oracle uses secure wipe tools on the boot and data areas any transfer appliance that cannot be processed. Complete another request for an appliance.

**ORACLE PREPARING**
Oracle approved your import appliance request. The status displays "Preparing" until the appliance is shipped to you.

**ORACLE RECEIVED**
Oracle received your import appliance shipment. The status displays "Oracle Received" until Oracle begins processing and uploading your data from the appliance.

**ORACLE RECEIVED CANCELED**
You canceled your import appliance after you shipped the appliance back to Oracle. Oracle received your canceled appliance does not upload any data from it.

**PREPARING**
You activated your import appliance. You can now copy your data onto the appliance. The status displays "Preparing" until you ship the appliance back to Oracle.

**PROCESSING**
Oracle is processing and uploading the data from your import appliance. The status displays "Processing" until Oracle completes uploading your data from the appliance.
REJECTED

Oracle denied your import appliance request.

**Important:**

If your appliance request is denied and you have questions, contact your Sales Representative or file a Service Request (SR).

REQUESTED

You successfully completed your request for an import appliance. The status displays requested until Oracle approves your appliance request.

RETURN SHIPPED

Oracle received confirmation from the shipping vendor that you shipped your import appliance back to Oracle. The status displays "Return Shipped" until Oracle receives your appliance.

RETURN SHIPPED CANCELLED

You canceled your import appliance after the appliance was delivered to you or after you shipped the appliance back to Oracle. Oracle received confirmation from the shipping vendor that your canceled transfer appliance is on the way back to Oracle. The status displays "Return shipped cancelled" until Oracle receives your appliance.

SHIPPING

Oracle completed the necessary preparations and shipped your import appliance. When the appliance is shipped, Oracle provides the serial number of the appliance, the shipping vendor, and the tracking number in the appliance details. The status displays shipping until the appliance is delivered to you.

**Reviewing the Upload Summary**

Oracle creates upload summary log files for each uploaded appliance. These log files are placed in the bucket where data was uploaded to Oracle Cloud Infrastructure. The upload summary file compares the appliance's manifest file to the contents of the target Oracle Cloud Infrastructure Object Storage bucket after file upload.

**Note:**

If you chose to upload your data to an Archive Storage bucket, you must first restore the log file object before you can download that file for review.

The top of the log report summarizes the overall file processing status:

| P | Present: The file is present in both the device and the target bucket |
| M | Missing: The file is present in the device but not the target bucket. It was likely uploaded and then deleted by another user before the summary was generated. |
| C | Name Collision: The file is present in the manifest but a file with the same name but different contents is present in the target bucket. |
| U | Unreadable: The file is not readable from the disk |
| N | Name Too Long: The file name on disk is too long and could not be uploaded |

Complete file upload details follow the summary.
If you upload more than 100,000 files, the upload details are broken into multiple pages. You can only download the first page from the Console. Download the rest of the pages directly from the Object Storage bucket. The subsequent pages have the same object name as the first page, but have an enumerated suffix.

Verifying Uploaded File Integrity

To verify object data integrity of files uploaded to Object Storage from the Data Transfer Appliance, a cryptographic hash using MD5 is provided for all objects uploaded to Object Storage from the Data Transfer Appliance. Oracle Cloud Infrastructure provides the object hash value in base64 encoding.

To download files imported into Object Storage and verify their integrity, run the following CLI command:

```
oci os object get --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --file <file_location>
```

For example:

```
oci os object get --namespace MyNamespace --bucket-name MyBucket1 --name JLA12B3C/XAABC12EFG/upload_summary.txt --file upload_summary.txt
```

Downloading object [####################################] 100%

Open the file and match the file names of the uploaded files with the MD5 column:

```
# SUMMARY FOR DEVICE [cloudstorage-appliance-1]
Generated at 2020-05-18 21:51:13
TOTAL: 10
### P present: 10
### M missing: 0
### C name collision: 0
### U unreadable: 0
### N nameTooLong: 0

<table>
<thead>
<tr>
<th>STATUS</th>
<th>NAME</th>
<th>LAST_MODIFIED</th>
<th>SIZE (MB)</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>present</td>
<td>file_5.txt</td>
<td>Mon May 18 21:51:13 UTC 2020</td>
<td>0.00</td>
<td>8gCSOiPiShA==</td>
</tr>
<tr>
<td>present</td>
<td>file_1.txt</td>
<td>Mon May 18 21:51:13 UTC 2020</td>
<td>0.00</td>
<td>EcN8s6dgT/9pGYA7Yxk1Q==</td>
</tr>
</tbody>
</table>
```

In this example, `file_1.txt` has the MD5 sum of: EcN8s6dgT/9pGYA7Yxk1Q==

To download `file_1.txt`, run the following CLI command:

```
oci os object get --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --file <file_location>
```

For example:

```
oci os object get --namespace example_namespace --bucket-name bucket-1 --name file_1.txt --file file_1.txt
```

Downloading object [####################################] 100%

Covert the base64 encoded hash value to hexadecimal, use the following command:

```
python -c 'print "BASE64-ENCODED-MD5-VALUE".decode("base64").encode("hex")'
```
For example:

```
python -c 'print "EoN8s6dgT/9pGYA7Yx1klQ==".decode("base64").encode("hex")'
12837cb3a7604fff6919803b631d6495
```

Now generate the md5sum on Linux and verify both values match:

```
md5sum <file_name>
```

For example:

```
md5sum file_1.txt
12837cb3a7604fff6919803b631d6495  file_1.txt
```

### Verifying Multipart Uploaded Files

Large files are split into 1 GB parts when they are uploaded from the Data Transfer Appliance to Object Storage. You can verify the md5sum after downloading a file that was transferred in multiple parts using one of several available scripts. See the following for more information and links to these scripts:


### Viewing Data Transfer Metrics

After the import appliance with your copied data is received by Oracle and the data transfer begins, you can view the metrics associated with the transfer job in the Transfer Appliance Details page in chart or table format.

**Tip:**

Set up your notifications to alert you when the data transfer from the appliance to Oracle Cloud Infrastructure is occurring. When the state changes from ORACLE_RECEIVED to PROCESSING, you can start viewing data transfer metrics. If you included the `--setup-notification` option when you made your appliance request from the CLI, this alert occurs automatically. See [Notifications Overview](#) on page 3350 for more information.

Select **Metrics** under **Resources** to display each of these measures:

- **Import Files Uploaded** - Total number of files uploaded for import.
- **Import Bytes Uploaded** - Total number of bytes uploaded for import.
- **Import Files Remaining** - Total number of files remaining for import upload.
- **Import Bytes Remaining** - Total number of bytes remaining for import upload.
- **Import Files in Error** - Total number of files in error for import.
- **Import Upload Verification Progress** - Progress of verification of files that have already been uploaded for import.

Select the **Start Time** and **End Time** for these measures, either by manually entering the days and times in their respective fields, or by selecting the Calendar feature and picking the times that way. As an alternative to selecting a start and end time, you can also select from a list of standard times (last hour, last 6 hours, and so forth) from the **Quick Selects** list for the period measured. The time period you specify applies to all the measures.

Specify the **Interval** (for example, 5 minutes, 1 hour) that each measure is recorded from the list.

Specify the **Statistic** being recorded (for example, Sum, Mean) for each measure from the list.
Data Transfer

Tip:
Mean is the most useful statistic for data transfer as it reflects an absolute value of the metric.

Choose additional actions from the Options list, including viewing the query in the Metrics Explorer, capturing the URL for the measure, and switching between chart and table view.

Click Reset Charts to delete any existing information in the charts and begin recording new metrics.

See Monitoring Overview on page 2660 for general information on monitoring your Oracle Cloud Infrastructure services.

Closing the Transfer Job

Close the transfer job when no further transfer job activity is required or possible. Closing a transfer job requires that the status of all associated import appliances be returned, canceled, or deleted.

To close a transfer job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the data transfer package for which you want to display the details.
3. Click the Actions icon ( ), and then click View Details.
   Alternatively, click the hyperlinked name of the transfer job.
4. Click Close Transfer Job.

To close a transfer job using the CLI

oci dts job close --job-id <job_id>

For example:

oci dts job close --job-id ocid1.datatransferjob.oc1..exampleuniqueID
{
    "data": {
        "attached-transfer-appliance-labels": [],
        "attached-transfer-device-labels": [],
        "attached-transfer-package-labels": [],
        "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
        "creation-time": "2020-05-20T22:00:43+00:00",
        "defined-tags": {},
        "device-type": "APPLIANCE",
        "display-name": "MyApplianceImportJob",
        "freeform-tags": {},
        "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
        "label": "JGX4N1XLI",
        "lifecycle-state": "CLOSED",
        "upload-bucket-name": "MyBucket"
    },
    "etag": "1"
}

The lifecycle-state attribute value is "CLOSED."

What’s Next

You have completed the process of setting up, running, and monitoring the Appliance-Based Data Import. If you determine that another appliance-based data transfers is required, repeat the procedure from the beginning.
Appliance Import Reference

This topic provides complete task details for certain components associated with Appliance-Based Data Imports. Use this topic as a reference to learn and use commands associated with components included in the Appliance-Based Data Import procedure.

Transfer Jobs

A transfer job is the logical representation of a data migration to Oracle Cloud Infrastructure. A transfer job is associated with one or more import appliances.

**Note:**

It is recommended that you create a compartment for each transfer job to minimize the required access your tenancy.

Creating Transfer Jobs

Create the transfer job in the same compartment as the upload bucket and supply a human-readable name for the transfer job.

Creating a transfer job returns a job OCID that you specify in other transfer tasks. For example:

```
oci1.datatransferjob.oci1..exampleuniqueID
```

To create a transfer job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Select the Compartment you are to use for data transfers from the list.
   A list of transfer jobs that have already been created is displayed.
3. Click Create Transfer Job.
   The Create Transfer Job dialog appears.
4. Enter a **Job Name**. Avoid entering confidential information. Then, select the **Upload Bucket** from the list.
5. Select Disk for the **Transfer Device Type**.
6. Click **Create Transfer Job**.

To create a transfer job using the CLI

```
oci dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type <device_type>
```

<display_name> is the name of the transfer job. Avoid entering confidential information.
<device_type> should always be appliance for Appliance-Based Data Import jobs.

For example:

```
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyApplianceImportJob --device-type appliance
```

```json
{
"data": {
"attached-transfer-appliance-labels": [],
"attached-transfer-device-labels": [],
"attached-transfer-package-labels": [],
"compartment-id": "ocid.compartment.oc1..exampleuniqueID",
"creation-time": "2019-12-18T19:43:58+00:00",
"defined-tags": {},
"device-type": "APPLIANCE",
"display-name": "MyApplianceImportJob",
```
Optionally, you can specify one or more defined or freeform tags when you create a transfer job. For more information about tagging, see Resource Tags on page 211.

**Defined Tags**

To specify defined tags when creating a job:

```bash
oci dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type appliance --defined-tags '{ "<tag_namespace>": { "<tag_key>": "<value>" } }'
```

For example:

```bash
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyApplianceImportJob --device-type appliance --defined-tags '{"Operations": {"CostCenter": "01"}}'
```

```json
{
   "data": {
      "attached-transfer-appliance-labels": [],
      "attached-transfer-device-labels": [],
      "attached-transfer-package-labels": [],
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "creation-time": "2019-12-18T19:43:58+00:00",
      "defined-tags": {
         "operations": {
            "costcenter": "01"
         }
      },
      "device-type": "APPLIANCE",
      "display-name": "MyApplianceImportJob",
      "freeform-tags": {},
      "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
      "label": "JAKQVAGJF",
      "lifecycle-state": "INITIATED",
      "upload-bucket-name": "MyBucket1"
   },
   "etag": "2--gzip"
}
```

**Freeform Tags**

To specify freeform tags when creating a job:

```bash
oci dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type appliance --freeform-tags '{ "<tag_key>": "<value>" }'
```

For example:

```bash
oci dts job create --bucket MyBucket1 --compartment-id ocid.compartment.oc1..exampleuniqueID --display-name MyApplianceImportJob --device-type appliance --freeform-tags '{"Pittsburg_Team": "brochures"}'
```
Data Transfer

```json
{
"data": {
"attached-transfer-appliance-labels": [],
"attached-transfer-device-labels": [],
"attached-transfer-package-labels": [],
"compartment-id": "ocid.compartment.oc1..exampleuniqueID",
"creation-time": "2019-12-18T19:43:58+00:00",
"defined-tags": {},
"device-type": "APPLIANCE",
"display-name": "MyApplianceImportJob",
"freeform-tags": {
"Pittsburg_Team": "brochures"
},
"id": "ocid1.datatransferjob.oc1..exampleuniqueID",
"label": "JAKQVAGJF",
"lifecycle-state": "INITIATED",
"upload-bucket-name": "MyBucket1"
},
"etag": "2--gzip"
}
```

**Note:**

Users create tag namespaces and tag keys with the required permissions. These items must exist before you can specify them when creating a job. See [Working with Defined Tags](#) on page 3914 for details.

### Multiple Tags

To specify multiple tags, comma separate the JSON-formatted key/value pairs:

```
oci dts job create --bucket <bucket> --compartment-id <compartment_id> --display-name <display_name> --device-type appliance --freeform-tags "{"<tag_key>"":<value>" },{ "<tag_key>"":<value>" }
```

### Notifications

To include notifications, include the `--setup-notifications` option. See [Setting Up Transfer Job Notifications from the CLI](#) on page 1029 for more information on this feature.

### Listing Transfer Jobs

To display the list of transfer jobs using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list. The transfer jobs in that compartment are displayed.

To display the list of transfer jobs using the CLI

```
oci dts job list --compartment-id <compartment_id>
```

For example:

```
oci dts job list --compartment-id ocid.compartment.oc1..exampleuniqueID

```

Oracle Cloud Infrastructure User Guide 1062
When you use the CLI to list jobs, tagging details are also included in the output if you specified tags.

**Displaying Transfer Job Details**

To display the details of a transfer job using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list.

   The transfer jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the transfer job whose details you want to view.

   Alternatively, you can click the **Actions** icon (⋮), and then click **View Details**.

The Details page for that transfer job appears.

To display the details of a transfer job using the CLI

```
oci dts job show --job-id <job_id>
```

For example:

```
oci dts job show --job-id ocid1.datatransferjob.oc1..exampleuniqueID
```

```json
{
  "data": {
    "attached-transfer-appliance-labels": [],
    "attached-transfer-device-labels": [],
    "attached-transfer-package-labels": [],
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2019-12-18T19:43:58+00:00",
    "defined-tags": {},
    "device-type": "APPLIANCE",
    "display-name": "MyApplianceImportJob",
    "freeform-tags": {},
    "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
    "label": "JAKQVAGJF",
    "lifecycle-state": "INITIATED",
    "upload-bucket-name": "MyBucket1"
  },
  "etag": "2--gzip"
}
```
When you use the CLI command to display the details of a job, tagging details are also included in the output if you specified tags.

**Editing Transfer Jobs**

To edit the name of a transfer job using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list.
   The transfer jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the transfer job whose name you want to edit.
   The Details page for that transfer job appears.

   Alternatively, you can click the **Actions** icon (⋮), and then click **View Details**.
4. Click **Edit** in the Details page.
   The Edit Transfer Job dialog appears.
5. Edit the name of the transfer job. Avoid entering confidential information.
6. Click **Edit Transfer Job**.
   You are returned to the Details page for that transfer job.

To edit the name of a transfer job using the CLI

```
oci dts job update --job-id <job_id> --display-name <display_name>
```

<display_name> is the new name of the transfer job. Avoid entering confidential information.

For example:

```
oci dts job update --job-id ocid1.datatransferjob.oc1..exampleuniqueID --display-name MyRenamedJob
```

```
{
   "data": {
      "attached-transfer-appliance-labels": [],
      "attached-transfer-device-labels": [],
      "attached-transfer-package-labels": [],
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "creation-time": "2019-12-18T19:43:58+00:00",
      "defined-tags": {},
      "device-type": "APPLIANCE",
      "display-name": "MyRenamedJob",
      "freeform-tags": {},
      "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
      "label": "JAKQVAGJE",
      "lifecycle-state": "INITIATED",
      "upload-bucket-name": "MyBucket1"
   },
   "etag": "3"
}
```

**Editing Transfer Job Tags**

To edit the tags associated with a transfer job using the CLI

The CLI command replaces any existing tags with the new key/value pairs you specify. For more information about tagging, see **Resource Tags** on page 211.
To edit defined tags, provide the replacement key value pairs:

```bash
oci dts job update --job-id <job_id> --defined-tags '{ "<tag_namespace>": {
  "<tag_key>": "<value>"
}}'
```

For example:

```bash
oci dts job update --job-id ocid1.datatransferjob.oc1..exampleuniqueID --
defined-tags '{"Operations": {"CostCenter": "42"}}'
```

```json
{
  "data": {
    "attached-transfer-appliance-labels": [],
    "attached-transfer-device-labels": [],
    "attached-transfer-package-labels": [],
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2019-12-18T19:43:58+00:00",
    "defined-tags": {
      "operations": {
        "costcenter": "42"
      }
    },
    "device-type": "APPLIANCE",
    "display-name": "MyApplianceImportJob",
    "freeform-tags": {},
    "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
    "label": "JAKQVAGJF",
    "lifecycle-state": "INITIATED",
    "upload-bucket-name": "MyBucket1"
  },
  "etag": "2--gzip"
}
```

To edit free-form tags, provide the replacement key/value pairs:

```bash
oci dts job update --job-id <job_id> --freeform-tags
'{ "<tag_key>": "<value>" }'
```

For example:

```bash
oci dts job update --job-id ocid1.datatransferjob.oc1..exampleuniqueID --
freeform-tags '{"Chicago_Team":"marketing_videos"}'
```

```json
{
  "data": {
    "attached-transfer-appliance-labels": [],
    "attached-transfer-device-labels": [],
    "attached-transfer-package-labels": [],
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2019-12-18T19:43:58+00:00",
    "defined-tags": {},
    "device-type": "APPLIANCE",
    "display-name": "MyApplianceImportJob",
    "freeform-tags": {
      "Chicago_Team": "marketing_videos"
    },
    "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
    "label": "JAKQVAGJF",
    "lifecycle-state": "INITIATED",
    "upload-bucket-name": "MyBucket1"
  },
  "etag": "2--gzip"
}
```
### Deleting Transfer Job Tags

To delete the tags associated with a transfer job using the CLI

The CLI command replaces any existing tags with the new key/value pairs you specify. If you want to delete some of the tags, specify a new tag string that does not contain the unwanted key/value pairs.

To delete all free-form tags:

```
oci dts job update --job-id <job_id> --freeform-tags '{}'
```

To delete all defined tags:

```
oci dts job update --job-id <job_id> --defined-tags '{}'
```

### Moving Transfer Jobs Between Compartments

#### To move transfer job to a different compartment using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list.
   
   The transfer jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the transfer job that you want to move.
   
   The Details page for that transfer job appears.

   Alternatively, you can click the **Actions** icon (⋮), and then click **Move Resource**.
4. Click **Move Resource** in the Details page.
   
   The Move Resource to a Different Compartment dialog appears.
5. Choose the compartment you want to which you want to move the transfer job from the list.
6. Click **Move Resource**.

   You are returned to the Details page for that transfer job.

#### To move a transfer job to a different compartment using the CLI

```
oci dts job move --job-id <job_id> compartment-id <compartment_id> <options>
```

<compartment_id> is the compartment to which the data transfer job is being moved.

<options> are:

- **--if-match**: The tag that must be matched for the task to occur for that entity. If set, the update is only successful if the object's tag matches the tag specified in the request.
- **--from-json**: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The **--generate-full-command-json-input** option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id -> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions.

For example:

```
oci dts job move --job-id ocid1.datatransferjob.oc1..exampleuniqueID compartment-id ocid.compartment.oc1..exampleuniqueID
```
To confirm the transfer, display the list of transfer jobs in the new compartment. See Listing Transfer Jobs on page 1062 for more information.

**Verifying Upload User Credentials**

*Note:* You can only use the CLI command to verify upload user credentials.

You can verify the current upload user credentials to see whether there are any problems or updates required. If any configuration file is incorrect or invalid, the upload fails.

To verify the upload user credentials using the CLI:

```bash
oci dts job verify-upload-user-credentials --bucket <bucket>
```

*bucket* is the upload bucket for the transfer job.

For example:

```bash
oci dts job verify-upload-user-credentials --bucket MyBucket1
```

created object BulkDataTransferTestObject in bucket MyBucket1
overwrote object BulkDataTransferTestObject in bucket MyBucket1
inspected object BulkDataTransferTestObject in bucket MyBucket1
read object BulkDataTransferTestObject in bucket MyBucket1

Depending on your user configuration, you may get an error message returned similar to the following:

```bash
WARNING: Permissions on /home/user/.oci/config_upload_user are too open.
To fix this please try executing the following command:
ocli setup repair-file-permissions --file /home/user/.oci/config_upload_user
Alternatively to hide this warning, you may set the environment variable,
OCI_CLI_SUPPRESS_FILE_PERMISSIONS_WARNING:
export OCI_CLI_SUPPRESS_FILE_PERMISSIONS_WARNING=True
```

ERROR: The config file at /home/user/.oci/config_upload_user is invalid:

```
+Config Errors+--------------+
| Key                | Error       | Hint |
+--------------------+-------------+------+
| fingerprint         | malformed   | openssl rsa -pubout -outform DER -in path to your private key | openssl md5 -c |
```

If a user credential issue is identified, fix it and rerun the `verify-upload-user-credentials` CLI to ensure that all problems are addressed. Then you can proceed with transfer job activities.

**Deleting Transfer Jobs**

You can delete transfer jobs when they are in the Initiated, Preparing, and Close states.

To delete a transfer job using the Console:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.
2. Select the **Compartment** from the list.
   
   The transfer jobs in that compartment are displayed.

3. Find the data transfer job that you want to delete.

4. Click the **Actions** icon (\(\text{\text{\textsuperscript{}}\text{\text{\textsuperscript{}}}}\)), and then click **Delete**.

   Alternatively, you can delete a transfer job from the **View Details** page.

5. Confirm the deletion when prompted.

To delete a transfer job using the CLI

```
oci dts job delete --job-id <job_id>
```

For example:

```
oci dts job delete --job-id ocid1.datatransferjob.oc1..exampleuniqueID
```

Confirm the deletion when prompted. The transfer job is deleted with no further action or return. To confirm the deletion, display the list of transfer jobs in the compartment. See **Listing Transfer Jobs** on page 1062 for more information.

**Closing Transfer Jobs**

Typically, you would close a transfer job when no further transfer job activity is required or possible. Closing a transfer job requires that the status of all associated transfer packages be returned, canceled, or deleted. In addition, the status of all associated transfer disks must be complete, in error, missing, canceled, or deleted.

When you close the transfer job, the status changes to **Closed**.

To close a transfer job using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.

2. Select the **Compartment** from the list.

   The transfer jobs in that compartment are displayed.

3. Find the data transfer package for which you want to display the details.

4. Click the **Actions** icon (\(\text{\text{\textsuperscript{}}\text{\text{\textsuperscript{}}}}\)), and then click **View Details**.

   Alternatively, click the hyperlinked name of the transfer job.

5. Click **Close Transfer Job**.

To close a transfer job using the CLI

```
oci dts job close --job-id <job_id>
```

For example:

```
oci dts job close --job-id ocid1.datatransferjob.oc1..exampleuniqueID
```

```json
{
  "data": {
    "attached-transfer-appliance-labels": [],
    "attached-transfer-device-labels": [],
    "attached-transfer-package-labels": [],
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2020-05-20T22:00:43+00:00",
    "defined-tags": {},
    "device-type": "APPLIANCE",
    "display-name": "MyApplianceImportJob",
    "freeform-tags": {},
    "id": "ocid1.datatransferjob.oc1..exampleuniqueID",
  }
}```
Data Transfer

"label": "JGX4N1XLI",
"lifecycle-state": "CLOSED",
"upload-bucket-name": "MyBucket"
},
"etag": "1"
}

Import Appliances

This section describes tasks associated with the Oracle-provided import appliance.

**Requesting Appliances**

**Tip:**

To save time, identify the data you intend to upload and make data copy preparations before requesting the import appliance.

Creating an import appliance request returns an Oracle-assigned appliance label. For example:

XAKWEGKZ5T

To request an appliance using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.

   Choose the transfer job for which you want to request an import appliance.

2. Under **Transfer Appliances**, click **Request Transfer Appliance**.

   The Request Transfer Appliance dialog appears.

3. Enter the shipping address details where you want the import appliance sent.

   - **Company Name**: Required. Specify the name of the company that owns the data being migrated to Oracle Cloud Infrastructure.
   - **Recipient Name**: Required. Specify the name of the recipient who receives the import appliance.
   - **Recipient Phone Number**: Required. Specify the recipient's phone number.
   - **Recipient Email Address**: Required. Specify the recipient's email address.
   - **Care Of**: Optional intermediary party responsible for transferring the import appliance shipment from the delivery vendor to the intended recipient.
   - **Address Line 1**: Required. Specify the street address where the import appliance is being sent.
   - **Address Line 2**: Optional identifying address details like building, suite, unit, or floor information.
   - **City/Locality**: Required. Specify the city or locality.
   - **State/Province/Region**: Required. Specify the state, province, or region.
   - **Zip/Postal Code**: Specify the zip code or postal code.
   - **Country**: Required. Select the country.

4. Click **Request Transfer Appliance**.

To request an appliance using the CLIs

```bash
oci dts appliance request --job-id <job_id> --addressee <addressee> 
--care-of <care_of> --address1 <address_line1> --city-or-
locality <city_or_locality> --state-province-region <state_province_region>
--country <country> --zip-postal-code <zip_postal_code> --phone-
number <phone_number> --email <email> <options>
```

<options> are:

- **--address2**: Optional address of the addressee (line 2).
- **--address3**: Optional address of the addressee (line 3).
- **--address4**: Optional address of the addressee (line 4).
--from-json: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The --generate-full-command-json-input option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions.

For example:

```bash
oci dts appliance request --job-id ocid1.datatransferjob.oc1..exampleuniqueID --addressee MyCompany --care-of "John Doe" --address1 "123 Main Street" --city-or-locality Anytown --state-province-region NY --country USA --zip-postal-code 12345 --phone-number 8005551212 --email john.doe@mycompany.com

{
  "data": {
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "creation-time": "2020-05-20T22:08:13+00:00",
    "customer-received-time": null,
    "customer-returned-time": null,
    "customer-shipping-address": {
      "address1": "123 Main Street",
      "address2": null,
      "address3": null,
      "address4": null,
      "addressee": "MyCompany",
      "care-of": "John Doe",
      "city-or-locality": "Anytown",
      "country": "USA",
      "email": "john.doe@mycompany.com",
      "phone-number": "3115551212",
      "state-or-region": "NY",
      "zipcode": "12345"
    },
    "delivery-security-tie-id": null,
    "label": "XAKWEGKZ5T",
    "lifecycle-state": "REQUESTED",
    "next-billing-time": null,
    "return-security-tie-id": null,
    "serial-number": null,
    "transfer-job-id": "ocid1.datatransferjob.oc1..exampleuniqueID",
    "upload-status-log-uri": "JAKQVAGJF/XAKWEGKZ5T/upload_summary.txt"
  }
}
```

When you submit an appliance request, Oracle generates a unique label (label": "XAKWEGKZ5T") to identify the import appliance and your request is sent to Oracle for approval and processing.

**Monitoring the Appliance Request Status**

The time it takes to approve, prepare, and ship your appliance request varies and depends on various factors, including current available inventory. Oracle provides status updates daily throughout the appliance request and ship process.

To monitor the status of your appliance request using the Console
1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Imports**.

2. Select the **Compartment** from the list. The transfer jobs in that compartment are displayed.

3. Find and select the transfer job for which you want to monitor associated appliance requests.

4. Under **Transfer Appliances**, find the appliance label Oracle assigned to your appliance request and look at the **Status** field.

Here are the key status values to look for when monitoring your appliance request:

- **Requested**: You successfully completed your request for an import appliance. The status displays **Requested** until Oracle approves your appliance request.
- **Rejected**: Oracle denied your appliance request.

**Important:** If your appliance request is denied and you have questions, contact your Sales Representative or file a Service Request (SR).

- **Oracle Preparing**: Oracle approved your appliance request. The status displays **Oracle Preparing** until the import appliance is shipped to you.

- **Shipping**: Oracle completed the necessary preparations and shipped your import appliance. When the import appliance is shipped, Oracle provides the serial number of the import appliance, the shipping vendor, and the tracking number in the **Transfer Appliance Details**. The status displays **Shipping** until the import appliance is delivered to you.

- **Delivered**: The shipping vendor delivered your import appliance. When the import appliance is delivered, Oracle provides the date and time the import appliance was received in the **Transfer Appliance Details**. The status displays **Delivered**.

To monitor the status of your appliance request using the CLI:

```
oci dts appliance show --job-id <job_id> --appliance-label <appliance label>
```

For example:

```
oci dts appliance show --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

```
{
    "data": {
        "appliance-delivery-tracking-number": null,
        "appliance-delivery-vendor": null,
        "appliance-return-delivery-tracking-number": null,
        "creation-time": "2020-05-20T22:08:13+00:00",
        "customer-received-time": null,
        "customer-returned-time": null,
        "customer-shipping-address": {
            "address1": "123 Main Street",
            "address2": null,
            "address3": null,
            "address4": null,
            "addressee": "MyCompany",
            "care-of": "John Doe",
            "city-or-locality": "Anytown",
            "country": "USA",
            "email": "john.doe@mycompany.com",
            "phone-number": "3115551212",
            "state-or-region": "NY",
            "zipcode": "12345"
        },
        "delivery-security-tie-id": null,
```

Oracle Cloud Infrastructure User Guide 1071
The request status is displayed as the value for lifecycle-state.

### Displaying the List of Appliances

To display the list of appliances using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Select the Compartment from the list.

   The transfer jobs in that compartment are displayed.
3. Choose the transfer job for which you want to display the list of associated import appliances.

   The list of import appliances is displayed below the transfer job details.

To display the list of appliances using the CLI

```bash
oci dts appliance list --job-id <job_id>
```

For example:

```json
oci dts appliance list --job-id ocid1.datatransferjob.oc1..exampleuniqueID
{
  "data": {
    "transfer-appliance-objects": [
      {
        "creation-time": "2020-05-20T22:08:13+00:00",
        "label": "XAKWEGKZ5T",
        "lifecycle-state": "PROCESSING",
        "serial-number": null
      }
    ]
  }
}
```

### Displaying Appliance Details

To display the details of an appliance using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Select the Compartment from the list.

   The transfer jobs in that compartment are displayed.
3. Find the transfer job for which you want to display the details of an associated import appliance.

   The list of appliances is displayed below the transfer job details.
4. Find the import appliance for which you want to display the details.
5. Click the Actions icon (giene), and then click View Details.

To display the details of an appliance using the CLI

```bash
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```
For example:

```
oci dts appliance show --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

```
{
  "data": {
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "creation-time": "2020-05-20T22:08:13+00:00",
    "customer-received-time": null,
    "customer-returned-time": null,
    "customer-shipping-address": {
      "address1": "123 Main Street",
      "address2": null,
      "address3": null,
      "address4": null,
      "addressee": "MyCompany",
      "care-of": "John Doe",
      "city-or-locality": "Anytown",
      "country": "USA",
      "email": "john.doe@mycompany.com",
      "phone-number": "3115551212",
      "state-or-region": "NY",
      "zipcode": "12345"
    },
    "delivery-security-tie-id": "exampleuniqueID",
    "label": "XAKWEGKZ5T",
    "lifecycle-state": "PROCESSING",
    "next-billing-time": null,
    "return-security-tie-id": "exampleuniqueID",
    "serial-number": "exampleuniqueserialnumber",
    "transfer-job-id": "ocid1.datatransferjob.oc1..exampleuniqueID",
    "upload-status-log-uri": "JAKQVAGJF/XAKWEGKZ5T/upload_summary.txt"
  }
}
```

**Editing the Appliance Request Shipping Information**

You can only edit the shipping information when the status is **Requested**.

To edit the appliance request shipping information using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the **Requested** import appliance that you want to edit the shipping information.
3. Click the Actions icon (†), and then click Edit.
4. Edit the shipping information for the import appliance.
5. Click Save.

To edit the appliance request shipping information using the CLI

```
oci dts appliance update-shipping-address --job-id <job_id> --appliance-label <appliance_label> --addressee <addressee> <changed_fields>
```

Include the addressee field even if it has not changed.
Data Transfer

<changed_fields> represents one or more of the following shipping address fields that you want to update:

--care-of <care_of> --address1 <address> --city <city> --state <addressee> --zip <zip> --country <country> --phone-number <phone_number> email <email>

You only need to include those fields that are being updated. For example:

oci dts appliance update-shipping-address --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T --addressee MyCompany --care-of "Richard Roe" --phone-number 3115559876 --email richard.roe@mycompany.com

Confirm the update of the appliance request shipping information when prompted. The appliance details are displayed with the updated information.

```
{
  "data": {
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "creation-time": "2020-05-20T22:08:13+00:00",
    "customer-received-time": null,
    "customer-returned-time": null,
    "customer-shipping-address": {
      "address1": "123 Main Street",
      "address2": null,
      "address3": null,
      "address4": null,
      "addressee": "MyCompany",
      "care-of": "Richard Roe",
      "city-or-locality": "Anytown",
      "country": "USA",
      "email": "john.doe@oracle.com",
      "phone-number": "3115559876",
      "state-or-region": "NY",
      "zipcode": "12345"
    },
    "delivery-security-tie-id": null,
    "label": "XAKWEGKZ5T",
    "lifecycle-state": "REQUESTED",
    "next-billing-time": null,
    "return-security-tie-id": null,
    "serial-number": null,
    "transfer-job-id": "ocid1.datatransferjob.oct1..exampleuniqueID",
    "upload-status-log-uri": "JAKQVAGJF/XAKWEGKZ5T/upload_summary.txt"
  }
}
```

Deleting an Appliance Request

You can delete an appliance request before Oracle approves the request—the status must be Requested. For example, you initiated the transfer by creating a transfer job and requested an appliance, but changed your mind.

To delete an appliance request using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Imports.
2. Find the data transfer job and appliance request that you want to delete.
3. Click the Actions icon ( ), and then click Delete.

Alternatively, you can delete an appliance request from the Transfer Appliance Details page.
4. Confirm the deletion when prompted.

To delete an appliance request using the CLI

```
oci dts appliance delete --job-id <job_id> --appliance-label <appliance_label>
```

For example:

```
oci dts appliance delete --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

Confirm the deletion when prompted.

**Displaying Registered Appliances**

You can display a list of all appliances registered through the initialize authentication command. See Initializing Authentication to the Import Appliance on page 1044 for more information.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can only use the CLI command to display a list of all appliances registered through the initialize authentication command.</td>
</tr>
</tbody>
</table>

To display the list of all registered appliances using the CLI

```
oci dts physical-appliance list
```

For example:

```
oci dts physical-appliance list
```

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Unregistering Appliances**

You can unregister an appliance previously registered through the initialize authentication command. See Initializing Authentication to the Import Appliance on page 1044 for more information.

To unregister an appliance using the CLI

```
oci dts physical-appliance unregister
```

**Configuring Import Appliance Encryption**

Configure the import appliance to use encryption. Oracle Cloud Infrastructure creates a strong passphrase for each appliance. The command securely collects the strong passphrase from Oracle Cloud Infrastructure and sends that passphrase to the Data Transfer service.

If your environment requires Internet-aware applications to use network proxies, ensure that you set up the required Linux environment variables. See for more information.
Important:

If you are working with multiple appliances at the same time, be sure the job ID and appliance label you specify in this step matches the physical appliance you are currently working with. You can get the serial number associated with the job ID and appliance label using the Console or the Oracle Cloud Infrastructure CLI. You can find the serial number of the physical appliance on the back of the device on the agency label.

Note:

You can only use the Oracle Cloud Infrastructure CLI to configure encryption.

Configuring Appliance Encryption

Note:

You can only use the CLI command to configure encryption for appliances.

To configure appliance encryption using the CLI

At the command prompt on the host, run `oci dts physical-appliance configure-encryption` to configure import appliance encryption.

```bash
oci dts physical-appliance configure-encryption --job-id <job_id> --appliance-label <appliance_label>
```

For example:

```bash
oci dts physical-appliance configure-encryption --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

Moving the state of the appliance to preparing...
Passphrase being retrieved...
Configuring encryption...
Encryption configured. Getting physical transfer appliance info...
{
    "data": {
        "availableSpaceInBytes": "Unknown",
        "encryptionConfigured": true,
        "finalizeStatus": "NA",
        "lockStatus": "LOCKED",
        "totalSpaceInBytes": "Unknown"
    }
}

Initializing Authentication to the Appliance

Note:

You can only use the Oracle Cloud Infrastructure CLI to initialize authentication.

Initialize authentication to allow the host machine to communicate with the import appliance. Use the values returned from the Configure Networking command. See Configuring the Transfer Appliance Networking for details.

Initializing Authentication

Note:

You can only use the CLI command to initialize authentication for appliances.
To initialize authentication using the CLI

```bash
oci dts physical-appliance initialize-authentication --job-id <job-id> --appliance-cert-fingerprint <fingerprint> --appliance-ip <ip_address> --appliance-label <appliance-label>
```

For example:

```bash
```

Retrieving the Appliance serial id from Oracle Cloud Infrastructure

Access token:

Registering and initializing the authentication between the CLI and the appliance

```json
{
  "data": {
    "availableSpaceInBytes": "Unknown",
    "encryptionConfigured": false,
    "finalizeStatus": "NA",
    "lockStatus": "NA",
    "totalSpaceInBytes": "Unknown"
  }
}
```

When prompted, supply the access token and system. The Control Host can now communicate with the import appliance.

**Datasets**

A dataset is a collection of files that are treated similarly. You can write up to 100 million files onto the appliance for import. We currently support one dataset per appliance.

**Note:**

You can only use the CLI to run dataset tasks.

**Creating the Dataset**

Appliance data transfer supports NFS version 3, 4, and 4.1 to write data to the import appliance. In preparation for writing data, create and configure a dataset to write to.

To create a dataset using the CLI

```bash
oci dts nfs-dataset create --name <dataset_name>
```

For example:

```bash
oci dts nfs-dataset create --name nfs-ds-1
```

Creating dataset with NFS export details nfs-ds-1

```json
{
  "data": {
    "datasetType": "NFS",
    "name": "nfs-ds-1",
    "nfsExportDetails": {
      "exportConfigs": null
    },
    "state": "INITIALIZED"
  }
}
```
**Activating the Dataset**

Activation creates the NFS export, making the dataset accessible to NFS clients.

To activate the dataset using the CLI

```
oci dts nfs-dataset activate --name <dataset_name>
```

For example:

```
oci dts nfs-dataset activate --name nfs-ds-1
```

Fetching all the datasets
Activating dataset small-files
Dataset nfs-ds-1 activated

**Configuring Export Settings on the Dataset**

To configure export settings on a dataset using the CLI

```
oci dts nfs-dataset set-export --name <dataset_name> --rw true --world true
```

For example:

```
oci dts nfs-dataset set-export --name nfs-ds-1 --rw true --world true
```

Settings NFS exports to dataset nfs-ds-1

```
{
  "data": {
    "datasetType": "NFS",
    "name": "nfs-ds-1",
    "nfsExportDetails": {
      "exportConfigs": [
        {
          "hostname": null,
          "ipAddress": null,
          "readWrite": true,
          "subnetMaskLength": null,
          "world": true
        }
      ],
      "state": "INITIALIZED"
    }
  }
}
```

Here is another example of creating the export to give read/write access to a subnet:

```
oci dts nfs-dataset set-export --name nfs-ds-1 --ip 10.0.0.0 --subnet-mask-length 24 --rw true --world false
```

Settings NFS exports to dataset nfs-ds-1

```
{
  "data": {
    "datasetType": "NFS",
    "name": "nfs-ds-1",
    "nfsExportDetails": {
      "exportConfigs": [
        {
          "hostname": null,
          "ipAddress": "10.0.0.0",
          "readWrite": true,
          "subnetMaskLength": "24",
          "world": true
        }
      ],
      "state": "INITIALIZED"
    }
  }
}
```
Deactivating the Dataset

**Note:**

Deactivating the dataset is only required if you are running appliance commands using the Data Transfer Utility. If you are using the Oracle Cloud Infrastructure CLI to run your Appliance-Based Data Import, you can skip this step and proceed to Sealing the Dataset on page 1079.

After you are done writing data, deactivate the dataset. Deactivation removes the NFS export on the dataset, disallowing any further writes.

To deactivate the dataset using the CLI

```
dts nfs-dataset deactivate --name <dataset_name>
```

For example:

```
dts nfs-dataset deactivate --name nfs-ds-1
```

Sealing the Dataset

Sealing a dataset stops all writes to the dataset. This process can take some time to complete, depending upon the number of files and total amount of data copied to the import appliance.

If you issue the `seal` command without the `--wait` option, the seal operation is triggered and runs in the background. You are returned to the command prompt and can use the `seal-status` command to monitor the sealing status. Running the `seal` command with the `--wait` option results in the seal operation being triggered and continues to provide status updates until sealing completion.

**Important:**

You can only copy regular files to transfer appliances. Special files (for example, symbolic links, device special, sockets, and pipes) cannot be copied directly. To transfer special files, create a tar archive of these files and copy the tar archive to the transfer appliance.

The sealing operation generates a manifest across all files in the dataset. The manifest contains an index of the copied files and generated data integrity hashes.

To seal the dataset using the CLI

```
oci dts nfs-dataset seal --name <dataset_name> [--wait]
```

For example:

```
oci dts nfs-dataset seal --name nfs-ds-1
```

Seal initiated. Please use seal-status command to get progress.

Monitoring the Dataset Sealing Process

To monitor the dataset sealing process using the CLI

```
oci dts nfs-dataset seal-status --name <dataset_name>
```
For example:

```
oci dts nfs-dataset seal-status --name nfs-ds-1
{
  "data": {
    "bytesProcessed": 2803515612507,
    "bytesToProcess": 2803515612507,
    "completed": true,
    "endTimeInMs": 1591990408804,
    "failureReason": null,
    "numFilesProcessed": 182,
    "numFilesToProcess": 182,
    "startTimeInMs": 1591987136180,
    "success": true
  }
}
```

### Downloading the Dataset Seal Manifest

After sealing the dataset, you can optionally download the dataset’s seal manifest to a user-specified location. The manifest file contains the checksum details of all the files. The transfer site uploader consults the manifest file to determine the list of files to upload to object storage. For every uploaded file, it validates that the checksum reported by object storage matches the checksum in manifest. This validation ensures that no files got corrupted in transit.

To download the dataset seal manifest file using the CLI

```
oci dts nfs-dataset get-seal-manifest --name <dataset_name> --output-file <file_path>
```

For example:

```
oci dts nfs-dataset get-seal-manifest --name nfs-ds-1 --output-file ~/Downloads/seal-manifest
```

### Reopening a Dataset

If changes are necessary after sealing a dataset or finalizing an import appliance, you must reopen the dataset to modify the contents. Make the required changes and again seal the dataset. Resealing the dataset generates a new manifest.

**Note:**

If an import appliance is rebooted or power cycled, follow the instructions in this topic to reopen the dataset.

### Step 1: Unlocking the Appliance

You must unlock the appliance before you can write data to it. Unlocking the appliance requires the strong passphrase that is created by Oracle Cloud Infrastructure for each appliance. Unlocking can be accomplished in two different ways:

- If you provide the `--job-id` and `--appliance-label` when running the `unlock` command, the data transfer system retrieves the passphrase from Oracle Cloud Infrastructure and sends it to the appliance during the unlock operation.
- You can query Oracle Cloud Infrastructure for the passphrase and provide that passphrase when prompted during the unlock operation.

To unlock the appliance and send the passphrase to the appliance

```
oci dts physical-appliance unlock --job-id <job_id> --appliance-label <label>
```
For example:

```
oci dts physical-appliance unlock --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
```

Retrieving the passphrase from Oracle Cloud Infrastructure

```
{
  "data": {
    "availableSpaceInBytes": "64.00GB",
    "encryptionConfigured": true,
    "finalizeStatus": "NOT_FINALIZED",
    "lockStatus": "NOT_LOCKED",
    "totalSpaceInBytes": "64.00GB"
  }
}
```

To query Oracle Cloud Infrastructure for the passphrase to provide to unlock the appliance

```
oci dts appliance get-passphrase --job-id <job_id> --appliance-label <label>
```

For example:

```
oci dts appliance get-passphrase --job-id ocid1.datatransferjob.oc1..exampleuniqueID --appliance-label XAKWEGKZ5T
{
  "data": {
    "encryption-passphrase": "passphrase"
  }
}
```

Then, run `dts physical-appliance unlock` without `--job-id` and `--appliance-label` and supply the passphrase when prompted.

```
oci dts physical-appliance unlock
```

Step 2: Reopening the Appliance

Reopen the dataset to write data to the import appliance again.

To reopen an NFS dataset

```
oci dts nfs-dataset reopen --name <dataset_name>
```

Step 3: Repeat Steps to Write Data to the Appliance

Repeat the same tasks you performed when you originally wrote data to the import appliance beginning with activating the dataset in the Copying Files to the NFS Share on page 1049 section.

Displaying the List of Datasets

To display the list of datasets using the CLI

```
oci dts nfs-dataset list
```

For example:

```
oci dts nfs-dataset list
```

Listing NFS datasets

```
{
  "data": [
  {
    "datasetType": "NFS",
```
"name": "nfs-ds-1",
"nfsExportDetails": {
  "exportConfigs": [
    {
      "hostname": null,
      "ipAddress": null,
      "readWrite": true,
      "subnetMaskLength": null,
      "world": true
    }
  ],
  "state": "ACTIVE"
}

Displaying Dataset Details
To display the details of a transfer job using the CLI

oci dts nfs-dataset show --name <dataset_name>

For example:

oci dts nfs-dataset show --name MyDataset

{
  "data": {
    "datasetType": "NFS",
    "name": "nfs-ds-1",
    "nfsExportDetails": {
      "exportConfigs": [
        {
          "hostname": null,
          "ipAddress": null,
          "readWrite": true,
          "subnetMaskLength": null,
          "world": true
        }
      ],
      "state": "ACTIVE"
    }
  }
}

Deleting a Dataset
To delete a dataset using the CLI

oci dts nfs-dataset delete --name <dataset_name>

For example:

oci dts nfs-dataset delete --name nfs-ds-1

Confirm the deletion when prompted. The dataset is deleted with no further action or return. To confirm the deletion, display the list of datasets. See Displaying the List of Datasets on page 1081 for more information.

Appliance Data Export

Data Export is Oracle's offline data export solution that lets you migrate petabyte-scale datasets from your Oracle Cloud Infrastructure Object Storage bucket to your data center using an Oracle-provided Data Transfer Appliance.
Use Data Export when you have stored terabytes or petabytes of data in Oracle Cloud Infrastructure and need to retrieve it from Object Storage more quickly than using the public internet. For example, you may have media content or processed datasets you need to share with a customer or business partner.

You cannot export data from multiple Object Storage buckets to the same export job. If you want to export data from more than one bucket, you must create an export job for each of the buckets.

**Note:**

Data Export does not support exporting files from an Archive Storage bucket. Move your data from the Archive Storage bucket to an Object Storage bucket and then create an export job specifying the Object Storage bucket. See Overview of Archive Storage on page 484 for more information.

**Note:**

Data Export is not available for free trial or Pay As You Go accounts.

**Data Export Concepts**

**EXPORT JOB**

An export job is the logical representation of an offline export of data from your Oracle Cloud Infrastructure Object Storage bucket to your data center. Exporting your data does not remove it from the original storage bucket on Oracle Cloud Infrastructure.

**Note:**

An export job is associated with a single export appliance. If your data export needs exceed the capacity of the appliance (150 TB), you need to create additional export jobs with their own dedicated appliances.

**DATA TRANSFER APPLIANCE**

The Data Transfer Appliance (export appliance) is a high-storage capacity device used to export data from Oracle Cloud Infrastructure to your data center. You request an export appliance from Oracle, specify the data files to be copied from your Object Storage bucket to the export appliance, and then have the export appliance containing the data shipped to you. After you receive the export appliance, copy your data to your data center. When you complete the copying of data, completely delete all the data from the export appliance before sending it back to Oracle.

**COMMAND LINE INTERFACE**

The command line interface (CLI) is a small footprint tool that you can use on its own or with the Console to complete Oracle Cloud Infrastructure tasks, including Appliance-Based Data Import jobs. See Command Line Interface (CLI) on page 4192 for more information.

**Note:**

You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

**HOST**

A physical computer at the customer site on which one or more of the logical hosts (Control, Data, Terminal Emulation) is running. Depending on your computing environment, you can have any of the following:

- A separate physical host for each logical host
- All three logical hosts consolidated onto a single physical host
- Two logical hosts on one physical host and the third logical host on a separate physical host
All physical hosts must be on the network used for the data transfer.

**CONTROL HOST**

The logical representation of the host computer at your site from which you perform data export tasks. Depending on your needs, you may use one or more separate hosts (Control and Data) to configure your export job.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can only run Oracle Cloud Infrastructure CLI commands from a Linux-based Control Host machine. You can run Console tasks from a browser running on a Windows machine.</td>
</tr>
</tbody>
</table>

**DATA HOST**

The logical representation of the host computer on your site that receives the data exported from Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only Linux machines can be used as Data Hosts.</td>
</tr>
</tbody>
</table>

**TERMINAL EMULATION HOST**

The logical representation of the host computer that uses terminal emulation software to communicate with, and allow you to command, the appliance.

**BUCKET**

The logical container in the Object Storage from where your data is copied to the appliance before it is shipped to you. A bucket is associated with a single compartment in your tenancy whose policies determine what actions a user can perform.

**APPLIANCE MANAGEMENT SERVICE**

Software running on the appliance that provides management functions. Users interact with this service through the Oracle Cloud Infrastructure CLI.

### Appliance Specifications

Use NFS versions 3, 4, or 4.1 to copy your data onto the appliance. Here are some details about the appliance:

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Capacity</td>
<td>150 TB of protected usable space</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Interfaces</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>- 10 GbE - RJ45</td>
<td></td>
</tr>
<tr>
<td>- 10 GbE - SFP+</td>
<td></td>
</tr>
<tr>
<td>You are responsible for providing all network cables. If you want to use SFP+, your transceivers must be compatible with Intel X520 NICs.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provided Cables</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>- NEMA 5–15 type B to C13</td>
<td></td>
</tr>
<tr>
<td>- C13 - 14 power</td>
<td></td>
</tr>
<tr>
<td>- USB - DB9 serial</td>
<td></td>
</tr>
</tbody>
</table>
### Environmental
- Operational temperature: 50–95°F (10–35°C)
- Operational relative humidity: 8–90% non-condensing
- Acoustics: < 75 dB @ 73°F (23°C)
- Operational altitude: -1,000 ft - 10,000 ft (approx. -300–3048 m)

### Power
- Consumption: 554 W
- Voltage: 100–240 VAC
- Frequency: 47–63 Hz
- Conversion efficiency: 89%

### Weight
- Unit: 38 lbs (approx. 17 kg)
- Unit + Transit Case: 64 lbs (approx. 29 kg)

### Height
3.5” (approx. 9 cm) (2U)

### Width
17” (approx. 43 cm)

### Depth
24” (approx. 61 cm)

### Shipping Case
11” x 25” x 28” (approx. 28 x 63.5 x 71 cm)

## Roles and Responsibilities

Depending on your organization, the responsibilities of using and managing the data transfer may span multiple roles. Use the following set of roles as a guideline for how you can assign the various tasks associated with the data export.

- **Project Sponsor:** Responsible for the overall success of the data export. Project Sponsors usually have complete access to their organization's Oracle Cloud Infrastructure tenancy. They coordinate with the other roles in the organization to complete the implementation of the data export. The Project Sponsor is also responsible for signing legal documentation and setting up notifications for the data export.

- **Infrastructure Engineer:** Responsible for integrating the export appliance into the organization's IT infrastructure where the data is being copied. Tasks associated with this role include connecting the export appliance to power, placing it within the network, and setting the IP address through a serial console menu using the provided USB-to-Serial adapter.

- **Data Administrator:** Responsible for identifying and preparing the data to be exported from Oracle Cloud Infrastructure to your data center. This person usually has access to, and expertise with, the data being exported.

These roles correspond to the various phases of the data export described in the following section. A specific role can be responsible for one or more phases.

## Task Flow for Data Export

Here is a high-level overview of the tasks involved in the data export from Oracle Cloud Infrastructure to your data center. Complete one phase before proceeding to the next one. Use the roles previously described to distribute the tasks across individuals or groups within your organization.
Secure Appliance Data Export from Oracle Cloud Infrastructure

This section highlights the security details of the data export process.

- Appliances are shipped from Oracle to you with a tamper-evident security tie on the transit case. A second tamper-evident security tie is included in the appliance transit case for you to secure the case when you ship the case back to Oracle. The number on the physical security ties must match the numbers logged by Oracle in the appliance details.
- The AES-256 encryption key is created by Oracle when the files are copied the export appliance.
- When you configure the appliance for the first time:
  - The encryption key is protected by an encryption passphrase that you must know to access the encrypted data. The system securely fetches a provided encryption passphrase from Oracle Cloud Infrastructure and registers that passphrase on the appliance.
  - All data copied to the appliance is encrypted.
  - Oracle erases all of your data from the transfer appliance after it has been returned. The erasure process follows the NIST 800-88 standards.
  - Keep possession of the security tie after you have finished unpacking and connecting the appliance. Include it when returning the appliance to Oracle. Failure to include the security tie can result in a delay in the completion of the export job.

What's Next

You are now ready to prepare the host for the data export. See Preparing for Data Export on page 1087 for more information.

Preparing for Data Export

This topic describes the tasks associated with preparing for the Data Export job. The Project Sponsor role typically performs these tasks. See Roles and Responsibilities on page 1085.

Installing and Using the Oracle Cloud Infrastructure Command Line Interface

The Oracle Cloud Infrastructure Command Line Interface (CLI) provides a set of command line-based tools for configuring and running Data Export jobs. Use the Oracle Cloud Infrastructure CLI as an alternative to running commands from the Console. Sometimes you must use the CLI to complete certain tasks as there is no Console equivalent.

Minimum Required CLI Version

The minimum CLI version required for Data Export is 2.12.1.

Determining CLI Versions

Access the following URL to see the currently available version of the CLI:
Enter the following command at the prompt to see the version of the CLI currently installed on your machine:

```bash
oci --version
```

If you have a version on your machine older than the version currently available, install the latest version.

**Note:**

Always update to the latest version of the CLI. The CLI is not updated automatically, and you can only access new or updated CLI features by installing the current version.

### Linux Operating System Requirements

See Requirements on page 4193 for a list of the Linux operating systems that support the CLI.

### Installing the CLI

Installation and configuration of the CLIs is described in detail in Command Line Interface (CLI) on page 4192.

### Using the CLI

You can specify CLI options using the following commands:

- `--option <value>`
- `--option= <value>`

The basic CLI syntax is:

```bash
oci dts <resource> <action> <options>
```

This syntax is applied to the following:

- `oci dts` is the shortened CLI command name
- `job` is an example of a `<resource>`
- `create` is an example of an `<action>`
- Other strings are `<options>`

The following command to create an export job shows a typical CLI command construct.

```bash
oci dts export create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket-name MyBucket1 --display-name MyExportJob --addressee "MyCompany Corp" --care-of "John Doe" --address1 "123 Main St." --city-or-locality Anytown --state-province-region CA --country USA --zip-postal-code 12345 --phone-number "555.555.1212" --email jdoe@mycompany.com
```

**Note:**

In the previous examples, provide a friendly name for the export job using the `##display#name` option. Avoid entering confidential information.

### Accessing Command Line Interface Help

All CLI help commands have an associated help component you can access from the command line. To view the help, enter any command followed by the `--help` or `-h` option. For example:

```bash
oci dts export --help
```
When you run the help option (\(--\text{help} \) or \(-h\)) for a specified command, all the subordinate commands and options for that level of CLI are displayed. If you want to access the CLI help for a specific subordinate command, include it in the CLI string, for example:

```
oci dts export create --help
```

NAME
dts_export_create -

DESCRIPTION
Creates a new Appliance Export Job that corresponds with customer's logical dataset

USAGE
oci dts export create [OPTIONS]

REQUIRED PARAMETERS
- --address1 [text]
  Address line 1.
- --addressee [text]
  Company or person to send the appliance to
- --bucket-name [text]
  Name of the object storage bucket for this export job
- --care-of [text]
  Place/person to direct the package to.
--city-or-locality [text]
:

**Setting Up the Oracle Cloud Infrastructure Configuration File**

Before using the command line utility, create a configuration file that contains the required credentials for working with Oracle Cloud Infrastructure. You can create this file using a setup dialog or manually using a text editor.

**Using the Setup CLI**

Run the `oci setup config` command line utility to walk through the first-time setup process. The command prompts you for the information required for the configuration file and the API public/private keys. The setup dialog generates an API key pair and creates the configuration file.

For more information about how to find the required information, see:

- [Where to Get the Tenancy's OCID and User's OCID on page 4184](#)
- [Regions and Availability Domains on page 180](#)

**Manual Setup**

If you want to set up the API public/private keys yourself and write your own config file, see [SDK and Tool Configuration](#).

**Tip:**

Use the `oci setup keys` command to generate a key pair to include in the config file.

Create the configuration file `/root/.oci/config` with the following structure:

```ini
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1
```

For example:

```ini
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1
```

For the data transfer administrator, you can create a single configuration file that contains different profile sections with the credentials for multiple users. Then use the `##profile` option to specify which profile to use in the command. Here is an example of a data transfer administrator configuration file with different profile sections:

```ini
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=4c:1a:6f:a1:5b:9e:58:45:f7:53:43:1f:51:0f:d8:45
key_file=/home/user/ocid1.user.oc1..exampleuniqueID.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-phoenix-1
```

For the data transfer administrator, you can create a single configuration file that contains different profile sections with the credentials for multiple users. Then use the `##profile` option to specify which profile to use in the command. Here is an example of a data transfer administrator configuration file with different profile sections:
By default, the DEFAULT profile is used for all CLI commands. For example:

```
oci dts export create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket-name MyBucket --display-name MyDisplay ...
```

Instead, you can issue any CLI command with the `--profile` option to specify a different data transfer administrator profile. For example:

```
oci dts export create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket-name MyBucket --display-name MyDisplay ... --profile MyProfile
```

Using the example configuration file above, the `<profile_name>` would be `profile1`.

If you created two separate configuration files, use the following command to specify the configuration file to use:

```
oci dts export create --compartment-id <compartment_id> --bucket <bucket_name> --display-name <display_name>
```

### Creating the Required IAM Policies

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization.

To use Oracle Cloud Infrastructure, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in.

You provide resource access to the data export administrators group using policies. See Managing Groups on page 2419 for more information.

Create this group using the following policies:

```
Allow group <group-name> to manage appliance-export-jobs in compartment <compartment-name>
Allow group <group-name> to manage buckets in compartment <compartment name>
Allow group <group-name> to manage objects in compartment <compartment name>
```

To enable notifications, add the following policies:

```
Allow group <group name> to manage ons-topics in tenancy
Allow group <group name> to manage ons-subscriptions in tenancy
Allow group <group name> to manage cloudevents-rules in tenancy
Allow group <group name> to inspect compartments in tenancy
```

See Getting Started with Policies on page 2135 for more information.

### Requesting Appliance Entitlement

If your tenancy is not entitled to use the Data Transfer Appliance, you must request the Data Transfer Appliance Entitlement before creating an export job.

*To request the Data Transfer Appliance Entitlement using the Console*

Open the Transfer Job page and click Request at the top. Otherwise, you are prompted to request the entitlement when attempting to create your first export job.
Once requested, the status of your request is visible at the top of the Transfer Job page. For example:

**Data Transfer Appliance Entitlement:** Granted

It can take a while to get the Data Transfer Appliance Entitlement approved. After Oracle receives your request, a Terms and Conditions Agreement is sent to the account owner via DocuSign to use the appliance. The entitlement request is approved once the signature is received. The Data Transfer Appliance Entitlement is a tenancy-wide entitlement that you need to request once for each tenancy.

**To request the Data Transfer Appliance Entitlement using the CLI**

```
oci dts appliance request-entitlement --compartment-id <compartment_id> --name <name> --email <email>
```

 `<name>` is the name of the requester.

 `<email>` is the email address of the requester.

For example:

```
oci dts appliance request-entitlement --compartment-id ocid.compartment.oc1..exampleuniqueID --name "John Doe" --email jdoe@mycompany.com
```

```
{
 "data": {
 "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
 "creation-time": "2019-12-18T18:29:15+00:00",
 "defined-tags": {},
 "display-name": null,
 "freeform-tags": {},
 "id": "ocid1.datatransferapplianceentitlement.oc1..exampleuniqueID",
 "lifecycle-state": "CREATING",
 "lifecycle-state-details": "REQUESTED",
 "requestor-email": "jdoe@mycompany.com",
 "requestor-name": "John Doe",
 "update-time": "2019-12-20T19:04:09+00:00"
 }
}
```

**To show the status of a Data Transfer Appliance Entitlement request using the CLI**

```
oci dts appliance show-entitlement --compartment-id <compartment_id>
```

For example:

```
oci dts appliance show-entitlement --compartment-id ocid.compartment.oc1..exampleuniqueID
```

```
{
 "data": {
 "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
 "defined-tags": null,
 "display-name": null,
 "freeform-tags": null,
 "id": null,
 "lifecycle-state": "ACTIVE",
 "lifecycle-state-details": "APPROVED",
 "requestor-email": null,
 "requestor-name": null
 }
}
```
Establishing the Data Transfer Appliance Entitlement Policy

Use the following policy to enable users in a specific group to request a Data Transfer Appliance Entitlement in your tenancy.

```
Allow group <group_name> to {DTA_ENTITLEMENT_CREATE} in tenancy
```

Entitlement Eligibility

Your request for a Data Transfer Appliance Entitlement in your tenancy may be denied if you are a free trial customer. If your request is denied, upgrade to a full account. You can also contact your Oracle Customer Support Manager or Oracle Support to determine your options for obtaining the entitlement.

Appliance Entitlement Eligibility

Your request for a Data Transfer Appliance Entitlement in your tenancy may be denied if you are a free trial customer. If your request is denied, upgrade to a full account. You can also contact your Oracle Customer Support Manager or Oracle Support to determine your options for obtaining the entitlement.

Setting Up Notifications

Set up rules for the Export Job notification resource that notify the appropriate administrators of the tenancy of events such as when someone creates an export job and when Oracle ships the export appliance.

The types of events you can set up are:

- CREATE
- DELETE
- UPDATE

See Notifications Overview on page 3350 and Overview of Events on page 1784 for more information.

You can also set up notifications for your export job using the CLI. See Setting Up Export Job Notifications on page 1097 for more information on this feature.

Notification Policies

Set up the following policies to support notifications for export jobs:

```
Allow group <group_name> to manage ons-topics in tenancy
Allow group <group_name> to manage ons-subscriptions in tenancy
Allow group <group_name> to manage cloudevents-rules in tenancy
Allow group <group_name> to inspect compartments in tenancy
```

Configuring Firewall Settings

Ensure that your local environment’s firewall can communicate with the Data Transfer Service running on the IP address ranges: 140.91.0.0/16. You also need to open access to the Object Storage IP address ranges: 134.70.0.0/17.

Creating Export Jobs

This section describes how to create an export job as part of the preparation for the data export. See Export Jobs on page 1113 for complete details on all tasks related to export jobs.

An export job represents the collection of files that you want to export and signals the intention to copy those files from your Oracle Cloud Infrastructure Object Storage or Archive Storage bucket to your data center using an Oracle-provided export appliance. Create the export job in the same compartment as the bucket and supply a human-readable name for the export job.

**Note:**

It is recommended that you create a compartment for each export job to minimize the required access your tenancy.
Creating an export job returns a job ID that you specify in other export tasks. For example:

ocid.compartment.oc1..exampleuniqueID

To create an export job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Select the Compartment you are to use for data exports from the list.
3. A list of export jobs that have already been created is displayed in the Export Jobs page.
4. Click Create Export Job.
5. Enter a Job Name. Avoid entering confidential information. Then, select the Bucket Name from the list.
6. Complete the following fields:
   - Company Name
   - Recipient Phone
   - Recipient Email
   - Care of - Optional intermediary party responsible for transferring the appliance from the delivery vendor to the intended recipient.
   - Address 1
   - Address 2
   - City/Locality
   - State/Province/Region
   - Zip/Postal Code
   - Country
7. (Optional) Add any tagging information, including the tag namespace, key, and value in the associated fields.
8. Click Create.

The export job you created is added to the list of export jobs.

To create an export job using the CLI

oci dts export create --compartment-id <compartment_id> --bucket-name <bucket_name> --display-name <display_name> --addressee <addressee> --care-of <care_of> --address <address> --city-or-locality <city_or_locality> --state-province-region <state_province_region> --country <country> --zip-postal-code <zip_postal_code> --phone-number <phone_number> --email <email> <options>

<display_name> is the name of the export job as it appears. Avoid entering confidential information.
<addressee> is the company or person to receiving the appliance.
<care_of> is the contact associated with the addressee.
<address> is the required address of the addressee.
<city_or_locality> is city or locality of the addressee.
<state_province_region> is the state, province, or region of the addressee.
<country> is the country of the addressee.
<zip_postal_code> is the zip or postal code of the addressee.
<phone_number> is the phone number of the addressee or contact.
<email> is the email address of the addressee or contact.
<options> are:
• **--prefix**: List of objects with names matching this prefix would be part of this export job.
• **--range-start**: Object names returned by a list query must be greater or equal to this parameter.
• **--range-end**: Object names returned by a list query must be strictly less than this parameter.
• **--freeform-tags**: Free-form tags for this resource. Each tag is a simple key-value pair with no predefined name, type, or namespace. Example: `{"Department": "Finance"}` This is a complex type whose value must be valid JSON. The value can be provided as a string on the command line or passed in as a file using the file://path/to/file syntax. The **--generate-param-json-input** option can be used to generate an example of the JSON which must be provided. We recommend storing this example in a file, modifying it as needed and then passing it back in via the file:// syntax.
• **--defined-tags**: Defined tags for this resource. Each key is predefined and scoped to a namespace. For more information, see [Resource Tags]. Example: `{"Operations": {"CostCenter": "42"}}` This is a complex type whose value must be valid JSON. The value can be provided as a string on the command line or passed in as a file using the file://path/to/file syntax. The **--generate-param-json-input** option can be used to generate an example of the JSON which must be provided. We recommend storing this example in a file, modifying it as needed and then passing it back in via the file:// syntax.
• **--wait-for-state**: This operation creates, modifies or deletes a resource that has a defined lifecycle state: CREATING, ACTIVE, IN PROGRESS, SUCCEEDED, FAILED, CANCELLED, or DELETED. Specify this option to perform the action and then wait until the resource reaches a given lifecycle state. Multiple states can be specified, returning on the first state. For example, **--wait-for-state SUCCEEDED --wait-for-state FAILED** would return on whichever lifecycle state is reached first. If timeout is reached, a return code of 2 is returned. For any other error, a return code of 1 is returned.
• **--max-wait-seconds**: The maximum time in seconds to wait for the resource to reach the lifecycle state defined by the **--wait-for-state** attribute. Default is 1200.
• **--wait-interval-seconds**: The check interval in seconds to determine whether the resource to see if it has reached the lifecycle state defined by the **--wait-for-state**. Default is 30.
• **--address2**: Optional address line 2.
• **--address3**: Optional address line 3.
• **--address4**: Optional address line 4.
• **--from-json**: Provide input to this command as a JSON document from a file using the file://path/to/file syntax. The **--generate-full-command-json-input** option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: [https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions].

For example:

```bash
oci dts export create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket-name MyBucket1 --display-name MyExportJob1 --addressee "MyCompany Corp" --care-of "John Doe" --address1 "123 Main St." --city-or-locality Anytown --state-province-region CA --country USA --zip-postal-code 12345 --phone-number "4085551212" --email jdoe@mycompany.com
```

```json
{
  "data": {
    "appliance-decryption-passphrase": "********",
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "appliance-serial-number": null,
    "bucket-access-policies": [
      "POLICIES CREATION IN PROGRESS"
    ],
    "bucket-name": "MyExportJobs",
```

Oracle Cloud Infrastructure User Guide 1095
Notifications To include notifications, include the `--setup-notifications` option. See Setting Up Export Job Notifications on page 1097 for more information on this feature.

Getting Export Job IDs

Each export job you create has a unique ID within Oracle Cloud Infrastructure. For example:

```
ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID
```

You will need to forward this export job ID to the Data Administrator.

To get the export job ID using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Select the Compartment from the list.
   The export jobs in that compartment are displayed.
3. Find the export job for which you want to display the details.
4. Click the Actions icon (agle), and then click View Details.

To get the export job ID using the CLI

```
oci dts export list --compartment-id <compartment_id>
```
For example:

```shell
oci dts export list --compartment-id ocid.compartment.oc1..exampleuniqueID
```

```
{
  "data": [
    {
      "bucket-name": "MyExportJobs",
      "creation-time": "2020-06-18T17:24:13+00:00",
      "defined-tags": {},
      "display-name": "MyExportJob1",
      "freeform-tags": {},
      "id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID",
      "lifecycle-state": "CREATING",
      "lifecycle-state-details": "PENDING_MANIFEST_GENERATION"
    },
    {
      "bucket-name": "MyTestExportJobs",
      "creation-time": "2020-06-18T18:07:59+00:00",
      "defined-tags": {},
      "display-name": "MyTestExportJob",
      "freeform-tags": {},
      "id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID",
      "lifecycle-state": "CREATING",
      "lifecycle-state-details": "PENDING_MANIFEST_GENERATION"
    }
  ]
}
```

The ID for each export job is included in the return:

```
"id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID"
```

**Tip:**

When you create an export job using the `oci dts export create` CLI, the export job ID is displayed in the CLI's return. You can also run the `oci dts export show` CLI for that specific job to get the ID.

### Setting Up Export Job Notifications

You can generate notifications that send messages regarding changes to a new or existing export job through the CLI. Using this feature creates a topic, subscription for a list of email addresses, and a rule that notifies you on all events related to the export job's activities and changes in state. This method provides a more convenient way to generate notifications tailored to export jobs.

The CLI command to set up export job notifications is different depending on whether you are creating a new export job or updating an existing export job. In both cases, running the CLI command prompts you to enter the email addresses of each notification subscriber as a comma separated list. Each recipient is sent an email with a link to confirm they want to receive the notifications.

You are prompted to enter those email addresses you want included in the notifications, separated by commas (","). When your list is complete, add a colon (";") followed by your own email address: `user1@mycompany.com, user2@mycompany.com : myemail@mycompany.com`.

For both of the notification commands, the following is returned:

If the commands fail to run, you can use the OCI CLI to do the setup manually:

```shell
export ROOT_COMPARTMENT_OCID=ocidv1:tenancy:oc1:exampleuniqueID
oci ons topic create --compartment-id $ROOT_COMPARTMENT_OCID --name DTSEExportTopic --description "Topic for data transfer service export jobs"
```
oci ons subscription create --protocol EMAIL --compartment-id $ROOT_COMPARTMENT_OCID --topic-id $TOPIC_OCID --endpoint $EMAIL_ID
oci events rule create --display-name DTExportRule --is-enabled true --compartment-id $ROOT_COMPARTMENT_OCID --actions '[{"actionType":"ONS","topicId":"$TOPIC_OCID","isEnabled":true}]' --condition '["eventType": ["com.oraclecloud.datatransferservice.addapplianceexportjob","com.oraclecloud.datatransferservice.deleteapplianceexportjob","com.oraclecloud.datatransferservice.updateapplianceexportjob","com.oraclecloud.datatransferservice.moveapplianceexportjob"]]' --description "Rule for data transfer service to send notifications for export jobs"
Creating topic for export

To set up notifications when creating an export job using the CLI

To set up notifications when creating an export job, include the --setup notifications option as part of the CLI:

oci dts export create --compartment-id <compartment_id> --bucket-name <bucket_name> --display-name <display_name> --addressee <addressee> --care-of <care_of> --address <address> --city-or-locality <city_or_locality> --state-province-region <state_province_region> --country <country> --zip-postal-code <zip_postal_code> --phone-number <phone_number> --email <email> <options> --setup-notifications

To set up notifications for an existing export job using the CLI

To set up notifications for an existing export job:

oci dts export setup-notifications

Generating the Export Manifest File

The data export job requires that you generate a manifest file for the files you want to be exported to you in the Data Transfer Appliance. This manifest file is stored in your export job's bucket. Oracle uses the manifest file to download from that bucket all the files that are listed in the manifest. When the Data Transfer Appliance is sent to you, the download summary is available at the root of the Data Transfer Appliance's mount point, allowing you to compare the manifest against the download summary.

Note:
You can only use the CLI command to generate the export manifest file.

To generate an export manifest file using the CLI

oci dts export generate-manifest --compartment-id <compartment_id> --job-id <job_id> --bucket <bucket> <options>

<options> are:
• --prefix: The subset of objects that needs to be exported whose names start with this prefix.
• --start: The subset of objects that needs to be exported starting with this object (inclusive).
• --end: The subset of objects that needs to be exported up to this object (inclusive).

Creating the Data Export Policy

Data export requires you to add the provided policy language to authorize a secure Oracle IAM user to have read-only access to the bucket for export. You must have administrator privileges in your tenancy to create the data export policy.

To create an export policy using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
Data Transfer

2. Select the Compartment from the list.
The export jobs in that compartment are displayed.
3. Click the export job link whose data export policies you want to access.
The Details page for that export job appears.
4. Find the export policies under Policy Language in the Details page.
5. Copy and use these policy statements in the policy you create in the Console.
See Getting Started with Policies on page 2135 for more information.
To create an export policy using the CLI
The export create-policy CLI automates the process of generating policies for export job. You do not need to use the
Console to create individual policies if you run this CLI.
oci dts export create-policy --job-id <job_id>
For example:
oci dts export create-policy --job-id
ocid1.datatransferapplianceentitlement.oc1..exampleuniqueID
Setting up the following policies in the root compartment. If the following
operation fails it means that you do not have enough privileges to create
policies. Re-run the below command with the correct user
NOTE: Sometimes you will need to replace a single quote with '"'"'
oci iam policy create --name e2e-export-test-af3df5176d46_Policy
--compartment-id $ROOT_COMPARTMENT --statements '["DEFINE TENANCY
OCI_TENANCY AS ocid1.tenancy.oc1..exampleuniqueID", "DEFINE GROUP
OCI_EXPORT_GROUP AS ocid1.group.region1..exampleuniqueID", "ADMIT GROUP
OCI_EXPORT_GROUP OF TENANCY OCI_TENANCY TO read objects IN TENANCY where
target.bucket.name='dtsTestBucket'", "ADMIT GROUP OCI_EXPORT_GROUP OF
TENANCY OCI_TENANCY TO read objectstorage-namespaces IN TENANCY"]' -description "The policies to allow DTS to process the export job"
{
"data": {
"compartment-id": "ocid1.tenancy.region1..exampleuniqueID",
"defined-tags": {},
"description": "The policies to allow DTS to process the export job",
"freeform-tags": {},
"id": "ocid1.policy.region1..uniqueID",
"inactive-status": null,
"lifecycle-state": "ACTIVE",
"name": "e2e-export-test-af3df5176d46_Policy",
"statements": [
"DEFINE TENANCY OCI_TENANCY AS ocid1.tenancy.oc1..exampleuniqueID",
"DEFINE GROUP OCI_EXPORT_GROUP AS
ocid1.group.region1..exampleuniqueID",
"ADMIT GROUP OCI_EXPORT_GROUP OF TENANCY OCI_TENANCY TO read objects
IN TENANCY where target.bucket.name='dtsTestBucket'",
"ADMIT GROUP OCI_EXPORT_GROUP OF TENANCY OCI_TENANCY TO read
objectstorage-namespaces IN TENANCY"
],
"time-created": "2020-07-09T18:37:23.332000+00:00",
"version-date": null
},
"etag": "20eb7654cd14fcfcaf8648de3c6dcc84d553069f"
}

Oracle Cloud Infrastructure User Guide

1099


**Requesting the Export Appliance**

This section describes how to request an export appliance from Oracle.

*To request an export appliance using the Console*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Exports**.
2. Select the **Compartment** from the list.

   The export jobs in that compartment are displayed.
3. Click the export job link for which you want to request the export appliance.

   The Details page for that export job appears.
4. Click **Request Export Appliance**.

   The Request Export Appliance dialog appears prompting you to review the manifest file before continuing with the export appliance request.

   Review the manifest file to ensure all your export job information, such as the bucket and contact information is correct. If anything is not correct, cancel the application request and correct the export job information before trying again to request an export application.
5. Click **Request**.

   The Details page is updated to indicate **Appliance Requested**. The state of your export job is updated to **Pending Approval** in the list of export jobs.

*To request an export appliance using the CLI*

```
oci dts export request-appliance --job-id <job_id>
```

For example:

```json
oci dts export request-appliance --job-id ocid1.datatransferapplianceentitlement.oc1..exampleuniqueID
{
  "data": {
    "appliance-decryption-passphrase": null,
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "appliance-serial-number": null,
    "bucket-access-policies": [
      "DEFINE TENANCY OCI_TENANCY AS ocid1.tenancy.oc1..exampleuniqueID",
      "DEFINE GROUP OCI_EXPORT_GROUP AS ocid1.group.region1..exampleuniqueID",
      "ADMIT GROUP OCI_EXPORT_GROUP OF TENANCY OCI_TENANCY TO read objects IN TENANCY where target.bucket.name='MyExportBucket'",
      "ADMIT GROUP OCI_EXPORT_GROUP OF TENANCY OCI_TENANCY TO read objectstorage-namespaces IN TENANCY"
    ],
    "bucket-name": "MyExportBucket",
    "compartment-id": "ocid1.compartment.region1..exampleuniqueID",
    "creation-time": "2020-07-09T18:36:59+00:00",
    "customer-shipping-address": {
      "address1": "123 Main St.",
      "address2": null,
      "address3": null,
      "address4": null,
      "addressee": "DTS",
      "care-of": "John Doe",
      "city-or-locality": "Anytown",
      "country": "USA",
      "state-or-province": null,
      "zip-code": null
    }
  }
}
```
"email": "jdoe@mycompany.com",
"phone-number": "4085551212",
"state-or-region": "CA",
"zipcode": "12345"
},
"defined-tags": {},
"display-name": "e2e-export-test-af3df5176d46",
"first-object": "oci_data_export_export-job-37",
"freeform-tags": {},
"id": "ocid1.datatransferapplianceexportjob.region1..exampleuniqueID",
"last-object": "oci_data_export_export-job-40",
"lifecycle-state": "ACTIVE",
"lifecycle-state-details": "PENDING_APPROVAL",
"manifest-file": "oci_data_export_manifest_ocid1.datatransferapplianceexportjob.region1..exampleuniqueID",
"manifest-md5": "NcEMgcgK2fK8HfvUV3eWAA==",
"next-object": null,
"number-of-objects": "2",
"prefix": null,
"range-end": "oci_data_export_export-job-50",
"range-start": "oci_data_export_export-job-37",
"receiving-security-tie": null,
"sending-security-tie": null,
"total-size-in-bytes": "85585303"
},
"etag": "1"
}

Tracking the Export Appliance Delivery

To track the export appliance delivery status using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports
2. Select the Compartment from the list.
   The export jobs in that compartment are displayed.
3. Click the export job for which you want to display the details.
   As an alternative, you can click the Actions icon ( ) associated with your export job, and then click View Details.

The status of the requested export appliance is listed under Appliance Information.

To track the export appliance delivery status using the CLI

oci dts export show --job-id <job_id> <options>

<options> are:

- --from-json: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The --generate-full-command-json-input option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options” link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions.
For example:

```bash
oci dts export show --job-id
ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID
```

```json
{
  "data": {
    "appliance-decryption-passphrase": "********",
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "appliance-serial-number": null,
    "bucket-access-policies": [
      "POLICIES CREATION IN PROGRESS"
    ],
    "bucket-name": "MyExportJobs",
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2020-06-18T17:24:13+00:00",
    "customer-shipping-address": {
      "address1": "123 Main St.",
      "address2": null,
      "address3": null,
      "address4": null,
      "addressee": "MyCompany",
      "care-of": "John Doe",
      "city-or-locality": "Anytown",
      "country": "US",
      "email": "jdoe@mycompany.com",
      "phone-number": "4085551212",
      "state-or-region": "CA",
      "zipcode": "12345"
    },
    "defined-tags": {},
    "display-name": "MyExportJob1",
    "first-object": null,
    "freeform-tags": {},
    "id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID",
    "last-object": null,
    "lifecycle-state": "CREATING",
    "lifecycle-state-details": "PENDING_MANIFEST_GENERATION",
    "manifest-file": null,
    "manifest-md5": null,
    "next-object": null,
    "number-of-objects": null,
    "prefix": null,
    "range-end": null,
    "range-start": null,
    "receiving-security-tie": null,
    "sending-security-tie": null,
    "total-size-in-bytes": null
  },
  "etag": "1--gzip"
}
```

The status of the requested export appliance is listed in the appliance attributes in the returned information.

**Notifying the Data Administrator**

When you have completed all the tasks in this topic, provide the Data Administrator of the following:

- IAM login credentials
- Oracle Cloud Infrastructure CLI configuration files
- Export job ID
What's Next

You can follow the progress of the export job and view the metrics associated with the copying of files from Oracle Cloud Infrastructure to your appliance. See Monitoring the Export Job Status and Data Transfer Metrics on page 1103.

Monitoring the Export Job Status and Data Transfer Metrics

This topic describes the monitoring tasks you can perform after your appliance request has been approved and the export job begins. The Project Sponsor role typically performs these tasks. See Roles and Responsibilities on page 1085.

Note:

You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

Once Oracle approves the appliance request and the export job begins, follow progress of the export job status.

To monitor the status of your export job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Select the Compartment from the list.
   - The export jobs in that compartment are displayed.
3. Click the export job for which you want to display the details.
   - As an alternative, you can click the Actions icon ( ⚙️ ) associated with your export job, and then click View Details.
4. Look at the State and Details fields. See Export Appliance State Values on page 1103 for a list of the states and their details.

To monitor the status of your export job using the CLI

At the command prompt on the host, run dts appliance show to monitor the export appliance status.

oci dts export show --job-id <job_id>

See Export Appliance State Values on page 1103 for a list of the states and their details.

Export Appliance State Values

Here are the export job and appliance state values, including their details:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating</td>
<td>The job is in the initialization phase. Additional steps are required from the user before it becomes Active.</td>
<td>Pending Manifest Generation</td>
<td>Generate an export manifest for the bucket from where data is being exported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pending Submission</td>
<td>The export job is in a pending state until you request an appliance for the export job.</td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Details</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>The job is awaiting approval from Oracle before an appliance can be assigned for this export job.</td>
<td>Appliance Provisioning</td>
<td>An appliance is being provisioned for the export job.</td>
</tr>
<tr>
<td>In Progress</td>
<td>The export job is approved and is actively being worked on.</td>
<td>Downloading</td>
<td>Data download to the appliance is in progress.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oracle Shipped</td>
<td>Oracle has shipped the appliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer Received</td>
<td>The appliance has been delivered to the customer site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer Processing</td>
<td>The appliance is being processed at the customer site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer Shipped</td>
<td>The appliance has been shipped to Oracle from the customer site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oracle Received</td>
<td>Oracle has received back the appliance after export.</td>
</tr>
<tr>
<td>Succeeded</td>
<td>The export is complete.</td>
<td>Closed</td>
<td>The export job is closed.</td>
</tr>
<tr>
<td>Failed</td>
<td>The export job failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cancelled</td>
<td>The export job was canceled before an appliance was requested for export.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deleted</td>
<td>The export job was canceled.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Viewing Data Transfer Metrics**

Once the data transfer begins, you can view the metrics associated with the export job in the Transfer Appliance Details page in chart or table format.

**Tip:**

Set up your notifications to alert you when the data transfer from Oracle Cloud Infrastructure to the appliance is occurring. When the state changes to **In Progress Downloading**, you can start viewing data transfer metrics.

Select **Metrics** under **Resources** to display each of these measures:

- **Export Files Downloaded** - Total number of files downloaded to the appliance for export.
- **Export Bytes Downloaded** - Total number of bytes downloaded to the appliance for export.
- **Export Files Remaining** - Total number of files left to be downloaded for export.
- **Export Bytes Remaining** - Total number of bytes left to be downloaded for export.
- **Export Files in Error** - Total number of files in error for export.
- **Export Download Verification Progress** - Progress of verification of files that have already been downloaded for export.

Select the **Start Time** and **End Time** for these measures. You can either set them manually by entering the days and times in their respective fields, or by selecting the Calendar feature and picking the times that way. You can also select from a list of standard times (last hour, last 6 hours, and so forth) from the **Quick Selects** list for the period measured. The time period you specify applies to all the measures.

Specify the **Interval** (for example, 5 minutes, 1 hour) that each measure is recorded from the list.

Specify the **Statistic** being recorded (for example, Sum, Mean) for each measure from the list.
Choose additional actions from the **Options** list, including viewing the query in the **Metrics Explorer**, capturing the URL for the measure, and switching between chart and table view.

Click **Reset Charts** to delete any existing information in the charts and begin recording new metrics.

See **Monitoring Overview** on page 2660 for general information on monitoring your Oracle Cloud Infrastructure services.

**What's Next**

You are now ready to configure the export appliance after you receive it from Oracle. See **Configuring the Export Appliance** on page 1105.

### Configuring the Export Appliance

This topic describes the tasks associated with configuring the export appliance after you receive it from Oracle. The Infrastructure Engineer role typically performs these tasks. See **Roles and Responsibilities** on page 1085.

#### Unpacking and Connecting the Appliance to the Network

When the shipping vendor delivers your export appliance, Oracle updates the status as **Delivered** and provides the date and time the appliance was received in the **Appliance Information** section.

Your export appliance arrives in a transit case with a telescoping handle and wheels. The case amenities allow for easy movement to the location where you intend to place the appliance to upload your data.

**Important:**

**Retain all packaging materials!** When shipping the export appliance back to Oracle, you must package the appliance in the same manner and packaging in which the appliance was received.

Here are the tasks involved in unpacking and getting your export appliance ready to configure.

1. Inspect the tamper-evident security tie on the transit case.
   
   If the appliance was tampered with during transit, the tamper-evident security tie serves to alert you.

   **Caution:**
   
   If the security tie is damaged or is missing, do not plug the appliance into your network! Immediately file a Service Request (SR).

2. Remove and compare the number on the security tie with the number logged by Oracle.
3. Open the transit case and ensure that the case contains the following items:
   
   - Appliance unit and power cable (two types of power cables provided: C14 and C13 to 14)
   - USB to DB-9 serial cable
   - Return shipping instructions (retain these instructions)
   - Return shipping label, label sleeve, tie-on tag, and zip tie
   - Return shipment tamper-evident security tie (use this tie to ensure secure transit case back to Oracle)
4. Compare the number on the return shipment security tie with the number logged by Oracle.
5. Remove the export appliance from the case and place the appliance on a solid surface or in a rack.

**Caution:**

We recommend assistance lifting the export appliance out of the transit case and placing the appliance in a rack or on a desk top. The total shipping weight is about 64 lbs (29.0299 kg) and appliance weight is 38 lbs (17.2365 kg).

6. Connect the appliance to your local network using one of the following:
   - 10GBase-T: Standard RJ-45
   - SFP+: The transceiver must be compatible with Intel X520 NICs.

7. Attach one of the provided power cords to the appliance and plug the other end into a grounded power source.

8. Turn on the appliance by flipping the power switch on the back of the appliance.

---

**To see the security tie number logged by Oracle using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Find the export job and export appliance associated with the removed security tie.
3. Click the Actions icon ( ), and then click View Details.
4. Look at the contents of the Send Security Tie ID field in the Appliance Information section and compare that number with the number on the physical tag.

**To see the security tie number logged by Oracle using the CLI**

At the command prompt on the Control Host, run `oci dts appliance show` to delete an export appliance.

```
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```

**Caution:**

If the number on the physical security tie does not match the number logged by Oracle, do not plug the appliance into your network! Immediately file a Service Request (SR).

**Note:**

Keep possession of the security tie after you have finished unpacking and connecting the appliance. Include it when returning the appliance to Oracle. Failure to include the security tie can result in a delay in the data migration process.

---

**To see the security tie number logged by Oracle using the Console**

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Find the export job and export appliance associated with the return shipment security tie.
3. Click the Actions icon ( ), and then click View Details.
4. Look at the contents of the Return Security Tie ID field in the Appliance Information section and compare that number with the number on the physical tag.

**To see the security tie number logged by Oracle using the CLI**

```
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```
Connecting the Appliance to the Terminal Emulation Host

Connect the appliance to your designated Terminal Emulation Host computer using the provided USB to DB-9 serial cable.

Note:
You might need to download the driver for this cable on your Terminal Emulation Host: https://www.cablestogo.com/product/26887/5ft-usb-to-db9-male-serial-rs232-adapter-cable#support

Setting Up Terminal Emulation

Set up terminal emulation so you can communicate with the appliance device through the appliance's serial console. This communication requires installing serial console terminal emulator software. We recommend using the following:

- PuTTY for Windows
- ZOC for OS X
- PuTTY or Minicom for Linux

Configure the following terminal emulator software settings:

- Baud Rate: 115200
- Emulation: VT102
- Handshaking: Disabled/off
- RTS/DTS: Disabled/off

Note:
PuTTY does not allow you to configure all of these settings individually. However, you can configure the PuTTY default settings by selecting the Serial connection type and specifying ”115200” for the Serial Line baud speed. This is sufficient to use PuTTY as a terminal emulator for the appliance.

Configuring the Export Appliance Networking

When the appliance boots up, an appliance serial console configuration menu is displayed on the Terminal Emulation Host to which the appliance is connected.

Oracle Cloud Data Transfer Appliance
- For use with minimum dts version: dts-0.4.140
- See "Help" for determining your dts version

1) Configure Networking
2) Show Networking
3) Reset Authentication
4) Show Authentication
5) Show Status
6) Collect Appliance Diagnostic Information
7) Generate support bundle
8) Shutdown Appliance
9) Reboot Appliance
10) Help

Caution:
If the number on the return security tie does not match the number logged by Oracle, file a Service Request (SR). These security tie numbers must match or Oracle cannot upload data from your returned export appliance.
The appliance supports a single active network interface on any of the 10-Gbps network ports. If only one interface is cabled and active, that interface is chosen automatically. If multiple interfaces are active, you are given the choice to select the interface to use.

**To configure your export appliance networking**

1. From the Terminal Emulation Host, select **Configure Networking** from the appliance serial console menu.
2. Provide the required networking information when prompted:
   - **IP Address**: IP address of the export appliance.
   - **Subnet Mask Length**: The count of leading 1 bit in the subnet mask. For example, if the subnet mask is 255.255.255.0 then the length is 24.
   - **Default Gateway**: Default gateway for network communications.

For example:

```
Configure Networking:
^C to cancel

Configuring IP address, subnet mask length, gateway
Example:
IP Address : 10.0.0.2
Subnet Mask Length : 24
Gateway : 10.0.0.1
Address: 10.0.0.1
Subnet Mask Length: 24
Gateway: 10.0.0.1

Configuring IP address 10.0.0.1 netmask 255.255.255.0 default gateway 10.0.0.1
Enabling enp0s3
Now trying to restart the network

Network configuration is complete
New authentication material created.
Client access token                   : 4iH1gw1okPJO
Press ENTER to return...
```

When you configure a network interface, the appliance software generates a new client access token and appliance X.509/SSL certificate. The access token is used to authorize your Control Host to communicate with the Data Transfer Appliance's Management Service. The x.509/SSL certificate is used to encrypt communications with the Data Transfer Appliance's Management Service over the network. Provide the access token and SSL certificate fingerprint values displayed here when you use the CLI commands to `initialize authentication on your host machine`.

You can change the selected interface, network information, and reset the authentication material at any time by selecting **Configure Networking** again from the appliance serial console menu.
Notify the Data Administrator

After completing the tasks in this topic, send the following appliance information IP address of the export appliance to the Data Administrator:

- Appliance IP address
- Access token
- SSL certificate fingerprint

What's Next

You are now ready to copy your data from the export appliance to your data center. See Copying Data from the Export Appliance on page 1109.

Copying Data from the Export Appliance

This topic describes the tasks associated with copying data from the export appliance to your data center's Data Host using the Control Host. The Data Administrator role typically performs these tasks. See Roles and Responsibilities on page 1085.

Note:

You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

Information Prerequisites

Before performing any export appliance copying tasks, you must obtain the following information:

- Appliance IP address - typically is provided by the Infrastructure Engineer.
- IAM login information, Data Transfer Utility configuration files, export job ID, and job label - typically is provided by the Project Sponsor.

Setting Up an HTTP Proxy Environment

You might need to set up an HTTP proxy environment on the Control Host to allow access to the public internet. This proxy environment allows the Oracle Cloud Infrastructure CLI to communicate with the Data Transfer Appliance Management Service and the export appliance over a local network connection. If your environment requires internet-aware applications to use network proxies, configure the Control Host to use your environment's network proxies by setting the standard Linux environment variables on your Control Host.

Assume that your organization has a corporate internet proxy at http://www-proxy.myorg.com and that the proxy is an HTTP address at port 80. You would set the following environment variable:

```
export HTTPS_PROXY=http://www-proxy.myorg.com:80
```

If you configured a proxy on the Control Host and the export appliance is directly connected to that host, the Control Host tries unsuccessfully to communicate with the export appliance using a proxy. Set a `no_proxy` environment variable for the appliance. For example, if the appliance is on a local network at 10.0.0.1, you would set the following environment variable:

```
export NO_PROXY=10.0.0.1
```

Setting Firewall Access

If you have a restrictive firewall in the environment where you are using the Oracle Cloud Infrastructure CLI, you may need to open your firewall configuration to the following IP address ranges: 140.91.0.0/16.
Configuring the Export Appliance

After you have physically set up the export appliance and connected it to your network, you can configure it using the CLI to allow the copying of the data it contains to your data center.

**Note:**
You can only use the CLI command to configure the appliance.

To configure the export appliance using the CLI:

```bash
oci dts export configure-physical-appliance --job-id <job-id> --appliance-cert-fingerprint <fingerprint> --appliance-ip <appliance_ip> --rw <rw> --world <world><options>
```

- `<fingerprint>` is the export appliance X.509/SSL certificate fingerprint.
- `<appliance_ip>` is the IP address of the export appliance.
- `<rw>` indicates whether the exported data has read/write permissions. Specify `true` or `false`.
- `<world>` indicates whether the exported data is accessible by all. Specify `true` or `false`.
- `<options>` are:
  - `--appliance-port`: The port number used by the export appliance.
  - `--appliance-profile`: User-defined name or description of the transfer appliance. This is useful if you have multiple transfer appliances.
  - `--access-token`: The access token to authenticate with the export appliance.
  - `--appliance-port`: The port number used by the export appliance.
  - `--subnet-mask-length`: The subnet mask length for the IP address.

### Setting Your Data Host as an NFS Client

**Note:**
Only Linux machines can be used as Data Hosts.

Set up your Data Host as an NFS client:

- For Debian or Ubuntu, install the `nfs-common` package. For example:
  ```bash
  sudo apt-get install nfs-common
  ```
- For Oracle Linux or Red Hat Linux, install the `nfs-utils` package. For example:
  ```bash
  sudo yum install nfs-utils
  ```

### Mounting the NFS Share

To mount the NFS share:

At the command prompt on the Data Host, create the mountpoint directory:

```bash
mkdir -p /mnt/<mountpoint>
```

For example:

```bash
mkdir -p /mnt/nfs-ds-1
```

Next, use the `mount` command to mount the NFS share.

```bash
mount -t nfs <appliance_ip>:/data/<dataset_name>/<mountpoint>
```
Data Transfer

For example:

```
mount -t nfs 10.0.0.1:/data/nfs-ds-1 /mnt/nfs-ds-1
```

**Note:**
The appliance IP address in this example (10.0.0.1) may be different that the one you use for your appliance.

After the NFS share is mounted, you can write data to the share.

Copying Files to the Data Host

Copy your file from the appliance to your NFS-mounted Data Host using normal file system tools.

Viewing Data Export Metrics

You can view the metrics associated with an export job in the Transfer Appliance Details page in chart or table format. Select Metrics under Resources to display each of these measures:

- **Export Files Downloaded** - Total number of files downloaded to the appliance for export.
- **Export Bytes Downloaded** - Total number of bytes downloaded to the appliance for export.
- **Export Files Remaining** - Total number of files left to be downloaded for export.
- **Export Bytes Remaining** - Total number of bytes left to be downloaded for export.
- **Export Files in Error** - Total number of files in error for export.
- **Export Download Verification Progress** - Progress of verification of files that have already been downloaded for export.

Select the **Start Time** and **End Time** for these measures, either by manually entering the days and times in their respective fields, or by selecting the Calendar feature and picking the times that way. As an alternative to selecting a start and end time, you can also select from a list of standard times (last hour, last 6 hours, and so forth) from the **Quick Selects** list for the period measured. The time period you specify applies to all the measures.

Specify the **Interval** (for example, 5 minutes, 1 hour) that each measure is recorded from the list.

Specify the **Statistic** being recorded (for example, Sum, Mean) for each measure from the list.

**Tip:**
Mean is the most useful statistic for data export.

Choose additional actions from the **Options** list, including viewing the query in the **Metrics Explorer**, capturing the URL for the measure, and switching between chart and table view.

Click **Reset Charts** to delete any existing information in the charts and begin recording new metrics.

See **Monitoring Overview** on page 2660 for general information on monitoring your Oracle Cloud Infrastructure services.

Erasing Files from the Export Appliance

Use standard system tools to remove your data from the export appliance after you have copied your files.

Notifying Export Appliance Return

When the erasure of the client data from the export appliance is complete, notify the Infrastructure Engineer that the appliance is ready to be returned to Oracle.

What's Next

You are now ready to ship the export appliance back to Oracle. See **Returning the Export Appliance to Oracle** on page 1112.
Returning the Export Appliance to Oracle

This topic describes the tasks associated with shipping the export appliance back to Oracle after you have copied your data to your data center. The Infrastructure Engineer role typically performs these tasks. See Roles and Responsibilities on page 1085.

**Note:**
You can only run Oracle Cloud Infrastructure CLI commands from a Linux host. This differs from running CLI commands for other Oracle Cloud Infrastructure Services on a variety of host operating systems. Appliance-based commands require validation that is only available on Linux hosts.

**Shutting down the Export Appliance**

Shut down the export appliance before packing up and shipping it back to Oracle.

*To shut down the export appliance*

Using the terminal emulator on the host machine, select **Shutdown** from the appliance serial console.

**Packing and Shipping the Export Appliance to Oracle**

Return the export appliance to Oracle within 30 days. If you need the appliance beyond the standard 30-day window, you can file a Service Request (SR) to ask for an extension of up to 60 days.

**Important:**
Review and follow the instructions that were provided in the transit case with the appliance.

*To pack and ship the export appliance*

1. Unplug the power cord from the power source and detach the other end of the cord from the export appliance.
2. Disconnect the appliance from your network.
3. Remove the return shipment tamper-evident security tie from the transit case.
4. Place the appliance, power cord, and serial cable in the transit case.

**Caution:**
We recommend assistance lifting and placing the appliance back into the transit case. The total shipping weight is about 64 lbs (29.0299 kg) and appliance weight is 38 lbs (17.2365 kg).

5. Close and secure the transit case with the return tamper-evident security tie.
6. Loop the top of the plastic tie-on tag with return shipping label through the handle of the transit case. Remove the protective tape from the back of the tie-on tag, exposing the adhesive area on which to secure the tag onto itself. Use the provided zip tie to secure the tie-on tag to the handle.
7. Return the transit case to FedEx by doing one of the following:
   - Drop off the packed, sealed, and labeled transit case to an FedEx Authorized ShipCenter location or a nearby FedEx Office location. Obtain a receipt from the vendor to certify transfer of custody.
   - Schedule a pickup with FedEx at your location. Ensure that the transit case is packed, sealed, and labeled before FedEx arrives for pickup.

The shipping vendor notifies Oracle when the appliance is returned to Oracle.

**Tracking the Export Appliance Return**

Use your shipping carrier's tracking feature to following the progress of your export appliance after you return it to Oracle.
Data Export Reference

This topic provides complete task details that are not otherwise fully documented in other topics. Use this topic as a reference to learn and use commands associated with components included in the data export procedure.

Export Jobs

Export Jobs are what determine how and when data is copied from Oracle Cloud Infrastructure to the export appliance. Perform the following export job tasks using the Console or the CLI:

Creating Export Jobs

To create an export job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Select the Compartment you are to use for data exports from the list.
   A list of export jobs that have already been created is displayed.
3. Click Create Export Job.
   The Create Export Job dialog appears.
4. Enter a Job Name. Avoid entering confidential information. Then, select the Upload Bucket from the list.
5. (Optional) Complete the following fields:
   - Prefix: List of objects with names matching this prefix would be part of this export job.
   - Range Start: Object names returned by a list query must be greater or equal to this parameter.
   - Range End: Object names returned by a list query must be strictly less than this parameter.
6. Complete the following fields:
   - Company Name
   - Recipient Name
   - Recipient Email
   - Address 1
   - Address 2
   - City/Locality
   - State/Province/Region
   - Zip/Postal Code
   - Country
7. (Optional) Add any tagging information, including the tag namespace, key, and value in the associated fields.
8. Click Create Transfer Job.

To create an export job using the CLI

oci dts export create --compartment-id <compartment_id> --bucket-name <bucket_name> --display-name <display_name> --addressee <addressee> --care-of <care_of> --address1 <address1> --city-or-locality <city_or_locality> --state-province-region <state_province_region> --country <country> --zip-postal-code <zip_postal_code> --phone-number <phone_number> --email <email> <options>

<display_name> is the name of the export job as it appears. Avoid entering confidential information.
<addressee> is the company or person to receiving the appliance.
<care_of> is the contact associated with the addressee.
<address> is the required address of the addressee.
<city_or_locality> is city or locality of the addressee.
<state_province_region> is the state, province, or region of the addressee.
**Data Transfer**

- `<country>` is the country of the addressee.
- `<zip_postal_code>` is the zip or postal code of the addressee.
- `<phone_number>` is the phone number of the addressee or contact.
- `<email>` is the email address of the addressee or contact.

**<options>** are:

- **--setup-notifications**: Sets up the required export notifications as part of the export job creation process.
- **--prefix**: List of objects with names matching this prefix would be part of this export job.
- **--range-start**: Object names returned by a list query must be greater or equal to this parameter.
- **--range-end**: Object names returned by a list query must be strictly less than this parameter.
- **--freeform-tags**: Free-form tags for this resource. Each tag is a simple key-value pair with no predefined name, type, or namespace. Example: `{"Department": "Finance"}` This is a complex type whose value must be valid JSON. The value can be provided as a string on the command line or passed in as a file using the file://path/to/file syntax. The `--generate-param-json-input` option can be used to generate an example of the JSON which must be provided. We recommend storing this example in a file, modifying it as needed and then passing it back in via the file:// syntax.
- **--defined-tags**: Defined tags for this resource. Each key is predefined and scoped to a namespace. For more information, see [Resource Tags]. Example: `{"Operations": {"CostCenter":"42"}}` This is a complex type whose value must be valid JSON. The value can be provided as a string on the command line or passed in as a file using the file://path/to/file syntax. The `--generate-param-json-input` option can be used to generate an example of the JSON which must be provided. We recommend storing this example in a file, modifying it as needed and then passing it back in via the file:// syntax.
- **--wait-for-state**: This operation creates, modifies or deletes a resource that has a defined lifecycle state: CREATING, ACTIVE, IN PROGRESS, SUCCEEDED, FAILED, CANCELLED, or DELETED. Specify this option to perform the action and then wait until the resource reaches a given lifecycle state. Multiple states can be specified, returning on the first state. For example, `--wait-for-state SUCCEEDED --wait-for-state FAILED` would return on whichever lifecycle state is reached first. If timeout is reached, a return code of 2 is returned. For any other error, a return code of 1 is returned.
- **--max-wait-seconds**: The maximum time in seconds to wait for the resource to reach the lifecycle state defined by the `--wait-for-state` attribute. Default is 1200.
- **--wait-interval-seconds**: The check interval in seconds to determine whether the resource to see if it has reached the lifecycle state defined by the `--wait-for-state`. Default is 30.
- **--address2**: Optional address line 2.
- **--address3**: Optional address line 3.
- **--address4**: Optional address line 4.
- **--from-json**: Provide input to this command as a JSON document from a file using the file://path/to/file syntax. The `--generate-full-command-json-input` option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id -> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusings.htm#AdvancedJSONOptions.

For example:

```bash
oci dts export create --compartment-id ocid.compartment.oc1..exampleuniqueID --bucket-name MyBucket1 --display-name MyExportJob1 --addressee "MyCompany Corp" --care-of "John Doe" --address1 "123 Main St." --city-or-locality Anytown --state-province-region CA --country USA --zip-postal-code 12345 --phone-number "4085551212" --email jdoe@mycompany.com
```
"data": {
    "appliance-decryption-passphrase": "********",
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "appliance-serial-number": null,
    "bucket-access-policies": ["POLICIES CREATION IN PROGRESS"],
    "bucket-name": "MyExportJobs",
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2020-06-18T17:24:13+00:00",
    "customer-shipping-address": {
        "address1": "123 Main St.",
        "address2": null,
        "address3": null,
        "address4": null,
        "addressee": "MyCompany Corp",
        "care-of": "John Doe",
        "city-or-locality": "Anytown",
        "country": "USA",
        "email": "jdoe@mycompany.com",
        "phone-number": "4085554321",
        "state-or-region": "CA",
        "zipcode": "12345"
    },
    "defined-tags": {},
    "display-name": "MyExportJob1",
    "first-object": null,
    "freeform-tags": {},
    "id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID",
    "last-object": null,
    "lifecycle-state": "CREATING",
    "lifecycle-state-details": "PENDING_MANIFEST_GENERATION",
    "manifest-file": null,
    "manifest-md5": null,
    "next-object": null,
    "number-of-objects": null,
    "prefix": null,
    "range-end": null,
    "range-start": null,
    "receiving-security-tie": null,
    "sending-security-tie": null,
    "total-size-in-bytes": null
},
"etag": "4--gzip"
}

Notifications

If you do not include the --setup-notification option when you run the command, the following is returned:

It is a pre-requisite to setup notifications for export. Do you want to setup notifications? [y/N]:

If you do not have the necessary permissions to set up the notifications for export, or if you have previously done this step, then select N. Otherwise, select y. See Setting Up Notifications on page 1093 for more information.

Listing Export Jobs

To display a list of export jobs using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Select the **Compartment** from the list.

The export jobs in that compartment are displayed.

To display a list of export jobs using the CLI

```
oci dts export list --compartment-id <compartment_id> <options>
```

<**options**> are:

- **--lifecycle-state**: Filter the returned export jobs by the specified lifecycle state (specify one only): CREATING, ACTIVE, INPROGRESS, SUCCEEDED, FAILED, CANCELLED, or DELETED.
- **--display-name**: Filter the returned exports jobs by the specified display name.
- **--limit**: The maximum number of results per page, or items to return. For important details about how pagination works, see [List Pagination]. Example: `50`
- **--page**: The value of the `opc- next-page` response header from the previous "List" call. For important details about how pagination works, see [List Pagination].
- **--all**: Returns all pages of results. If you provide this option, then you cannot provide the **--limit** option.
- **--page-size**: Specify the number of export jobs returned per call. Only valid when used with **--all** or **--limit**, and ignored otherwise.
- **--from-json**: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The **--generate-full-command-json-input** option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our “using CLI with advanced JSON options” link: [https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions].

For example:

```
oci dts export list --compartment-id ocid.compartment.oc1..exampleuniqueID
{
  "data": [
  {
    "bucket-name": "MyExportJobs",
    "creation-time": "2020-06-18T17:24:13+00:00",
    "defined-tags": {},
    "display-name": "MyExportJob1",
    "freeform-tags": {},
    "id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID",
    "lifecycle-state": "CREATING",
    "lifecycle-state-details": "PENDING_MANIFEST_GENERATION"
  }
  {
    "bucket-name": "MyTestExportJobs",
    "creation-time": "2020-06-18T18:07:59+00:00",
    "defined-tags": {},
    "display-name": "MyTestExportJob",
    "freeform-tags": {},
    "id": "ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID",
    "lifecycle-state": "CREATING",
    "lifecycle-state-details": "PENDING_MANIFEST_GENERATION"
  }
  ]
}
```

**Displaying Export Job Details**
Data Transfer

**Displaying Export Job Details**

To show the details of an export job using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Exports**.
2. Select the **Compartment** from the list.
   
   The export jobs in that compartment are displayed.
3. Find the export job for which you want to display the details.
4. Click the **Actions** icon (⋮), and then click **View Details**.

To show the details of an export job using the CLI

```
oci dts export show --job-id <job_id> <options>
```

<options> are:

- `--from-json`: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The `--generate-full-command-json-input` option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: [https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions](https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions).

For example:

```
oci dts export show --job-id ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID

{
  "data": {
    "appliance-decryption-passphrase": "********",
    "appliance-delivery-tracking-number": null,
    "appliance-delivery-vendor": null,
    "appliance-return-delivery-tracking-number": null,
    "appliance-serial-number": null,
    "bucket-access-policies": [
      "POLICIES CREATION IN PROGRESS"
    ],
    "bucket-name": "MyExportJobs",
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "creation-time": "2020-06-18T17:24:13+00:00",
    "customer-shipping-address": {
      "address1": "123 Main St.",
      "address2": null,
      "address3": null,
      "address4": null,
      "addressee": "MyCompany",
      "care-of": "John Doe",
      "city-or-locality": "Anytown",
      "country": "US",
      "email": "jdoe@mycompany.com",
      "phone-number": "4085551212",
      "state-or-region": "CA",
      "zipcode": "12345"
    },
    "defined-tags": {},
    "display-name": "MyExportJob1",
    "first-object": null,
  },
```

Oracle Cloud Infrastructure User Guide 1117
Editing Export Jobs

To edit an export job using the Console

1. Open the navigation menu. Under Core Infrastructure, go to Object Storage and click Data Transfer - Exports.
2. Select the Compartment from the list.
   The export jobs in that compartment are displayed.
3. Click the link under Transfer Jobs for the export job whose name you want to edit.
   The Details page for that export job appears.

   Alternatively, you can click the Actions icon ( ), and then click View Details.
4. Click Edit in the Details page.
   The Edit Export Job dialog appears.
5. Edit any of the attributes displayed, including the job name, bucket, and address.
   Avoid entering confidential information.
6. Click Save Changes.
   You are returned to the Details page for that export job.

To edit an export job using the CLI

oci dts export update --job-id <job_id> <options>

<options> are:

• --bucket-name: Name of the bucket associated with the data export. Avoid entering confidential information.
• --prefix: List of objects with names matching this prefix would be part of this export job.
• --range-start: Object names returned by a list query must be greater or equal to this parameter.
• --range-end: Object names returned by a list query must be strictly less than this parameter.
• --display-name: Name of the export job as it appears.
• --lifecycle-state: CREATING, ACTIVE, INPROGRESS, SUCCEEDED, FAILED, CANCELLED, or DELETED.
• --lifecycle-state-details: A property that can contain details on the lifecycle.
• --manifest-file: Manifest file associated with this export job.
• --manifest-md5: md5 digest of the manifest file.
• --number-of-objects: Total number of objects that are exported in this job.
• --total-size-in-bytes: Total size of objects in bytes that are exported in this job.
Data Transfer

- **--first-object**: First object in the list of objects that are exported in this job.
- **--last-object**: Last object in the list of objects that are exported in this job.
- **--next-object**: First object from which the next potential export job could start.
- **--freeform-tags**: Free-form tags for this resource. Each tag is a simple key-value pair with no predefined name, type, or namespace. Example: `{"Department": "Finance"}`. This is a complex type whose value must be valid JSON. The value can be provided as a string on the command line or passed in as a file using the file://path/to/file syntax. The --generate-param-json-input option can be used to generate an example of the JSON which must be provided. We recommend storing this example in a file, modifying it as needed and then passing it back in via the file:// syntax.
- **--defined-tags**: Defined tags for this resource. Each key is predefined and scoped to a namespace. For more information, see [Resource Tags]. Example: `{"Operations": {"CostCenter": "42"}}`. This is a complex type whose value must be valid JSON. The value can be provided as a string on the command line or passed in as a file using the file://path/to/file syntax. The --generate-param-json-input option can be used to generate an example of the JSON which must be provided. We recommend storing this example in a file, modifying it as needed and then passing it back in via the file:// syntax.
- **--if-match**: The tag that must be matched for the task to occur for that entity. If set, the update is only successful if the object's tag matches the tag specified in the request.
- **--force**: Perform task without prompting for confirmation.
- **--wait-for-state**: This operation creates, modifies or deletes a resource that has a defined lifecycle state: CREATING, ACTIVE, IN PROGRESS, SUCCEEDED, FAILED, CANCELLED, or DELETED. Specify this option to perform the action and then wait until the resource reaches a given lifecycle state. Multiple states can be specified, returning on the first state. For example, --wait-for-state SUCCEEDED --wait-for-state FAILED would return on whichever lifecycle state is reached first. If timeout is reached, a return code of 2 is returned. For any other error, a return code of 1 is returned.
- **--max-wait-seconds**: The maximum time in seconds to wait for the resource to reach the lifecycle state defined by the --wait-for-state attribute. Default is 1200.
- **--wait-interval-seconds**: The check interval in seconds to determine whether the resource to see if it has reached the lifecycle state defined by the --wait-for-state. Default is 30.
- **--address**: Company or person to receiving the appliance.
- **--care-of**: Contact associated with the addressee.
- **--address1**: Required address of the addressee (line 1).
- **--address2**: Optional address of the addressee (line 2).
- **--address3**: Optional address of the addressee (line 3).
- **--address4**: Optional address of the addressee (line 4).
- **--city-or-locality**: City or locality of the addressee.
- **--state-province-region**: State, province, or region of the addressee.
- **--country**: Country of the addressee.
- **--zip-postal-code**: Zip or postal code of the addressee.
- **--phone-number**: Phone number of the addressee or contact.
- **--email**: Email address of the addressee or contact.
- **--from-json**: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The --generate-full-command-json-input option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions.
For example:

```bash
oci dts export update --job-id ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID --care-of "Robert Roe" --phone-number 4085554321 --email rroe@mycompany.com
```

Running the command displays the following message:

```
WARNING: Updates to customer-shipping-address and freeform-tags and defined-tags will replace any existing values. Are you sure you want to continue? [y/N]:
```

Confirm you want to continue. The information returned contains the update items you specified:

```json
"bucket-name": "MyExportJobs",
"compartment-id": "ocid.compartment.oc1..exampleuniqueID",
"creation-time": "2020-06-18T17:24:13+00:00",
"customer-shipping-address": {
  "address1": "123 Main St.",
  "address2": null,
  "address3": null,
  "address4": null,
  "addressee": "MyCompany",
  "care-of": "Robert Roe",
  "city-or-locality": "Anytown",
  "country": "US",
  "email": "rroe@mycompany.com",
  "phone-number": "4085554321",
  "state-or-region": "CA",
  "zipcode": "12345"
}
```

**Moving Export Jobs Between Compartments**

To move an export job to a different compartment using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Exports**.
2. Select the **Compartment** from the list.
   The export jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the export job that you want to move.
   The Details page for that export job appears.

   Alternatively, you can click the **Actions** icon ( ⚙ ), and then click **Move Resource**.
4. Click **Move Resource** in the Details page.
   The Move Resource to a Different Compartment dialog appears.
5. Choose the compartment you want to which you want to move the export job from the list.
6. Click **Move Resource**.
   You are returned to the Details page for that export job.

To move an export job to a different compartment using the CLI

```bash
oci dts export change-compartment --job-id <job_id> compartment-id <compartment_id> <options>
```

<compartment_id> is the compartment to which the data export job is being moved.
<options> are:
• **--if-match**: The tag that must be matched for the task to occur for that entity. If set, the update is only successful if the object’s tag matches the tag specified in the request.

• **--from-json**: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The **--generate-full-command-json-input** option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our “using CLI with advanced JSON options’ link: [https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions](https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions).

For example:

```
oci dts export change-compartment --jpb-id
ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID --compartment-id
ocid.compartment.oc1..exampleuniqueID
```

To confirm the transfer, display the list of transfer jobs in the new compartment. See [Listing Export Jobs](#) on page 1115 for more information.

**Deleting Export Jobs**

To delete an export job using the Console

1. Open the navigation menu. Under **Core Infrastructure**, go to **Object Storage** and click **Data Transfer - Exports**.
2. Select the **Compartment** from the list.
   
   The export jobs in that compartment are displayed.
3. Click the link under **Transfer Jobs** for the export job whose name you want to delete.
   
   The Details page for that export job appears.
   
   Alternatively, you can click the **Actions** icon (⋮), and then click **Delete**.
4. Click **Delete** in the Details page.
   
   The Delete Export Job dialog appears to confirm the deletion.
5. Click **Delete**.
   
   The export job is deleted and you are returned to the export jobs page.

To delete an export job using the CLI

```
oci dts export delete --job-id <job_id> <options>
```

<options> are:

• **--if-match**: The tag that must be matched for the task to occur for that entity. If set, the update is only successful if the object’s tag matches the tag specified in the request.

• **--force**: Perform task without prompting for confirmation.

• **--wait-for-state**: This operation creates, modifies or deletes a resource that has a defined lifecycle state: CREATING, ACTIVE, IN PROGRESS, SUCCEEDED, FAILED, CANCELLED, or DELETED. Specify this option to perform the action and then wait until the resource reaches a given lifecycle state. Multiple states can be specified, returning on the first state. For example, **--wait-for-state SUCCEEDED --wait-for-state FAILED** would return on whichever lifecycle state is reached first. If timeout is reached, a return code of 2 is returned. For any other error, a return code of 1 is returned.

• **--max-wait-seconds**: The maximum time in seconds to wait for the resource to reach the lifecycle state defined by the **--wait-for-state** attribute. Default is 1200.

• **--wait-interval-seconds**: The check interval in seconds to determine whether the resource to see if it has reached the lifecycle state defined by the **--wait-for-state**. Default is 30.
Data Transfer

- **--from-json**: Provide input to this command as a JSON document from a file using the file://path-to/file syntax. The --generate-full-command-json-input option can be used to generate a sample JSON file to be used with this command option. The key names are pre-populated and match the command option names (converted to camelCase format, e.g. compartment-id --> compartmentId), while the values of the keys need to be populated by the user before using the sample file as an input to this command. For any command option that accepts multiple values, the value of the key can be a JSON array. Options can still be provided on the command line. If an option exists in both the JSON document and the command line then the command line specified value will be used. For examples on usage of this option, please see our "using CLI with advanced JSON options" link: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliusing.htm#AdvancedJSONOptions.

For example:

```bash
oci dts export delete --job-id ocid1.datatransferapplianceexportjob.oc1..exampleuniqueID
```

Confirm the deletion when prompted. The export job is deleted with no further action or return. To confirm the deletion, display the list of export jobs in the compartment. See Displaying Export Job Details on page 1117 for more information.

### Troubleshooting

This topic describes various troubleshooting issues related to the Data Transfer Service.

#### General

Troubleshooting entries in this section can apply to all data transfer methods.

**Installing a Specific CLI Version**

You may need to change the version of the Oracle Cloud Infrastructure command line interface (CLI) to address issues with a particular feature. Installation of a CLI version other than the one currently installed requires the following steps in order:

1. Go to the following site: https://github.com/oracle/oci-cli/releases.
2. Scroll down to the version you need and download it to your local machine.

**Uninstalling the Existing version of the CLI Version**

If you manually installed the CLI using `pip`, run the following command:

```
pip uninstall oci-cli
```

If you manually installed the CLI in a virtualenv, run the following command:

```
<virtualenv_path>/bin/pip uninstall oci-cli
```

**Installing the Downloaded CLI Version**

See Manual Installation on page 4197 for installation instructions for your downloaded CLI version.

**Appliance-Based Data Transfers**

These troubleshooting entries are associated with appliance-based import and export jobs.

**Troubleshooting the Appliance**

You can generate performance information for troubleshooting issues with the appliance through the terminal emulator on the host machine. Select Collect Appliance Diagnostic Information from the serial console.
configuration menu. The diagnostic tool generates system, network, storage, and performance data while the transfer job is running. It then forwards the data to the appliance serial console. Here you can scroll through the terminal to view it.

You can also use the log capture feature of the serial port emulator to capture the output. Serial port emulators often support the ability to copy the session to a file. Refer to the documentation of your serial port emulation package for instructions. Copying to a log file is useful if you need assistance from Oracle or if your emulation session does not allow you to scroll back and see all the output.

For each operation, the display shows exactly what command was executed and all the options.

Here is an example of the diagnostic output:

```
- systemctl -l --type service --state=active
```

UNIT LOAD ACTIVE SUB DESCRIPTION
audid.service loaded active running Security Auditing Service
blk-availability.service loaded active exited Availability of block devices
chronyd.service loaded active running NTP client/server
console-diags@39-3147-1001.service loaded active running Diagnostic Collection Server for the XA (PID 3147/UID 1001)
crond.service loaded active running Command Scheduler
data-transfer-appliance.service loaded active running Data Transfer Appliance
data-transfer-console.service loaded active running Data Transfer Serial Console

Any problem with the diagnostic data collection results in the console output being written to the log file of the service. Failure of the commands is indicative of a serious problem, perhaps requiring the return of the appliance. Here is an example of the log:

```
Mar 6 17:55:33 localhost console-diags: {"Module": "main", "Type": "Info", "Message": "Received message {"cmd": "collect"}"}
Mar 6 17:55:33 localhost console-diags: {"Module": "main", "Type": "Info", "Message": "Setting up output file. First to remove all /tmp/xa-diags-results"}
```

**Initializing Appliance Fails Because of IP Address Issues**

Initializing the Appliance can fail because of using the incorrect IP address. The IP address for `initialize-auth` can differ from the IP address obtained when running ping or ssl connect. If you experience an initialization failure, ensure that you are using the correct IP address for your Appliance and try initializing again.

**Initialize Authentication Fails with "connection refused" or "connection timed out"**

If you try to configure networking using the appliance serial console but fail with a "connection refused" or "connection timed out" message, follow these troubleshooting steps.

Run the following command at the command prompt on the host:

```
ping <appliance_ip>
```

If a failure occurs, run the following command to verify appliance IP and the path to appliance.

```
ping -I <local_interface> <appliance_ip>
```

To determine expected interface, run `ip route` or an equivalent command. Verify that routing table is sane. Try running `traceroute` if you’re not sure to see the network path to the appliance IP.
Run the following command:

```
curl -k https://<appliance_ip>
```

You should receive the response "Not found." This failure can indicate the IP address may be wrong. For example, nothing is listening on port 443. If you receive a failure message, run the following command:

```
openssl s_client -showcerts -connect <appliance_ip>:443
```

You should see a certificate issued for "Oracle Cloud Infrastructure" / "Data Transfer Appliance."

This command is similar to `curl` but does not use HTTPS and so proxies do not affect it. If this command works, and `curl` fails, then verify there are no proxy environmental variables.

**Dataset Sealing Process Fails**

The dataset sealing process can fail sometimes because there are special files in the dataset:

```
dts nfs-dataset seal-status --name nfs-ds-1
```

Seal Status:
- success : false
- failureReason :
Number of special files : 5
- startTime : 2019/03/26 11:52:37 PDT
- endTime : 2019/03/26 11:52:39 PDT
- numFilesToProcess : 0
- numFilesProcessed : 0
- bytesToProcess : 0.00 KB
- bytesProcessed : 0.00 KB

At the command prompt on the host, reactivate the NFS dataset.

```
ocli dts nfs-dataset activate --name <dataset_name>
```

Then run `find` to get the full list of all special files and the specific type of each one.

```
find <mountpoint> ! -type f ! -type d | xargs file
```

For example:

```
$ find /mnt/nfs-ds-1 ! -type f ! -type d | xargs file
/mnt/nfs-ds-1/myfile1: symbolic link to `/home/user1/myfile1'
/mnt/nfs-ds-1/myfile2: symbolic link to `/home/user1/myfile2'
```

Next, review the list and remove all special files from the NFS mount point.

```
find <mountpoint> ! -type f ! -type d | xargs rm
```

Deactivate the NFS dataset.

```
ocli dts nfs-dataset deactivate --name <dataset_name>
```

Finally, reseal the dataset.

```
ocli dts nfs-dataset seal --name <dataset_name> [--wait]
```

Monitor the seal progress. Wait for it to complete successfully and continue with the subsequent steps.
Special Characters in Names Cause Data Sealing Failures

Data sealing fails if the names of the files being transferred contain characters that are not UTF-8, contain a newline, or include a return. The error returned is similar to the following:

failureReason": "nNumber of file paths with invalid chars: 1

If this error occurs, activate the data set, mount it, and run the following find command on the filesystem:

```
find . -print0 | perl -n0e 'chomp; print $_, "\n" if /[[:^ascii:][:cntrl:]]/'
```

Rename or delete those files that appear in the returned list.

Disk-Based Data Transfers

These troubleshooting entries are associated with disk-based import jobs.

Data Transfer Utility Fails because of Lack of Exclusive Access to Disk

The Data Transfer Utility requires exclusive access to the disk. If you have any drivers that already claim exclusive access to the disk, then the Data Transfer Utility fails. For example, if you employ a devicemapper multipath driver over all your disk devices, you must first remove the disk used for the data transfer from the list of devices managed by the multipath driver.

Be sure that access to the disk is not done through any devicemapper or volume manager. During the data transfer, the expectation is that the file system is created on a "raw" device. Any layering or mapping through intermediate drivers or abstraction layers makes it impossible for the disk to be uploaded at the transfer site. The source of these failures can include drivers like multipath, md, striping, logical volume managers, and potentially others as well.

You can confirm that the Data Transfer Utility has exclusive access by attempting to manually format the disk being used for your data transfer. The Data Transfer Utility uses the `cryptsetup` utility to create an encrypted device.

You can run `cryptsetup` from the command line (root privileges required):

```
cryptsetup luksFormat -c aes-xts-plain64 -s 512 -h sha512 --iter-time 2000 --use-random /dev/<sdXX>
```

<sdXX> is the name of the disk being used for the data transfer.

When prompted, respond that you do want to encrypt the device. You are required to provide a passphrase. Any passphrase is acceptable as the `cryptsetup` utility can run on a disk repeatedly without any problems.

If the command succeeds, then you know that the Data Transfer Utility can gain exclusive ownership of the disk to do the necessary for the data transfer.

Data Transfer Utility Fails with "Processing exception..." While Communicating to Oracle Cloud Infrastructure

Check if your environment has proxies to the internet. If so, update them to the latest version and set "https_proxy." If you are using the appliance, set "no_proxy" environmental variables. See Installing the Data Transfer Utility on page 974 for more information on proxies.

Data Transfer Utility Fails with "invalid configuration file"

If you attempt to run Data Transfer commands and receive the error message "invalid configuration file," verify that the following files are present on your host and are correctly set up:

- ~/.oci/config
- ~/.oci/config_upload_user

Both files must have "[DEFAULT] " as the first line. Use of the "~" character in a path is not valid in the file's contents.
Creating Transfer Disk Fails Because of Serial Number Error

Creating a transfer disk using the Data Transfer can fail because of a serial number error:

dts disk create --job-id ocid1.datatransferjob.ocl..exampleuniqueID --block-device /dev/sdb
ERROR : Unable to determine serial number for device /dev/sdb

This error may result from a garbled serial number resulting from the `hdparm -I` command. For example:

```
/bin/sh -c "hdparm -I /dev/sdb"
/dev/sdb:
SG_IO: bad/missing sense data, sb[]: 70 00 05 00 00 00 00 0a 00 00 00 00 24
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ATA device, with non-removable media
Standards:
Likely used: 1
Configuration:
Logical max current
heads 0 0
sectors/track 0 0
-
Logical/Physical Sector size: 512 bytes
device size with M = 1024*1024: 0 MBytes
device size with M = 1000*1000: 0 MBytes
cache/buffer size = unknown
Capabilities:
IORDY not likely
Cannot perform double-word IO
R/W multiple sector transfer: not supported
DMA: not supported
PIO: pio0
```

If you see this type of error, use the following workaround:

1. Run the following command at the prompt:

```
lsblk --nodeps -no serial /dev/<device> <serial_number>
```

2. Create an `hdparm` script in your Home directory using the following command:

```
vi $HOME/hdparm
#!/usr/bin/bash
while getopts ":Iht" opt;do
case ${opt} in
h) # process option h
;;
t)
;;
I)
    echo "Serial Number: <serial_number>"
;;
esac
done
```

Use the same serial number in your script that was returned when you ran the `lsblk` command in the previous step.

3. Make the script you just created executable.
4. Change your path using the following command:

```bash
export PATH=/<home_dir_path>:PATH
```

5. Retry creating the transfer disk.

**Help Sheets**

Oracle provides a number of help sheets to print and carry with you as you perform your data transfer tasks.

**Disk Import**

- Disk Import Job Checklist
- Prepare for Disk Import Jobs
- Disk Import Procedures

**Appliance Import**

- Appliance Import Job Checklist
- Prepare for Appliance Import Job
- Appliance Import Procedures

**Help Sheet - Disk Import Job Checklist**

Use this checklist for preparing to use the transfer disk for use in an import job. Check each item in order to ensure you are fully prepared for the data transfer.

- USB 2.0/3.0 external hard disk drive.
- Someone tasked to create labels for the FedEx, UPS, or DHL carriers.
- Linux machine running Oracle Linux 6 or greater, Ubuntu 14.04 or greater, or SUSE 11 or greater.
- Users interacting with the Linux machine must have *root* access.
- Physical access to the Linux machine to connect the hard disk drive.
- Linux operating system can create an EXT file system.
- Java 1.8 or Java 1.11 installed on Linux machine.
- Hdfparm 9.0 or later installed on Linux machine.
- Cryptsetup 1.2.0. or greater installed on Linux machine.
- Open firewall for Linux machine to OCI Data Transfer Service on the IP address ranges: 140.91.0.0/16.
- Open firewall to OCI Object Storage IP address ranges: 134.70.0.0/17.
- Download and install the Data Transfer Utility.
- Install OCI Command Line Interface.
- Generate public/ private keys for users who will copy data on the Linux machine (run `oci setup keys` command)
- Administrative user on tenancy who can create users, groups, compartments, and add policies

**Help Sheet - Prepare for Disk Import Jobs**

Use this help sheet to preparing and running your disk import job.
Preparing

1. Ensure you have the following set up in your environment:
   - USB 2.0/3.0 external hard disk drive (disk) to be used as your import disk.
   - Computer running one of the following Linux operating systems:
     - Oracle Linux 6 or greater
     - Ubuntu 14.04 or greater
     - SUSE 11 or greater

   All Linux operating systems must have the ability to create an EXT file system. Make sure the system has the following installed:
     - Java 1.8 or Java 1.11
     - hdparm 9.0 or later
     - Cryptsetup 1.2.0 or greater

2. Download and install the Data Transfer Utility on the Linux machine where the data will be copied from and the disk will be mounted. You should have root access to this machine.

   Installation instructions are located at: https://docs.cloud.oracle.com/iaas/Content/DataTransfer/Tasks/disk_preparing.htm

3. Install OCI Command Line Interface on the Linux machine where the data will be copied from and the disk will be mounted. You should have root access to this Linux machine.

   Installation instructions are located at: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliinstall.htm

4. On the machine where data will be copied from generate public/private keys for the user(s) who will do the data copy, run the following command:

   `oci setup keys`

   See https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm for more information on keys.

5. Login to OCI with an Administrative user for the tenancy.

6. Create the user policies. Ensure that the policies include the following:

   `Allow group <group_name> to {DTA_ENTITLEMENT_CREATE} in tenancy`

   See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingpolicies.htm for more information on policies

7. Create a compartment where the transfer job and landing bucket will reside.

   See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm for more information on compartments.

8. Create the necessary user accounts for those individuals who will copy data to the disk. Include the public key that was previously generated.

   See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingusers.htm for more information on users.

   See https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm for more information on public keys.

9. Create a group for the user who will copy data to the disk. Include the following policies in the group:

   ```
   Allow group <group_name> to manage data-transfer-jobs in compartment <compartment_name>
   Allow group <group_name> to manage buckets in compartment <compartment_name>
   ```
Allow group <group_name> to manage objects in compartment <compartment_name>

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managinggroups.htm for more information on groups.

If you want to include notifications for the group, includes these additional policies:

- Allow group <group name> to manage ons-topics in tenancy
- Allow group <group name> to manage ons-subscriptions in tenancy
- Allow group <group name> to manage cloudevents-rules in tenancy
- Allow group <group name> to inspect compartments in tenancy

See https://docs.cloud.oracle.com/iaas/Content/Notification/Concepts/notificationoverview.htm for more information on notifications.

See https://docs.cloud.oracle.com/iaas/Content/Events/Concepts/eventsoverview.htm for more information on events.

10. Create an upload user for Oracle personnel to upload data into the bucket.

   See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingusers.htm for more information on users.

11. Create a group for the upload user, and include the public key that was previously generated.

   See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managinggroups.htm for more information on groups.

   See https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm for more information on public keys.

12. Add the following policies for the upload user group:

- Allow group <group_name> to manage buckets
  in compartment <compartment_name> where all
  
  - request.permission='BUCKET_READ', target.bucket.name='<bucket_name>'

- Allow group <group_name> to manage objects
  in compartment <compartment_name> where all
  
  - target.bucket.name='<bucket_name>', any
    
    - request.permission='OBJECT_CREATE',
    - request.permission='OBJECT_OVERWRITE',
    - request.permission='OBJECT_INSPECT'}

The permissions for upload users allow Oracle personnel to upload standard and multi-part objects on your behalf and inspect bucket and object metadata. The permissions do not allow Oracle personnel to inspect the actual data.

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingpolicies.htm for more information on policies.

13. Open firewall to OCI Data Transfer Service on the IP address ranges:

   140.91.0.0/16

14. Open firewall to OCI Object Storage IP address ranges:

   134.70.0.0/17

Creating the Transfer Job

Run these command line items on the host where you plan on mounting USB HDD and copying data and/or the host that you will use to manage the data transfer job:

1. As root, create the configuration files:

   ```
   sudo bash
   mkdir /root/.oci
   cd /root/.oci
   ```
vi config
[DEFAULT]
user=<The OCID for the data transfer administrator>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user's private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>

vi config_upload_user
[DEFAULT]
user=<The OCID for the data transfer upload user>
fingerprint=<The fingerprint of the above user's public key>
key_file=<The _absolute_ path to the above user's private key file on the host machine>
tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>
endpoint=https://objectstorage.<region information>.com

2. Get the tenancy namespace:
oci os ns get

3. Create a bucket in the compartment created for the transfer job
oci os bucket create --namespace <object_storage_namespace> --name <bucket name> --compartment-id <compartment_id>

4. Verify the data transfer upload user credentials:
dts job verify-upload-user-credentials --bucket <bucket_name>

5. Create the transfer job:
dts job create --bucket <bucket_name> --compartment-id <compartment_id> --display-name <display_name>

The job OCID is displayed in the Data Transfer Utility return after you create the job. Send this job OCID to the person who will copy data to the disk.

6. (Optional) Add notifications:
oci dts job setup-notifications --job-id <job_id>

7. Create a virtual representation of the physical shipping package for the disk called a transfer package:
dts package create --job-id <job_id>

8. Get the package label:
dts job show --job-id <job_id>

The package label is included in the Data Transfer Utility return. Send it to the person who will copy data to the disk.
9. Get the shipping address for the disk:

   dts package show --job-id <job_id> --package-label <package_label>

Shipping information is included in the Data Transfer Utility return. Send it to the person who will create the shipping labels.

10. Create a FedEx, UPS, or DHL shipping label for the disk using the address from above to ship the disk to Oracle. Send the carrier-provided tracking to the person who will copy data to the disk.

11. Create a return label for the disk and send it electronically or in person to the person who will ship the disk. Send the tracking number for the return label to the person who will copy data to the disk.

Help Sheet - Disk Import Procedures

Before Starting

Before starting, ensure the following:

- You have the following information available:
  - The disk transfer job OCID
  - The package label
  - The shipping vendor and tracking ID
  - The return shipping vendor and tracking ID
- You have root access to the Linux machine where the data will be copied
- The configuration files and Data Transfer Utility are already installed on the Linux machine where the data will be copied.

Attach and Create the Transfer Disk

To attach and create the transfer disk:

1. Physically attach the import disk to the Linux host where data will be copied.

   As part of this process, do the following:
   a. Run `lsblk` and verify you can see the device, take note of the device path as it will be needed in future steps
   b. Run `hdparm -I <device>` and verify the disk provides a valid response, particularly a readable serial number.

      The disk should have not have any partitions or filesystems. If it does, run:

       `wipefs -a /dev/<path>`

2. Use the Data Transfer Utility to create the transfer disk, it will also generate and display an encryption passphrase, create a unique mount point, and mount the disk:

   dts disk create --job-id <job_id> --block-device <block_device>

   The encryption passphrase will be displayed to output. Store it in a secure place as it will not be displayed or accessible again.

   Record the disk label from the output. You will need it later in the procedure.

   Verify there is a new mount point called `/mnt/orcdts_<disk_label>`
3. Copy files to the data transfer disk using the mount point from the previous step. We recommend the `tar` is recommended but you can use other types of copy methods such as `cp` or `rsync`.

Here are two examples:

```
• tar -cvzf /mnt/<disk_label>/filesystem.tgz filesystem/
• tar -cvzf /mnt/<disk_label>/filesystem.tgz filesystem/ | xargs -I '{}' sh -c "test -f '{}' \&\& md5sum '{}'" | tee tarzip_md5
```

You can only copy regular files to disks. Special files (links, sockets, pipes, and so forth) cannot be copied directly. To transfer special files, create a tar archive of the files and copy the tar archive to the disk.

Do not disconnect the disk until you copy all files from the Data Host and generate the manifest file. If you accidentally disconnect the disk before copying all files, you must unlock the disk using the encryption passphrase.

4. Generate a manifest file after all data has been copied to the disk:

```
dts disk manifest --job-id <job_id> --disk-label <disk_label>
```

The manifest file will be on the transfer disk.

5. Lock the transfer disk:

```
dts disk lock --job-id <job_id> --disk-label <disk_label> --block-device <block_device>
```

6. Attach the transfer disk to the transfer package:

```
dts disk attach --job-id <job_id> --package-label <package_label> --disk-label <disk_label>
```

7. Update the transfer package with the tracking information:

```
dts package ship --job-id <job_id> --package-label <package_label> --package-vendor <vendor_name> --tracking-number <tracking_number> --return-tracking-number <return_tracking_number>
```

8. Physically disconnect the disk from the Linux host.

9. Have the disk packaged, insert the printed return label, attach the shipping label to the outside of the package.

10. Pass the disk to the vendor to ship to Oracle

11. Monitor the status of the transfer package:

```
dts package show --job-id <job_id> --package-label <package_label>
```

12. Review the upload status after Oracle receives the disk and uploads your files.

13. Close the transfer job after the job is complete and the import disk is returned to you:

```
dts job close --job-id <job_id>
```

**Help Sheet - Appliance Import Job Checklist**

Use this checklist for preparing to use the Data Transfer Appliance (import appliance) for use in an import job. Check each item in order to ensure you are fully prepared for the data transfer.

- **Administrative user to the tenancy who can create users, groups, compartments, add policies, and request import appliance entitlement.**
- **Access to the main buyer or administrator who is VP-level or higher who can sign the terms and conditions document.**
Data Transfer

- Linux machine running Oracle Linux 6.10/7.3-7.5/8.0, Ubuntu 16.04/18.04, or CentOS 6.9/6.10/7.0.
- Root access for the prepare and copy on the Linux machine.
- Someone who has physical access to where the import appliance will be installed.
- Meet all appliance specifications and physical environment requirements.
- Terminal emulation host that can connect to the import appliance using USB or DB-9 serial cable.
- Terminal emulation host with one of the following installed: PuTTY for Windows, ZOC for OS X, PuTTY or Minicom for Linux.
- Network connection to the import appliance consisting of either a 10GBase-T: Standard RJ-45 or SFP+ with transceiver compatible with Intel X520NICS.
- IP address for the import appliance ________.
- Subnet mask length for the import appliance subnet ________.
- Default gateway for the import appliance network ________.
- NFS communication between the import appliance subnet and servers from where data will be copied
- HTTP Proxy information if your corporation uses an internet proxy ________.
- Open firewall for Linux machine for preparation and copying to OCI Data Transfer Service on the IP address ranges: 140.91.0.0/16.
- Open firewall for Linux machine for preparation and copying to OCI Object Storage IP address ranges: 134.70.0.0/17.
- Installation of OCI Command Line Interface.
- Generate public/private keys for users who will copy data on the Linux machine (run `oci setup keys` command).

Help Sheet - Prepare for Appliance Import Jobs

Use this help sheet to prepare and use your Data Transfer Appliance

Preparing

1. Install the OCI Command Line Interface on the Linux machine where the data will be copied from and the Data Transfer Appliance will be mounted. You should have root access to the Linux machine.
   
   Installation instructions are located at: https://docs.cloud.oracle.com/iaas/Content/API/SDKDocs/cliinstall.htm
   
   On the machine where data will be copied from generate public/private keys for the user(s) who will do the data copy, run the following command:

   ```
   oci setup keys
   ```
   
   See https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm for more information on keys.
   
2. Login to OCI with an Administrative user for the tenancy.

3. Create the user policies. Ensure that the policies include the following:

   ```
   Allow group <group_name> to (DTA_ENTITLEMENT_CREATE) in tenancy
   ```
   
   See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingpolicies.htm for more information on policies.
4. Create a compartment where the transfer job and landing bucket will reside. This compartment must be in a region that supports usage of the Data Transfer Appliance.

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm for more information on compartments.

5. Create the necessary user accounts for those individuals who will copy data to the appliance. Include the public key that was previously generated.

6. Create a group for the user who will copy data to the appliance. Include the following policies in the group:

```
Allow group <group_name> to manage data-transfer-jobs in compartment <compartment_name>
Allow group <group_name> to manage buckets in compartment <compartment_name>
Allow group <group_name> to manage objects in compartment <compartment_name>
```

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managinggroups.htm for more information on groups.

If you want to include notifications for the group, includes these additional policies:

```
Allow group <group_name> to manage ons-topics in tenancy
Allow group <group_name> to manage ons-subscriptions in tenancy
Allow group <group_name> to manage cloudevents-rules in tenancy
Allow group <group_name> to inspect compartments in tenancy
```

See https://docs.cloud.oracle.com/iaas/Content/Notification/Concepts/notificationoverview.htm for more information on notifications.

See https://docs.cloud.oracle.com/iaas/Content/Events/Concepts/eventsoverview.htm for more information on events.

7. Create an upload user for Oracle personnel to upload data into the bucket.

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingusers.htm for more information on users.

8. Create a group for the upload user, and include the public key that was previously generated.

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managinggroups.htm for more information on groups.

9. Add the following policies for the upload user group:

```
Allow group <group_name> to manage buckets
in compartment <compartment_name> where all
{ request.permission='BUCKET_READ', target.bucket.name='<bucket_name>' }
Allow group <group_name> to manage objects
in compartment <compartment_name> where all
{ target.bucket.name='<bucket_name>', any
{ request.permission='OBJECT_CREATE',
request.permission='OBJECT_OVERWRITE',
request.permission='OBJECT_INSPECT' }}
```

The permissions for upload users allow Oracle personnel to upload standard and multi-part objects on your behalf and inspect bucket and object metadata. The permissions do not allow Oracle personnel to inspect the actual data.

See https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingpolicies.htm for more information on policies.

10. Open firewall to OCI Data Transfer Service on the IP address ranges:

140.91.0.0/16

11. Open firewall to OCI Object Storage IP address ranges:

134.70.0.0/17
Creating the Transfer Job

Run these command line items on the host where you plan on mounting USB HDD and copying data and/or the host that you will use to manage the data transfer job:

1. As root, create the configuration files:

   ```bash
   sudo bash
   mkdir /root/.oci
   cd /root/.oci
   vi config
   [DEFAULT]
   user=<The OCID for the data transfer administrator>
   fingerprint=<The fingerprint of the above user's public key>
   key_file=<The _absolute_ path to the above user's private key file on the host machine>
   tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
   region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>
   vi config_upload_user
   [DEFAULT]
   user=<The OCID for the data transfer upload user>
   fingerprint=<The fingerprint of the above user's public key>
   key_file=<The _absolute_ path to the above user's private key file on the host machine>
   tenancy=<The OCID for the tenancy that owns the data transfer job and bucket>
   region=<The region where the transfer job and bucket should exist. Valid values are: us-ashburn-1, us-phoenix-1, eu-frankfurt-1, and uk-london-1.>
   endpoint=https://objectstorage.<region information>.com
   ```

2. Get the tenancy namespace:

   ```bash
   oci os ns get
   ```

3. Create a bucket in the compartment created for the transfer job:

   ```bash
   oci os bucket create -namespace <object_storage_namespace> --name <bucket_name> --compartment-id <compartment_id>
   ```

4. Verify the data transfer upload user credentials:

   ```bash
   dts job verify-upload-user-credentials --bucket <bucket_name>
   ```

5. Create the transfer job:

   ```bash
   oci dts job create --bucket <bucket_name> --compartment-id <compartment_id> --display-name <display_name>
   ```

   The job OCID is displayed in the CLI return after you create the job. Send this job OCID to the person who will copy data to the disk.

6. (Optional) Add notifications:

   ```bash
   oci dts job setup-notifications --job-id <job_id>
   ```

7. Request the appliance:

   ```bash
   oci dts appliance request --job-id <job_id> --addressee <addressee> --care-of <care_of> --address1 <address_line1> --
Help Sheet - Appliance Import Procedures

Follow the tasks in this help sheet after you login to the host where you will be mounting the Data Transfer Appliance (import appliance) and copying data. You need to run all Command Line Interface (CLI) tasks as sudo.

• Make sure you have the IP address for the import appliance.
• Make sure you have the access token for the import appliance.
• Have the transfer job OCID.
• Have the appliance label information.
• Make sure there is no firewall and communication is open between the import appliance the host where it will be mounted.
• Open firewall to OCI Data Transfer Service on the IP address ranges: 140.91.0.0/16.
• Open firewall to OCI Object Storage IP address ranges: 134.70.0.0/17.
• Set the environment variable If HTTP proxy environment is needed to allow access to the internet. The proxy environment allows Oracle Cloud Infrastructure CLI to communicate with the Data Transfer Appliance Management Service and the import appliance over a local network connection.

    export HTTPS_PROXY=http://www-proxy.myorg.com:80

• Go to root as sudo and install NFS utilities if they are not already installed (first command for RHEL, OEL and second command for Debian, Ubuntu):

    sudo yum install nfs-utils
    sudo apt-get install nfs-common

• Continue as root.
• Initialize the appliance. Have the import appliance access token ready.

    oci dts physical-appliance initialize-authentication --job-id <job_id> --appliance-cert-fingerprint <fingerprint> --appliance-ip <appliance_ip> --appliance-label <appliance_label>

When prompted, supply the access token, and answer y to permit overwriting of data.

• Configure the import appliance encryption:

    oci dts physical-appliance configure-encryption --job-id <job_id> --appliance-label <appliance_label>

Note the appliance label in the output (the label will begin with "XA"). You will need to this label value for other commands involving the appliance.

To include job notifications when requesting an import appliance, include the --setup-notifications option:

    oci dts appliance request --job-id <job_id> --addressee <addressee> --address1 <address_line1> --city-or-locality <city_or_locality> --state-or-region <state_or_region> --country <country> --zip-postal-code <zip_postal_code> ...
    --setup-notifications

If you have already made your appliance request without including notifications, but subsequently want to include them, run the following:

    oci dts appliance setup-notifications --appliance-label <appliance_label>
- Unlock the import appliance:

```
oci dts physical-appliance unlock --job-id <job_id> --appliance-label <appliance_label>
```

- Create an NFS dataset:

```
oci dts nfs-dataset create --name <dataset_name>
```

- Export the dataset:

```
oci dts nfs-dataset set-export --name <dataset_name> --rw true --world true
```

- Activate the dataset:

```
oci dts nfs-dataset activate --name <dataset_name>
```

- Check the dataset is exported:

```
showmount -e <appliance_IP>
```

- Mount the dataset:

```
mkdir -p /mnt/<mountpoint_name>
oci dts nfs-dataset activate --name <dataset_name>
```

- Copy files to the DTA. The `tar` method is recommended but other types of copies such as `cp` or `rsync` can also be used.

Here are two examples:

- `tar -cvzf /mnt/nfs-dts-1/filesystem.tgz filesystem/`

- `tar cvzf /mnt/nfs-dts-1/filesystem.tgz filesystem/ | xargs -I '{}' sh -c "test -f '{}' && md5sum '{}"" | tee tarzip_md5`

- Deactivate the dataset:

```
oci dts nfs-dataset deactivate --name <dataset_name>
```

- Seal the dataset. Note this can be a long running process.

```
oci dts nfs-dataset seal --name <dataset_name> [--wait]
```

- Monitor the sealing process:

```
oci dts nfs-dataset seal-status --name <dataset_name>
```

- Download the dataset seal manifest:

```
oci dts nfs-dataset get-seal-manifest --name <dataset_name> --output-file <file_path>
```

- Finalize the import appliance:

```
oci dts physical-appliance finalize --job-id <job_id> --appliance-label <appliance_label>
```

- Shut down the import appliance by selecting option #8 on the terminal emulation host.
- Have the import appliance packed and shipped to Oracle.
• Monitor the status of the data upload from the DTA to your object storage bucket in OCI:

```bash
oci dts appliance show --job-id <job_id> --appliance-label <appliance_label>
```

• Once the data upload is finished, check the object storage bucket from the Console and get the upload file location

• Download the upload file and review them to understand what was transferred:

```bash
oci os object get --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --file <file_location>
```

• Close the import job:

```bash
oci dts job close --job-id <job_id>
```

• Delete the import appliance associated with the import job:

```bash
oci dts appliance delete --job-id <job_id> --appliance-label <appliance_label>
```

• Delete the transfer job:

```bash
oci dts job delete --job-id <job_id>
```
This chapter explains how to launch a DB System and manage databases on DB Systems.

**Overview of the Database Service**

The Database service offers autonomous and co-managed Oracle Database cloud solutions. Autonomous databases are preconfigured, fully-managed environments that are suitable for either transaction processing or for data warehouse workloads. Co-managed solutions are bare metal, virtual machine, and Exadata DB systems that you can customize with the resources and settings that meet your needs.

You can quickly provision an autonomous database or co-managed DB system. You have full access to the features and operations available with the database, but Oracle owns and manages the infrastructure.

You can also extend co-managed database services into your data center by using Exadata Cloud@Customer, which applies the combined power of Exadata and Oracle Cloud Infrastructure while enabling you to meet your organization's data-residency requirements.

For details about each offering, start with the following overview topics:

**Autonomous Databases**

The Database service offers Oracle's Autonomous Database with transaction processing and data warehouse workload types.

**Co-managed Systems**

- Bare Metal and Virtual Machine DB Systems on page 1352
- Exadata Cloud Service on page 1221
- Exadata Cloud@Customer

**Note:**

For information about MySQL Database, see MySQL Database.

**License Types and Bring Your Own License (BYOL) Availability**

**Database Service License Options**

Oracle Cloud Infrastructure supports a licensing model with two license types. With License included, the cost of the cloud service includes a license for the Database service. With Bring Your Own License (BYOL), Oracle Database customers can use existing licenses with Oracle Cloud Infrastructure. Note that Oracle Database customers remain responsible for complying with license restrictions applicable to their BYOL licenses, as defined in their program order for those licenses.

You do not need separate on-premises licenses and cloud licenses. BYOL databases support all advanced Database service manageability functionality, including backing up and restoring a DB system, patching, and Oracle Data Guard.
You can choose BYOL when you launch a cloud-hosted Oracle Cloud Infrastructure database or DB system. Choosing BYOL impacts how the usage data for the instance is metered and subsequent billing. You can also switch license types after provisioning.

Note that on some provisioning dialogs in the Console, the BYOL option is labeled **My Organization Already Owns Oracle Database Software Licenses**.

For additional information about license pricing and features, see Oracle Cloud Database Services. For guidelines on using Oracle Database licenses, see Database Licensing.

**Switching Database Service License Types**

You can switch license type after provisioning your resource. For information about switching the license type, see the following:

- To change the license type of an Autonomous Database on page 1172
- To change the license type of an Exadata Cloud Service cloud VM cluster or DB system on page 1261
- To change the license type of a bare metal or virtual machine DB system on page 1387

**Always Free Database Resources**

The Database service is one of the Oracle Cloud Infrastructure services that provides you with Always Free resources as a part of Oracle's Free Tier. For an introduction to the Free Tier, see Oracle Cloud Infrastructure Free Tier on page 140. For details about the Always Free Autonomous Database, see Always Free Availability on page 1149 in the Autonomous Database overview topic. To provision an Always Free Autonomous Database, see To create an Always Free Autonomous Database on page 1159.

**Moving Database Resources to a Different Compartment**

You can move DB systems, Autonomous Database resources, and Exadata Cloud@Customer resources from one compartment to another. When you move a Database resource to a new compartment, its dependent resources move with it. After you move the resource to the new compartment, inherent policies apply immediately and affect access to that resource and its dependent resources through the Console.

**Important:**

- To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Database resources, see Details for the Database Service on page 2240.
- If your database resource is in a security zone compartment, the destination compartment must also be in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

**Dependent Resource Details**

Details about dependent resources are as follows:

- **Bare metal, virtual machine, and Exadata DB systems**: Dependent resources that move with these DB systems include Database Homes and databases, as well as the metadata for automatic backups. To verify the compartment of a dependent resource, check the compartment of the DB system.
- **Autonomous Database**: Autonomous Database dependent resources are limited to its automatic backups. Autonomous Exadata Infrastructure instances and Autonomous Container Databases have no dependent resources that move with them. Associated (non-dependent) resources remain in their current compartments.
- **Exadata Cloud@Customer**: Resources that can be moved are Exadata Infrastructure, VM clusters, and backup destinations. VM cluster networks are dependent resources of Exadata Infrastructure instances, so they move with
them. VM clusters have the following dependent resources: Database Homes, and databases and their automatic backups. Backup destinations have no dependent resources.

For more information about moving resources to other compartments, see To move a resource to a different compartment on page 2444.

**Monitoring Resources**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about available Database service metrics and how to view them, see Database Metrics on page 1578.

**Creating Automation with Events**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

See Database on page 1843 for details about Database resources that emit events.

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For more information on tenancies and compartments, see Key Concepts and Terminology in the Oracle Cloud Infrastructure Getting Started Guide. For general information about using the API, see REST APIs on page 4368. For information on deprecated Database Service APIs, see Deprecated Database Service APIs on page 1672.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to write policies that provide stricter access to database resources, see Details for the Database Service on page 2240.

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.
If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For common policies used to authorize Oracle Cloud Infrastructure Database users, see Common Policies.

For in-depth information on granting users permissions for the Database service, see Details for the Database Service in the IAM policy reference.

Security Zone Integration

A security zone is associated with a compartments and a set of policies called a security zone recipe. When you create and update resources in a security zone, Oracle Cloud Infrastructure validates these operations against the list of policies defined in the security zone recipe. If any security zone policy is violated, then the operation is denied.

The Database service allows you to create and update your databases and associated resources in security zones. For a general overview of the security zones, see the Security Zone documentation. For an overview of the Database service's integration with the security zone feature, see Security Zone Integration on page 1574.

Limits on the Database Service

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Note:

Service limits and compartment quotas do not apply to Exadata Cloud@Customer.

Many Database API operations are subject to throttling.

Work Requests Integration

The Database service is integrated with the Oracle Cloud Infrastructure Work Requests API. Work requests allow you to monitor long-running operations such as the provisioning of DB systems. A work request is an activity log that enables you to track each step in the operation's progress. Each work request has an OCID that allows you to interact with it programmatically and use it for automation.

For general information on using work requests in Oracle Cloud Infrastructure, see Work Requests on page 258 and the Work Requests API. See Database Service Work Requests Reference on page 1143 for a listing of Database service operations that create work requests.

Database Service Work Requests Reference

This topic lists the Database service operations generate work requests. For general information on using work requests in Oracle Cloud Infrastructure, see Work Requests on page 258 and the Work Requests API.

Autonomous Database on Shared Exadata Infrastructure

Lifecycle operations:

- Create
- Delete
- Start
- Restart
- Stop
- Restore

Database management operations:

- Scale
• Rename
• Reset password
• Update license type
• Update workload type
• Update open mode / permission level (*read-only/read-write, and admin only/all users*)
• Upgrade version
• Update tags
• Change compartment
• Rotate instance wallet
• Rotate regional wallet

*Network access operations:*
• Update network ACL (*public endpoint only*)
• Update network security group (NSG) (*private endpoint only*)
• Update private endpoint

*Backup operations:*
• Create backup
• Delete backup

*Refreshable clone operations:*
• Manual refresh
• Disconnect refreshable clone
• Update refreshable lag time

*Autonomous Data Guard operations:*
• Enable Data Guard
• Disable Data Guard
• Failover
• Switchover

*Associated services operations:*
• Register with Data Safe
• Deregister with Data Safe
• Enable Operations Insights
• Disable Operations Insights

**Autonomous Database on Dedicated Exadata Infrastructure**

*Database lifecycle operations:*
• Create
• Update
• Delete
• Start
• Restart
• Stop
• Restore

*Backup operations:*
• Create backup
• Delete backup

*Container database operations:*
- Create
- Delete
- Update
- Restart
- Rotate container database encryption key
- Rotate database encryption key

*Infrastructure resource operations:*
- Create
- Terminate
- Update

*Autonomous Data Guard operations:*
- Setup Data Guard
- Failover Autonomous Container Database
- Switchover Autonomous Container Database
- Reinstate Autonomous Container Database

*Associated services operations:*
- Register with Data Safe
- Deregister with Data Safe

**Exadata Cloud Service, Virtual Machine DB Systems, and Bare Metal DB Systems**

**DB systems (Exadata, bare metal, and virtual machine)**

*Lifecycle operations:*
- Create
- Create from backup
- Update
- Terminate

*DB system management operations:*
- Change compartment
- Scale storage
- Scale CPU
- Add SSH key
- Update license type
- Configure IORM
- Update shape
- Apply FIPS security

*Maintenance operations:*
- Precheck system for patching
- Patch system
- Upgrade database
- Install DB system component
- Switch to the new exadata API and user experience

**Note:**

Virtual machine DB systems have a single database that is created and terminated as part of the creation or termination of the parent DB system.
**Cloud Exadata infrastructure operations (new resource model)**
- Create
- Update
- Scale (*flexible shape systems only*)
- Delete
- Change compartment

**Exadata Cloud VM cluster operations**

*Lifecycle operations:*
- Create
- Delete

*Management operations:*
- Change compartment
- Scale CPU
- Add SSH key
- Update license type
- Scale compute (*flexible shape systems only*)
- Scale storage (*flexible shape systems only*)

*Maintenance operations:*
- Precheck for grid infrastructure (GI) patch
- Apply GI patch
- Precheck for grid infrastructure (GI) upgrade
- Upgrade grid infrastructure (GI)
- Upgrade database
- Precheck for OS update
- Apply OS update

**Database Homes: Exadata, Virtual Machine, and Bare Metal Cloud Service Instances**

*Lifecycle operations:*
- Create
- Delete

*Maintenance operations:*
- Patch
- One-off Patch

**Database Nodes: Exadata, Virtual Machine, and Bare Metal Cloud Service Instances**

- Start
- Stop
- Reboot

**Virtual Machines: Exadata Cloud Service (New Infrastructure Resource Model only)**

- Start
- Stop
- Reboot
- Precheck customer-managed (Vault service) database key
Migrate customer-managed (Vault service) database key
Rotates customer-managed (Vault service) database key

**Databases: Exadata, Virtual Machine, and Bare Metal Cloud Service Instances**

*Lifecycle operations:*
- Create
- Update
- Restore
- Delete

*Maintenance operations:*
- Upgrade database
- Rollback database upgrade

*Note:*
Virtual machine DB systems have a single database that is created and terminated as part of the creation or termination of the parent DB system

**Database Backups: Exadata, Virtual Machine, and Bare Metal Cloud Service Instances**

Create
Delete

**Data Guard: Exadata, Virtual Machine, and Bare Metal Cloud Service Instances**

Create Data Guard
Delete Data Guard
Switch over Data Guard
Fail over Data Guard
Reinstate Data Guard

**Exadata Cloud Service Instances (New Infrastructure Resource Model)**

**Cloud Exadata infrastructure operations**

*Lifecycle operations:*
- Create
- Update
- Delete

*Management operations:*
- Scale (flexible shape systems only)
- Change compartment

**Cloud VM cluster operations**

*Lifecycle operations:*
- Create
- Delete

*Management operations:*
- Change compartment
• Scale CPU
• Add SSH key
• Update license type
• Scale compute \textit{(flexible shape systems only)}
• Scale storage \textit{(flexible shape systems only)}

\textit{Maintenance operations:}
• Precheck for grid infrastructure (GI) patch
• Apply grid infrastructure (GI) Patch
• Precheck for grid infrastructure (GI) upgrade
• Upgrade grid infrastructure (GI)
• Precheck for OS update
• Apply OS update

\textbf{Exadata Cloud@Customer Systems}

\textit{Exadata Cloud@Customer infrastructure operations:}
• Create
• Update
• Activate
• Delete

\textit{Exadata Cloud@Customer VM cluster operations:}
• Create
• Update
• Delete
• Change compartment

\textit{Exadata Cloud@Customer Autonomous VM cluster operations:}
• Create
• Update
• Delete
• Change compartment

\textit{Exadata Cloud@Customer VM cluster network operations:}
• Create
• Update
• Validate
• Delete

\textit{Additional maintenance and management operations:}
• Update VM cluster licence type
• Patch VM cluster
• Patch VM cluster database
• Update VM cluster OCPU count
• Update SSH key
• Update VM cluster memory
• Update VM cluster Exadata storage
• Update VM cluster local storage
• Update Exadata database backup configuration
Databases Software Images

- Creating a Database Software Image
- Deleting a Database Software Image
- Moving a Database Software Image to a new compartment

Getting Oracle Support Help for Your Database Resources

You can open a My Oracle Support ticket for individual Database resources while viewing them in the Oracle Cloud Infrastructure Console. For more information, see Getting Help and Contacting Support on page 125.

Overview of Autonomous Databases

Oracle Cloud Infrastructure's Autonomous Database is a fully-managed, preconfigured database environment with three workload types available, Autonomous Transaction Processing, Autonomous Data Warehouse and Autonomous JSON Database. You do not need to configure or manage any hardware or install any software. After provisioning, you can scale the number of CPU cores or the storage capacity of the database at any time without impacting availability or performance. Autonomous Database handles creating the database, as well as the following maintenance tasks:

- Backing up the database
- Patching the database
- Upgrading the database
- Tuning the database

Always Free Availability

Autonomous Database can be used without charge as part of Oracle Cloud Infrastructure's suite of Always Free resources. Users of both paid and free Oracle Cloud Infrastructure accounts have access to two Always Free instances of Autonomous Database. Always Free Autonomous Databases have a fixed 8 GB of memory, 20 GB of storage, 1 OCPU, and can be configured for either Autonomous Transaction Processing or Autonomous Data Warehouse workloads.

Always Free databases have only single available version. You can see the version that is being used for your database in the details screen. After a newer Oracle Database version is available in Oracle Cloud Infrastructure, your database will be automatically upgraded during one of your database's upcoming maintenance windows.

To learn about Free Tier Databases, see Oracle Cloud Infrastructure Free Tier on page 140. To learn about the details of the Always Free Autonomous Database, see Overview of the Always Free Autonomous Database on page 1220. To provision an Always Free Autonomous Database, see Creating an Autonomous Database on Shared Exadata Infrastructure on page 1157.

For information on regional availability of Always Free Autonomous Database, see the "Always Free Cloud Services" section of Data Regions for Platform and Infrastructure Services.

Available Workload Types

Autonomous Database offers the following workload types:

- **Autonomous Data Warehouse**: Built for decision support and data warehouse workloads. Offers fast queries over large volumes of data.
  
  For a complete product overview of Autonomous Data Warehouse, see Autonomous Data Warehouse. For Autonomous Data Warehouse tutorials, see Quick Start tutorials.

  
  Autonomous JSON Database is Oracle Autonomous Transaction Processing, but specialized for developing NoSQL-style applications that use JavaScript Object Notation (JSON) documents. You can upgrade an
Autonomous JSON Database service to an Autonomous Transaction Processing service if you need the additional functionality of Autonomous Transaction Processing. Currently available on shared Exadata infrastructure.

For a complete product overview of Autonomous JSON Database, see Using Oracle Autonomous JSON Database. Also available in the Oracle Help Center are Autonomous JSON Database tutorials and the JSON Developer's Guide.

- **Autonomous Transaction Processing**: Built for transactional workloads. Offers high concurrency for short-running queries and transactions.

  For a complete product overview of Autonomous Transaction Processing, see Autonomous Transaction Processing. For Autonomous Transaction Processing tutorials, see Quick Start tutorials.

- **Oracle APEX Application Development (APEX Service)**: Optimized for application developers, who want a transaction processing database for application development using Oracle APEX, that enables creation and deployment of low-code applications, including databases. See Oracle APEX Application Development Documentation for more information about the APEX service and Oracle APEX Application Development Specific Limitations for a list of use restrictions.

  **Note:**
  You can use the APEX service with each of the other workload types.

**Infrastructure Options**

Autonomous Databases have the following Exadata infrastructure options:

- **Dedicated Exadata Infrastructure**: With this option, you have exclusive use of the Exadata hardware. Dedicated Exadata infrastructure offers multitenant database architecture, allowing you to create and manage multiple Autonomous Databases within a single database system. Both workload types (transaction processing and warehouse) can be provisioned on dedicated Exadata infrastructure. You have the following hardware configuration options:
  - **System Models**: X7 and X8
  - **Configurations**: quarter rack, half rack, and full rack

  See Overview of Autonomous Database on Dedicated Exadata Infrastructure on page 1193 for more information about dedicated Exadata infrastructure architecture, features, and hardware specifications.

- **Shared Exadata Infrastructure**: With this option, you provision and manage only the Autonomous Database, while Oracle deploys and manages the Exadata infrastructure. Both workload types (transaction processing and warehouse) can be provisioned with shared Exadata infrastructure.

**Oracle Data Guard for Autonomous Databases with Shared Exadata Infrastructure**

Autonomous Database uses a feature called Autonomous Data Guard to enable a standby (peer) database to provide data protection and disaster recovery for Autonomous Databases using shared Exadata infrastructure. For more information, see Using a Standby Database with Autonomous Database.

**Per-Second Billing Billing for Autonomous Database Resources**

**Shared Exadata Infrastructure**

Autonomous Database on Shared Exadata infrastructure uses per-second billing. This means that OCPU and storage usage is billed by the second. OCPU resources have a minimum usage period of 1 minute.

**Dedicated Exadata Infrastructure**

For each Autonomous Exadata Infrastructure instance you provision, you are billed for the infrastructure for a minimum of 48 hours, and then by the second after that. Each OCPU you add to the system is billed by the second, with a minimum usage period of 1 minute.
Private Endpoint for Autonomous Databases with Shared Exadata Infrastructure

When you provision an Autonomous Database with Shared Exadata infrastructure, you can configure the network access so that the database uses a private endpoint within one of your tenancy's virtual cloud networks (VCNs). When you use a private endpoint, your database is only accessible via the IP address of the associated private endpoint. For more information, see Autonomous Database with Private Endpoint on page 1163.

CPU Scaling

You can manually scale the database's base number of CPU cores up or down at any time. Note the following:

- CPU scaling does not require any downtime.
- CPU utilization information is available for all Autonomous Databases on the database details page in the Metrics section. CPU utilization is reported as a percentage of available CPUs, aggregated across all consumer groups.

For databases using Shared Exadata infrastructure, you can also view hourly snapshots of the database's CPU usage (actual number of cores allocated) over the most recent 8 days. This information is available in the Service Console, in the Overview page graph "Number of OCPUs Allocated". For more information, see To view OCPU allocation hourly snapshot data for an Autonomous Database on page 1171.

Autonomous Database's auto scaling feature allows your database to use up to three times the current base number of CPU cores at any time. As demand increases, auto scaling automatically increases the number of cores in use. Likewise, as demand drops, auto scaling automatically decreases the number of cores in use. Scaling takes place without any lag time, and you are only billed for your actual average CPU core usage per hour. Note the following points regarding the auto scaling feature:

- Auto scaling is enabled by default and can be enabled or disabled at any time.
- The auto scaling status for a database (enabled or disabled) is displayed on the database details page.
- The base number of OCPU cores allocated to a database is guaranteed. For databases on dedicated Exadata infrastructure, the maximum number of cores available to a database depends on the total number of cores available in the Exadata infrastructure instance, and is further limited by the number of free cores that aren't being used by other auto scaling databases to meet high-load demands. Available OCPU cores are enabled on a "first come, first served basis" for autoscaling databases sharing an Autonomous Exadata Infrastructure instance.

The following table illustrates OCPU core availability for a single database on an X8 quarter rack dedicated Exadata infrastructure instance. As you increase the database's base core count from 1 to 40 cores, the maximum core count scales until it reaches the hardware limit of 100 OCPUs. The final column, which shows the remaining available OCPUs that can be allocated to additional databases, assumes that no other databases exist on the quarter rack instance.

Example: OCPU auto scaling for a single database on an X8 quarter rack as base OCPU is increased

<table>
<thead>
<tr>
<th>Base OCPU core count</th>
<th>Maximum OCPU core count</th>
<th>OCPU cores remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>99</td>
</tr>
<tr>
<td>8</td>
<td>24</td>
<td>92</td>
</tr>
<tr>
<td>32</td>
<td>96</td>
<td>68</td>
</tr>
<tr>
<td>40</td>
<td>100</td>
<td>60</td>
</tr>
</tbody>
</table>

The following table illustrates OCPU core availability for four databases on an X8 half rack dedicated Exadata infrastructure instance. The hardware limit is 200 OCPUs. The Base OCPU count for each database is guaranteed to be available to the database at all times. In the example, the three database with auto scaling enabled are in contention for the 60 available cores that are not allocated to any database as base cores. Databases Sales and Development each auto scaled to take a combined 140 OCPU, and database Chicago (with auto scaling disabled) is using its 10 base OCPU. That leaves only 50 OCPU remaining in the half rack hardware instance, and the base OCPU of database HR is 50. Therefore, database HR cannot auto scale up until cores are released by the other auto scaling databases.

Example: OCPU auto scaling for four databases on an X8 half rack
Storage Scaling

Autonomous Database allows you to scale the storage capacity of the database at any time without impacting availability or performance.

Performance Monitoring using Oracle Performance Hub

You can monitor and analyze the performance of an Autonomous Database in the Oracle Cloud Infrastructure Console using the Performance Hub ASH Analytics, SQL Monitoring, Workload, Blocking Sessions, and ADDM features.

- The Blocking Sessions feature provides information about blocking and waiting sessions for a selected Autonomous Database, includes procedures to display detailed information about the sessions, and explains how to kill sessions as needed.
- The ADDM feature displays findings and recommendations for performance problems.

Detailed information about these features and how to use them is located in Using Performance Hub to Analyze Database Performance on page 1597.

Operations Insights

Operations Insights is a cloud-native service that enables users to make informed, data-driven, Oracle Autonomous database resource and performance management decisions. See To enable or disable Operations Insights on an Autonomous Database on page 1174 for information about managing Operations Insights.

Oracle Database Preview Version Availability

Oracle Cloud Infrastructure periodically offers Autonomous Database preview versions of Oracle Database for testing purposes. You can provision an Autonomous Database using preview version software to test applications before the general availability of the software in Autonomous Database. Oracle will notify Autonomous Database customers when preview versions are available. Preview version software is available for a limited time. Databases provisioned with preview version software will display the end date of the preview period at the top of the database details page in the Console. If you are using the Console, you can also see the end date of the preview period in the Create Database provisioning dialog before the database is created.

Preview version software should not be used for production databases or for databases that need to persist beyond the limited preview period. Note that preview databases and their associated resources (including backups) are terminated automatically at the conclusion of the preview period. Oracle will notify customers prior to the conclusion of the preview period regarding the end date of the preview.

Any existing Autonomous Database (including those provisioned with preview version software) can be cloned using a preview version of Autonomous Database. However, preview version databases cannot be cloned using the regular (general-availability) Autonomous Database software.

See Creating an Autonomous Database on Shared Exadata Infrastructure on page 1157 for details on provisioning a preview version of Autonomous Database.
Oracle Database Versions for Autonomous Database with Shared Exadata Infrastructure

Depending on the region where you provision or clone your database, Autonomous Database supports one or more Oracle Database versions.

When multiple database versions are available, you choose an Oracle Database version when you provision or clone a database.

Note:
Always Free Autonomous Databases can be provisioned with either version 19c or version 21c, depending on the region. Most regions offer both versions. Note that Always Free Autonomous Databases can only be provisioned in the home region of your tenancy or account. See Overview of the Always Free Autonomous Database on page 1220 for more information.

Upgrading a Database

Autonomous Database instances currently use Oracle Database 19c. There is no database software upgrade currently available.

Regional Availability

Autonomous Database is currently available in all regions of the commercial realm. Autonomous Database is currently not available in regions within the Government Cloud realm.

Security Considerations

Safeguard Your Data with Data Safe on Autonomous Database

Oracle Data Safe is a fully-integrated, regional Cloud service providing features that help you protect sensitive and regulated data in your Autonomous Transaction Processing database. See the Data Safe documentation for more information.

Private Access Using a Service Gateway

Autonomous Database is one of the Oracle Cloud Infrastructure services that can be privately accessed through a service gateway within a VCN. This means you do not need a public IP or NAT to access your Autonomous Database instance from any of the cloud services within the Oracle Services Network. For example, if you have a Compute instance that uses a VCN with a service gateway, you can route traffic between your Compute instance and an Autonomous Database in the same region without the traffic going over the internet. For information on setting up a VCN service gateway and configuring it to access all supported Oracle Service Network services (which include Autonomous Database), see Access to Oracle Services: Service Gateway on page 3256.

Access Control Lists (ACLs) for Databases on Shared Exadata Infrastructure

For Autonomous Databases on shared Exadata infrastructure, an access control list (ACL) provides additional protection for your database by allowing only specified IP addresses and VCNs in the list to connect to the database. Specified IP addresses can include private IP addresses from your on-premises network that connect to your database using transit routing and allow traffic to move directly from your on-premises network to your Autonomous Database without going over the internet. See Transit Routing: Private Access to Oracle Services on page 2803 for more information on this method of access.

You can add the following to your ACL:

- Public IP addresses (individually, or in CIDR blocks)
- An entire VCN (specified by OCID)
- Private IP addresses within a specified VCN (individually, or in CIDR blocks)
- Private IP addresses within an on-premises network that have access using a transit routing
You can create an ACL during database provisioning, or at any time thereafter. You can also edit an ACL at any time. Removing all entries from the list makes the database accessible to all clients with the applicable credentials. See To manage the access control list of an Autonomous Database on shared Exadata infrastructure on page 1176 to learn how to create, update, or delete an ACL.

**Important:**

If you want to only allow connections coming through a service gateway you need to use the IP address of the service gateway in your ACL definition. To do this you need to add an ACL rule using the CIDR source type and the value 240.0.0.0/4. Note that this is not recommended. Instead, you can specify individual VCNs in your ACL definition for the VCNs you want to allow access from. See Access to Oracle Services: Service Gateway on page 3256 for more information.

Note the following about using an ACL with your Autonomous Database:

- When you restore a database the existing ACLs are not overwritten by the restore.
- The network ACL applies to the database connections and Oracle Machine Learning notebooks. If an ACL is defined and you try to login to Oracle Machine Learning from a client whose IP is not specified on the ACL you will see a "login rejected based on access control list set by the administrator" error.
- Oracle Application Express (APEX), RESTful services, and Oracle Database Actions are subject to ACLs. You can create rules specifying Virtual Cloud Networks, Virtual Cloud Network OCIDs, IP addresses, or CIDR blocks to control access to these tools.
- The Autonomous Database Service console is not subject to ACL rules.
- If you have a private subnet in your VCN that is configured to access the public internet through an NAT gateway, you need to enter the public IP address of the NAT gateway in your ACL definition. Clients in the private subnet do not have public IP addresses. See NAT Gateway on page 3247 for more information.

**Network Security Groups for Databases Resources That Use Private Endpoints**

Network security groups (NSGs) are an optional Networking security feature available for dedicated Exadata infrastructure and databases on shared Exadata infrastructure that use private endpoints. NSGs act as a virtual firewall for your Autonomous Database resources. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice within a single VCN. For more information, see the following topics:

- Network Security Groups on page 2841
- NSG security rule guidelines for private endpoint on page 1163
- To edit the network security groups (NSGs) for your Autonomous Exadata Infrastructure resource on page 1204
- To update the network configuration of an Autonomous Database on shared Exadata infrastructure that uses a private endpoint on page 1177

**Automatic Maintenance**

For Autonomous Databases on shared Exadata infrastructure, Oracle manages the automatic maintenance. You can view the next scheduled maintenance in the Console on the details page for your Autonomous Database. For Autonomous Databases on dedicated Exadata infrastructure, see Overview of Dedicated Exadata Infrastructure Maintenance on page 1196.

**Development and Administration Tools**

Oracle's Database Actions, Application Express (APEX), and Machine Learning applications are available for Autonomous Databases. For information on how to use these applications and access them from the Console, see Autonomous Database Tools on page 1216.

**Compartment Quotas for Autonomous Databases**

You can use compartment quotas to control how Autonomous Database OCPU and storage resources are allocated to Oracle Cloud Infrastructure compartments. You can use compartment quota policy statements to control
OCPU and storage resources by both workload type and Exadata infrastructure type. For example, you can allocate 10 Autonomous Transaction Processing OCPUs on shared Exadata infrastructure to a specific compartment. This would not affect the number of OCPUs available to Autonomous Data Warehouse databases, or databases using dedicated Exadata infrastructure. For more information on using compartment quotas, see Compartment Quotas on page 243 and Database Quotas on page 252.

Using the Oracle Cloud Infrastructure Console to Manage Autonomous Databases

For information on provisioning, managing, and backing up an Autonomous Database in the Oracle Cloud Infrastructure Console, see the following topics:

- Creating an Autonomous Database on Shared Exadata Infrastructure on page 1157
- Managing an Autonomous Database on page 1169
- Connecting to an Autonomous Database on page 1181
- Backing Up an Autonomous Database Manually on page 1184
- Restoring an Autonomous Database on page 1187

Additional Autonomous Database Product Information

Autonomous Database on Shared Exadata Infrastructure

For in-depth documentation on using and managing your Autonomous Transaction Processing database on shared Exadata infrastructure, see the following topics:

- Getting Started with Autonomous Database
- Connecting to Autonomous Database
- Loading Data with Autonomous Database
- Querying External Data with Autonomous Database
- Creating Dashboards, Reports, and Notebooks with Autonomous Database
- Managing Users on Autonomous Database
- Managing and Monitoring Performance of Autonomous Database

For information on using a database client to manage your database, see Connect Autonomous Database Using a Client Application.

Autonomous Database Tutorials

Autonomous Database Quickstart

Learn about Autonomous Database on Shared Infrastructure and learn how to create an Autonomous Database in just a few clicks. Then load data into your database, query it, and visualize it.

Autonomous Database Quickstart Workshop

- Provision Autonomous Database
- Load Data
- Query and Visualize Data
- Wallets
- Manage and Monitor
- Scale

Analyzing Your Data with Autonomous Database

Connect using secure wallets and monitor your Autonomous Database instances. Use Oracle Analytics Desktop to visualize data in Autonomous Database. Use Oracle Machine Learning Notebooks to try your hand at predictive analytics.

Analyzing your data with Autonomous Database Workshop

- Provision Autonomous Database
- Load Data
• Query and Visualize Data
• Wallets
• Manage and Monitor
• Scale
• Machine Learning Notebooks
• Build a Machine Learning Algorithm

**Autonomous Database on Dedicated Exadata Infrastructure**

For in-depth documentation on using and managing your Autonomous Database on dedicated Exadata infrastructure, see the following topics:

- Getting Started with Autonomous Database
- Connecting to Autonomous Database
- Loading Data into Autonomous Database
- Managing Dedicated Autonomous Databases
- Managing Database Users
- Managing and Monitoring Performance
- Backing Up and Restoring Autonomous Database
- Cloud Object Storage URI Formats
- Using Oracle Database Features in Dedicated Autonomous Database Deployments

For information on how application developers connect their applications to Autonomous Databases, see Developer’s Guide to Oracle Autonomous Database on Dedicated Exadata Infrastructure.

See Fleet Administrator’s Guide to Oracle Autonomous Database on Dedicated Exadata Infrastructure for information on administering multiple sets of Autonomous Database resources provisioned on dedicated Exadata Infrastructure.

For known issues, see Known Issues for Oracle Autonomous Database on Dedicated Exadata Infrastructure.

**Autonomous JSON Database**

Autonomous JSON Database is available on shared Exadata infrastructure. For in-depth documentation on using and managing your Autonomous JSON Database, see the following topics:

- Get Started Using Autonomous JSON Database
- Use SQL Developer Web with JSON Collections
- Develop RESTful Services
- Build an Application
- Load JSON Documents
- Code for High Performance

See JSON Developer's Guide for information on using Autonomous JSON Database as a part of application development.

**Oracle APEX Application Development**

Oracle APEX Application Development is available on Autonomous Database for shared Exadata infrastructure. For in-depth documentation on using and managing your Oracle APEX Application Development instance, see the following topics:

- What's Included in Oracle APEX Application Development
- Sign Up for Oracle APEX Application Development
- Access APEX Service
- Manage APEX Service
- Learn About Oracle Application Express
Creating an Autonomous Database on Shared Exadata Infrastructure

This topic describes how to provision a new Autonomous Database on Shared Exadata infrastructure using the Oracle Cloud Infrastructure Console or the API. Autonomous Databases can be provisioned on Dedicated Exadata infrastructure or Shared Exadata infrastructure. Your database can be optimized for either data warehouse, JSON, transaction processing, or APEX service workloads.

To provision an Always Free Autonomous Database, see To create an Always Free Autonomous Database on page 1159. For more information on the Free Tier, see Oracle Cloud Infrastructure Free Tier on page 140.

For Oracle By Example tutorials on provisioning Autonomous Databases, see Provisioning Autonomous Transaction Processing and Provisioning Autonomous Data Warehouse Cloud.

Prerequisites

- To create an Autonomous Database, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service.

  Tip:

  See Let database and fleet admins manage Autonomous Databases on page 2151 for sample Autonomous Database policies. See Details for the Database Service on page 2240 for detailed information on policy syntax.

- For information on additional prerequisites for provisioning an Autonomous Transaction Processing database, see What Do You Need? Likewise, for information on additional prerequisites for provisioning an Autonomous Data Warehouse, see What Do You Need?

- To create an Autonomous Transaction Processing database on Dedicated Exadata infrastructure, you must first provision the infrastructure and at least one Autonomous Container Database. For more information, see Creating an Autonomous Exadata Infrastructure Resource on page 1198 and Creating an Autonomous Container Database on page 1205.

Using the Oracle Cloud Infrastructure Console

To create an Autonomous Database on shared Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Provide the following information for the Autonomous Database:

   - **Compartment:** Select the compartment of the Autonomous Database.
   - **Display name:** A user-friendly description or other information that helps you easily identify the resource. The display name does not have to be unique. Avoid entering confidential information.
   - **Database name:** The database name must consist of letters and numbers only, starting with a letter. The maximum length is 14 characters.

Note:

You cannot use the same database name concurrently for an Autonomous Data Warehouse, an Autonomous JSON, or an Autonomous Transaction Processing database for databases using shared Exadata infrastructure.
Names associated with databases terminated within the last 60 days cannot be used when creating a database.

3. Choose a workload type. See About Autonomous Data Warehouse, About Autonomous JSON Database, About Autonomous Transaction Processing, and About Oracle Application Express for information about each workload type.

4. Choose the **Shared Infrastructure** deployment type.

   **Note:**
   
   If you choose JSON or APEX as your workload type, then Shared Infrastructure is the only available deployment type.

5. Configure the database:

   - **Always Free**: Use this selector to show only Always Free configuration options if you are provisioning an Always Free Autonomous Database. See Overview of the Always Free Autonomous Database on page 1220 for more information.

     **Note:**
     
     This option is not available for either JSON or APEX workload types.

   - **Choose database version**: Select a database version from the available versions.

   - **OCPU count**: Specify the number of cores for your Autonomous Database. The actual number of available cores is subject to your tenancy's service limits.

     Deselect **Auto scaling** to disable auto scaling. By default auto scaling is enabled to allow the system to automatically use up to three times more CPU and IO resources to meet workload demand. See CPU Scaling for more information.

   - **Storage (TB)**: Specify the storage you wish to make available to your Autonomous Database, in terabytes.

   - **Enable preview version**: *(This option only displays during periods when a preview version of Autonomous Database is available)* Select this option to provision the database with an Autonomous Database preview version. Preview versions of Autonomous Database are made available for limited periods for testing purposes. Do not select this option if you are provisioning a database for production purposes or if you will need the database to persist beyond the limited availability period of the preview version.

6. **Create administrator credentials**: Set the password for the Autonomous Database ADMIN user by entering a password that meets the following criteria. You use this password when accessing the Autonomous Database service console and when using a SQL client tool.

   **Password criteria:**
   
   - Contains from 12 to 30 characters and includes at least one uppercase letter, one lowercase letter, and one numeric character.
   - Does not contain the string "admin", regardless of case
   - Is not one of the last four passwords used for the ADMIN user
   - Does not contain the double quotation mark ("")
   - Cannot be the same password that was set less than 24 hours ago

7. Choose the type of network access.

   - **Allow secure access from anywhere**: This option provides access using a public endpoint that you secure with an access control list (ACL). Use this option if you need to access your database from the internet or your on-premises network. See Adding an Access Control List (ACL) to an Autonomous Database with a Public Endpoint on page 1161 for more information.

   - **Virtual cloud network**: This option creates a private endpoint for your database within a specified VCN. See Configuring a Virtual Cloud Network (VCN) for Private Endpoint Access to Your Autonomous Database on page 1162 for more information.
Choose a license type. Your choice affects metering for billing. You have the following options:

- **Bring Your Own License (BYOL):** Bring my existing database software licenses to the database cloud service.
- **License Included:** Subscribe to new database software licenses and the Database cloud service.

**Note:**
If you choose either JSON or APEX as your workload type, then License Included is the only available license type.

Clicking **Show Advanced Options** allows you to configure the following:

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

**Click Create Autonomous Database.**

**WHAT NEXT?**

- Connect to the database
- Create database users - Data Warehouse | Transaction Processing
- Load data into the database - Data Warehouse | JSON | Transaction Processing
- Connect applications that use the database - Data Warehouse | JSON | Transaction Processing
- Create APEX applications that use the database - Data Warehouse | Transaction Processing
- Register the database with Data Safe
- Set up Object Storage for manual backups

**To create an Always Free Autonomous Database**

**Note:**
An Always Free Autonomous Database cannot be created in a security zone compartment. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse or Autonomous Transaction Processing.

**Note:**
The JSON workload type is not available for Always Free Autonomous Database. You can use the Autonomous Transaction Processing workload type to work with JSON objects. Always Free Autonomous Transaction Processing databases can be converted to paid Autonomous JSON Databases.

2. Provide the following information for the Autonomous Database:

- **Compartment:** Select the compartment of the Autonomous Database.
- **Display name:** A user-friendly description or other information that helps you easily identify the resource. The display name does not have to be unique. Avoid entering confidential information.
- **Database name:** The database name must consist of letters and numbers only, starting with a letter. The maximum length is 14 characters.

**Note:**
You cannot use the same database name concurrently for both an Autonomous Data Warehouse and an Autonomous Transaction Processing database for databases using shared Exadata infrastructure.
3. Choose a workload type. See About Autonomous Data Warehouse, About Autonomous JSON Database, About Autonomous Transaction Processing, and About Oracle Application Express for information about each workload type.

**Note:**
The Oracle Application Express workload type is not available with Always Free Autonomous Databases

4. Choose the **Shared Infrastructure** deployment type.

5. Configure the database:

- **Always Free:** Move this selector to the right so that the provisioning workflow shows only the Always Free configuration options. Note that the **Core CPU count** and **Storage** configuration fields are disabled when provisioning an Always Free Autonomous Database. Your database will have 1 OCPU, 8 GB of memory, and 20 GB of storage.
- **Choose database version:** Select a database version from the available versions.

**Note:**
You can select only the current database version or a newer one. You cannot downgrade to an older database version.

6. **Create administrator credentials:** Set the password for the Autonomous Database ADMIN user by entering a password that meets the following criteria. You use this password when accessing the Autonomous Database service console and when using a SQL client tool.

Password criteria:

- Contains from 12 to 30 characters and includes at least one uppercase letter, one lowercase letter, and one numeric character.
- Does not contain the string "admin", regardless of case
- Is not one of the last four passwords used for the ADMIN user
- Does not contain the double quotation mark ("")
- Cannot be the same password that was set less than 24 hours ago

7. Network access for Always Free Autonomous Database is **Allow secure access from anywhere**. This option provides access using a public endpoint that you secure with an access control list (ACL). Use this option if you need to access your database from the internet or your on-premises network. See Adding an Access Control List (ACL) to an Autonomous Database with a Public Endpoint on page 1161 for more information on creating an ACL.

8. Clicking **Show Advanced Options** allows you to configure the following:

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

9. Click **Create Autonomous Database**.

**Note:**
The following naming restrictions apply to Autonomous Transaction Processing and Autonomous Data Warehouse databases using Shared Exadata Infrastructure:

- Names associated with databases terminated within the last 60 days cannot be used when creating a new database.
- A database name cannot be used concurrently for two Autonomous Databases, regardless of workload type.

**WHAT NEXT?**
- Create database users - Data Warehouse | Transaction Processing
• Load data into the database - Data Warehouse | Transaction Processing
• Connect applications that use the database - Data Warehouse | Transaction Processing
• Create APEX applications that use the database - Data Warehouse | Transaction Processing
• Connect to the database

Using the API

Use the CreateAutonomousDatabase API operation to create Autonomous Databases of either the Autonomous Data Warehouse (DW), Autonomous JSON Database (AJD), or Autonomous Transaction Processing (OLTP) workload types.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For More Information

Autonomous Database: Autonomous Transaction Processing and Autonomous Data Warehouse

• Using Oracle Autonomous Database on Shared Exadata Infrastructure (full product documentation)
• Autonomous Database Quickstart Workshop (Learn about Autonomous Database on Shared Infrastructure and learn how to create an Autonomous Database in just a few clicks. Then load data into your database, query it, and visualize it.)

Autonomous JSON Database

• Using Autonomous JSON Database (full product documentation)
• Autonomous JSON Database Videos (video tutorials)

Oracle APEX Application Development

• Oracle APEX Application Development (full product documentation)
• Oracle APEX Application Development Videos (video tutorials)

Adding an Access Control List (ACL) to an Autonomous Database with a Public Endpoint

This topic describes how to add an access control list (ACL) when provisioning an Autonomous Database on shared Exadata infrastructure that uses the Allow secure access from anywhere networking option. See Choose the type of network access in the To create an Autonomous Database on shared Exadata infrastructure on page 1157 topic to return to the provisioning instructions.

The network access rules you create for an access control list (ACL) provide protection for your Autonomous Database by allowing only the public and VCN IP addresses in the list to connect to the database. Click Configure Access Control Rules in the Create Autonomous Database dialog to create an ACL for your database.

You can specify the following types of addresses in your list by using the IP notation type drop-down selector:

• IP Address allows you to specify one or more individual public IP address. Use commas to separate your addresses in the input field.
• CIDR Block allows you to specify one or more ranges of public IP addresses using CIDR notation. Use commas to separate your CIDR block entries in the input field.
• Virtual Cloud Network allows you to specify an existing VCN. The drop-down listing in the input field allows you to choose from the VCNs in your current compartment for which you have access permissions. Click the Change Compartment link to display the VCNs of a different compartment.
• Virtual Cloud Network (OCID) allows you input the OCID of a VCN in a text box. You can use this input method if the VCN you are specifying is in a compartment which you do not have permission to access.
Caution:

If you want to specify multiple IP addresses or CIDR ranges within the same VCN, do not create multiple ACL entries. Use one ACL entry with the values for the multiple IP addresses or CIDR ranges separated by commas.

If you add a Virtual Cloud Network to your ACL, you can limit further by specifying allowed VCN IP addresses or CIDR ranges. Enter those addresses or CIDR blocks in the IP Addresses or CIDRs field that is displayed below your Virtual Cloud Network choice. Use commas to separate your VCN addresses and CIDR blocks in the input field.

You can specify the following types of IP addresses at the VCN level:

- Private IP addresses within your Oracle Cloud Infrastructure VCN
- Private IP addresses within an on-premises network that have access to your Autonomous Database using a transit routing and a private connection via FastConnect or VPN Connect.

Click + Another Entry to add additional access rules to your list.

Return to the Create Autonomous Database dialog instructions

Configuring a Virtual Cloud Network (VCN) for Private Endpoint Access to Your Autonomous Database

This topic describes how to configure a virtual cloud network (VCN) when provisioning an Autonomous Database on shared Exadata infrastructure that uses the Virtual cloud network networking option to provide private endpoint access. See Choose the type of network access in the To create an Autonomous Database on shared Exadata infrastructure on page 1157 topic to return to the provisioning instructions.

Note:

- See Networking Prerequisites Needed for Private Endpoint on page 1163 for information on creating the Networking resources needed for this configuration.
- If you are creating an Autonomous Database in a security zone compartment, your private endpoint networking configuration must use a subnet that is also in a security zone compartment. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

Select Virtual cloud network in the Create Autonomous Database dialog to configure private access, then specify the following information:

- **Virtual cloud network**: The VCN in which to launch the Autonomous Database. Click Change Compartment to select a VCN in a different compartment. **Important**: You cannot change the specified VCN after provisioning, except by switching to the Allow secure access from anywhere option, then switching back to the Virtual cloud network option and creating a new private endpoint network configuration.

- **Subnet**: The subnet to which the Autonomous Database should attach. Click change compartment to select a subnet in a different compartment. **Important**: You cannot change the specified subnet after provisioning, except by switching to the Allow secure access from anywhere option, then switching back to the Virtual cloud network option and creating a new private endpoint network configuration.

- **Hostname prefix**: Optional. This specifies a host name prefix for the Autonomous Database and associates a DNS name with the database instance, in the following form:

  hostname_prefix.adb.region.oraclecloud.com

  The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). You can use up to 63 alphanumeric characters for your hostname prefix.

  If you choose not to specify a hostname prefix, Oracle creates a unique DNS name for your database.

- **Network security groups**: You must specify at least one network security group (NSG) for your Autonomous Database. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to
your database. A maximum of five NSGs can be specified. See NSG security rule guidelines for private endpoint on page 1163 for details on configuring an NSG for your Autonomous Database.

For more information on creating and working with NSGs, see Network Security Groups on page 2841.

Note that if you choose a subnet with a security list, the security rules for the database will be a union of the rules in the security list and the NSGs.

**Tip:**

When connecting to your database from an on-premises network, Oracle recommends using a FastConnect connection. If you are using an IPSec VPN connection, see the configuration tips in the Hanging Connection on page 3327 topic in the Networking service documentation to avoid connection problems.

*Return to the Create Autonomous Database dialog instructions*

**Autonomous Database with Private Endpoint**

**Note:**

This topic applies only to Autonomous Databases with shared Exadata infrastructure.

*Private endpoint* refers to a network setup for your Autonomous Database with shared Exadata infrastructure where all network traffic moves through a private endpoint within a VCN in your tenancy. If your organization has strict security mandates that do not allow you to have a public endpoint for your database, this provides you with the necessary private endpoint. Additionally, this configuration uses no public subnets and allows you to keep all traffic to and from your Autonomous Database off of the public internet.

**Overview of Private Endpoint**

Enabling a private endpoint for an Autonomous Database ensures that the only access path to the database is via a VCN inside your Oracle Cloud Infrastructure tenancy. This network configuration completely blocks access to the database from public endpoints. A private endpoint offers the following advantages over other methods of private network access:

- Does not require you to set up transit routing in you VCN and use a service gateway to connect.
- Can satisfy security requirements that forbid the use of a public endpoint.

The private endpoint option is available for both new and existing Autonomous Databases on shared Exadata infrastructure. See To create an Autonomous Database on shared Exadata infrastructure on page 1157 for instructions on creating a new Autonomous Database with a private endpoint. See To change the network access of an Autonomous Database on shared Exadata infrastructure from private endpoint to public endpoint for information on switching network access configuration of an existing database.

**Networking Prerequisites Needed for Private Endpoint**

To provision an Autonomous Database with a private endpoint, you must have the following resources already created:

- A VCN within the region that will contain your Autonomous Database with shared Exadata infrastructure. Cannot be changed after provisioning.
- A private subnet within your VCN configured with default DHCP options. Cannot be changed after provisioning.
- At least 1 network security group (NSG) within your VCN for the Autonomous Database. Can be changed or edited after provisioning.

NSGs create a virtual firewall for your Autonomous Database using security rules. You can specify up to five NSGs to control access to your Autonomous Database.

*NSG security rule guidelines for private endpoint*

Your security rules for the NSG of your Autonomous Database need to be configured as follows:
• The private endpoint feature supports both stateful and stateless security rules within NSGs.
• Your rule covering ingress traffic must specify the **IP Protocol** "TCP", and your **Destination Port Range** must be 1522.
• To use Oracle Application Express, Oracle SQL Developer Web, and Oracle REST Data Services, add port 443 to the NSG rule.

To connect another resource located inside Oracle Cloud Infrastructure (for example, a Compute instance) to your Autonomous Database, the second resource needs a security rule that allows all egress traffic to the NSG of the Autonomous Database. This means you specify the NSG of the Autonomous Database as the **Destination** for this security rule. The second resource’s security rule can be part of an NSG or a security list.

See [Network Security Groups](#) on page 2841 and [To create an NSG](#) on page 2847 for more information on working with NSGs.

**Connecting to an Autonomous Database with a Private Endpoint**

You can connect to an Autonomous Database that uses a private endpoint from within Oracle Cloud Infrastructure resources, or from your data center. See [To find the Fully Qualified Domain Name (FQDN) and IP address of your private endpoint](#) for information on locating the IP address and URL of your endpoint.

**Example 1: Connecting from Within Oracle Cloud Infrastructure**

You can connect from a resource (like a Compute instance) within the same VCN as the private endpoint. Note that you can also connect from a resource located in a different VCN from the private endpoint by using local or remote VCN peering.

![Diagram of connecting to an Autonomous Database with a private endpoint](image)

Example network layout for connecting to an Autonomous Database with a private endpoint from within Oracle Cloud Infrastructure

You set up:

• A **VCN and a private subnet**
• An NSG for the Autonomous Database that includes either stateful or stateless security rules, as described in Networking Prerequisites Needed for Private Endpoint

Example stateful security rule for the Autonomous Database NSG. Note that stateless rules are also supported.

• An NSG security rule for the resource that will be allowed access to the Autonomous Database. This stateful egress security rule allows all egress traffic to the NSG of the Autonomous Database.

Example stateful egress security rule for the NSG of the resource connecting to the Autonomous Database

Example 2: Connecting from an On-Premise Data Center

Example network layout for connecting to an Autonomous Database with a private endpoint from an on-premises network

You set up:

• A VCN and a private subnet
• An NSG for the Autonomous Database that includes one or more security rules as described in see Networking Prerequisites Needed for Private Endpoint allowing traffic to a CIDR within your on-premises network

Example stateful security rule for the Autonomous Database NSG
• A Oracle Cloud Infrastructure FastConnect dedicated private connection or a VPN Connect IPSec VPN connection
• A dynamic routing gateway (DRG)
• A route table

Tip:
When connecting from an on-premises network, Oracle recommends using a FastConnect connection. If you are using an IPSec VPN connection, see the configuration tips in the Hanging Connection on page 3327 topic in the Networking service documentation to avoid connection problems.

To find the Fully Qualified Domain Name (FQDN) and IP address of your private endpoint

Your database's private endpoint IP address is displayed on the Autonomous Database Details page in the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click the display name of the database you want to connect to.
4. On the Autonomous Database Details page, in the Network section, the Private Endpoint IP Private Endpoint URL fields display the IP address and URL of the endpoint.

To resolve the Autonomous Database private endpoint in your on-premise host's /etc/hosts file

To resolve the Autonomous Database private endpoint, a Fully Qualified Domain Name (FQDN) requires that you add an entry in your on-premise client's hosts /etc/hosts file. For example:

# example /etc/hosts entry
10.0.2.7 example.adb.us-phoenix-1.oraclecloud.com

To use Oracle Application Express, Oracle SQL Developer Web, and Oracle REST Data Services, add another entry with the same IP. For example:

# example /etc/hosts entry
10.0.2.7 example.adb.ca-toronto-1.oraclecloudapps.com

You find the private endpoint IP and the FQDN as follows:
• The Private IP is shown on the Oracle Cloud Infrastructure Console Autonomous Database details page for the instance.
• The FQDN is shown in the tnsnames.ora file in the Autonomous Database client credential wallet.

Alternatively you can set up a hybrid DNS in Oracle Cloud Infrastructure for DNS name resolution.

Additional Information
See To create an Autonomous Database on shared Exadata infrastructure on page 1157 for instructions on provisioning an Autonomous Database that uses a private endpoint.
See To update the network configuration of an Autonomous Database on shared Exadata infrastructure that uses a private endpoint on page 1177 for information on editing networking settings related to a private endpoint.

See Private Access on page 3253 in the Networking service documentation for an overview of the options for enabling private access to services within Oracle Cloud Infrastructure.

See Hanging Connection on page 3327 in the Networking service documentation for troubleshooting IPSec VPN connection issues that can occur when connecting from your on-premises network.

Creating an Autonomous Database on Dedicated Exadata Infrastructure

This topic describes how to provision a new Autonomous Database on dedicated Exadata infrastructure using the Oracle Cloud Infrastructure Console or the API. Autonomous Databases can be provisioned on either dedicated Exadata infrastructure or shared Exadata infrastructure. Your database can be optimized for either transaction processing or data warehouse workloads, and you can create a standby database to facilitate disaster recovery by enabling Autonomous Data Guard.

For Oracle By Example tutorials on provisioning Autonomous Databases, see Provisioning Autonomous Transaction Processing and Provisioning Autonomous Data Warehouse Cloud.

Prerequisites

• To create an Autonomous Database, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service.

Tip:

See Let database and fleet admins manage Autonomous Databases on page 2151 for sample Autonomous Database policies. See Details for the Database Service on page 2240 for detailed information on policy syntax.

• For information on additional prerequisites for provisioning an Autonomous Transaction Processing database, see What Do You Need? Likewise, for information on additional prerequisites for provisioning an Autonomous Data Warehouse, see What Do You Need?

• To create an Autonomous Transaction Processing database on Dedicated Exadata infrastructure, you must first provision the infrastructure and at least one Autonomous Container Database. For more information, see Creating an Autonomous Exadata Infrastructure Resource on page 1198 and Creating an Autonomous Container Database on page 1205.

Using the Oracle Cloud Infrastructure Console

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Provide the following information for the Autonomous Database:

   • Compartment: Select the compartment of the Autonomous Database.
   • Display name: A user-friendly description or other information that helps you easily identify the resource. The display name does not have to be unique. Avoid entering confidential information.
   • Database name: The database name must consist of letters and numbers only, starting with a letter. The maximum length is 14 characters.

3. Choose a workload type. See About Autonomous Data Warehouse and About Autonomous Transaction Processing for information about each workload type.

4. Click the Dedicated Infrastructure deployment type.
5. In the **Choose Autonomous Container Database** section, select an Autonomous Container Database from the **Autonomous Container Database in compartment** drop-down.

You can change the compartment from which to choose an Autonomous Container Database by clicking the **CHANGE COMPARTMENT** link.

You can provision a standby Autonomous Container Database to provide data protection, high availability, and to facilitate disaster recovery for the primary database.

**a.** Select **Autonomous Data Guard-enabled Autonomous Container Databases** to list Autonomous Container Databases that have Oracle Data Guard enabled.

**b.** Select an Autonomous Container Database from the **Autonomous Container Database in compartment** drop-down.

**Note:**

The standby Autonomous Container Database inherits the resource configuration (OCPUs count and amount of storage) from the primary database.

- See **Creating an Autonomous Container Database** on page 1205 for information about provisioning a container database.
- See **Database System Resource types** on page 1193 in the Dedicated Deployment overview for information about the container database resource type.
- See **Managing a Standby Autonomous Container Database** on page 1214 for more information about Oracle Data Guard.

6. Configure the database:

- **OCPUs count:** Specify the number of cores for your Autonomous Database. The actual number of available cores is subject to your tenancy’s service limits.

  Deselect **Auto scaling** to disable auto scaling. By default auto scaling is enabled to allow the system to automatically use up to three times more CPU and IO resources to meet workload demand. See **CPU Scaling** for more information.

- **Storage (TB):** Specify the storage you wish to make available to your Autonomous Database, in terabytes.

7. **Create administrator credentials:** Set the password for the Autonomous Database ADMIN user by entering a password that meets the following criteria. You use this password when accessing the Autonomous Database service console and when using a SQL client tool.

Password criteria:

- Contains from 12 to 30 characters and includes at least one uppercase letter, one lowercase letter, and one numeric character.
- Does not contain the string "admin", regardless of case
- Is not one of the last four passwords used for the ADMIN user
- Does not contain the double quotation mark ("),
- Cannot be the same password that was set less than 24 hours ago

**Note:**

If you enable Autonomous Data Guard, then the standby Autonomous Database that gets provisioned has the same ADMIN user password as the primary database.
8. Click **Show Advanced Options** to configure the following:

   - **Encryption Key**: Whichever encryption key-management choice you made, either Oracle managed or your own encryption key, when you created the Autonomous Container Database, is displayed. The Autonomous Database you are creating inherits key management from the Autonomous Container Database.

     See [Managing Keys](#) on page 3962 for more information about encryption keys.

   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

9. Click **Create Autonomous Database**.

### Using the API

Use the `CreateAutonomousDatabase` API operation to create Autonomous Databases of either the Autonomous Data Warehouse (DW), Autonomous JSON Database (AJD), or Autonomous Transaction Processing (OLTP) workload types.

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

### For More Information

**Full Autonomous Database product documentation for dedicated Exadata infrastructure**

[Getting Started with Autonomous Database](#)

**Tutorials**

- [Autonomous Transaction Processing: Tutorials](#) (Oracle By Example tutorials)
- [Autonomous Data Warehouse: Tutorials](#) (Oracle By Example tutorials)

**Videos**

- [Autonomous Transaction Processing: Videos](#) (video tutorials)
- [Autonomous Data Warehouse: Videos](#) (video tutorials)

### Managing an Autonomous Database

**Autonomous Database**

This topic describes the database management tasks for Autonomous Databases that you complete using the Oracle Cloud Infrastructure Console or the API. These tasks apply to Autonomous Databases of either the Data Warehouse, JSON Database, or Transaction Processing workload types. You can filter Autonomous Databases by workload type on the [Autonomous Databases](#) page of the Oracle Cloud Infrastructure Console.

**Note:**

Some database management tasks not described here are performed using the [Autonomous Transaction Processing service console](#) or the [Autonomous Data Warehouse service console](#).

**Prerequisites**

To perform the management tasks in this topic, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See [Authentication and Authorization](#) for more information on user authorizations for the Oracle Cloud Infrastructure Database.
Using the Console

_Lifecycle Management Operations_

To check the lifecycle state of your Autonomous Database

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. In the Information tab, note the value displayed for **Lifecycle State**. For some lifecycle states, an information icon (ⓘ) is displayed to provide additional details regarding the lifecycle state or ongoing operations such as backups, restores, or terminations. The database has one of the following lifecycle states:

   - Available
   - Available needs attention
   - Backup in progress
   - Provisioning
   - Restore in progress
   - Scaling in progress
   - Starting
   - Stopping
   - Stopped
   - Terminating
   - Terminated
   - Unavailable

To stop or start an Autonomous Database

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Go to **More Actions**, and then click **Stop** (or **Start**). When you stop your Autonomous Database, billing stops for CPU usage. Billing for storage continues when the database is stopped.
5. Confirm that you want to stop or start your Autonomous Database in the confirmation dialog.

**Note:**

Stopping your database has the following consequences:

- On-going transactions are rolled back.
- CPU billing is halted
- You will not be able to connect to your database using database clients or tools.

To restart an Autonomous Database

**Tip:**

Restarting a database is equivalent to manually stopping and then starting the database. Using restart allows you to minimize downtime and requires only a single action.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Go to **More Actions**, and then click **Restart**.
5. Confirm that you want to restart your Autonomous Database in the confirmation dialog. The system stops and then immediately starts your database.

To terminate an Autonomous Database

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminating an Autonomous Database permanently deletes it. The database data, including automatic backups, will be lost when the system is terminated. Manual backups remain in Object Storage and are not automatically deleted when you terminate an Autonomous Database. Oracle recommends that you create a manual backup prior to terminating.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Go to **More Actions**, and then click **Terminate**.
5. Confirm that you want to terminate your Autonomous Database in the confirmation dialog.

To scale the CPU core count or storage of an Autonomous Database

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Click **Scale Up/Down**.
5. Enter a new value for **CPU Core Count** or **Storage** from 1 to 128. The number you enter represents the total value for your database's CPU core count or storage.

   The number of available cores is subject to your tenancy's service limits. An Autonomous Database database can have a maximum of 128 cores and 128 TB of storage. Scaling the CPU core count affects your CPU billing.
6. Click **Update**.

To enable or disable auto scaling for an Autonomous Database

Note the following points regarding the auto scaling feature:

- With auto scaling enabled, the database can use up to three times more CPU and IO resources than specified by the number of OCPUs currently shown in the **Scale Up/Down** dialog. See **CPU Scaling** for more information.
- If auto scaling is disabled while more CPU cores are in use than the database's currently assigned number of cores, then Autonomous Database scales the number of CPU cores in use down to the assigned number.
- Enabling auto scaling does not change the concurrency and parallelism settings for the predefined services. See **Managing Concurrency and Priorities on Autonomous Data Warehouse** and **Managing Priorities on Autonomous Transaction Processing** for more information.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Click **Scale Up/Down**.
5. Check **Auto Scaling** to enable the auto scaling feature, or uncheck **Auto Scaling** to disable the feature.
6. Click **Update**.

To view OCPU allocation hourly snapshot data for an Autonomous Database
1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. In the list of Autonomous Databases, click the display name of the database for which you want to view CPU usage data.

4. Click the Service Console button. The Service Console opens in a new tab or window.

5. In the Overview screen, the Number of OCPUs allocated graph shows hourly snapshot data of OCPU allocation over the last eight days. Place your cursor over the graph and move it to the left or right to see data for a specific day and hour.

Database Management Tasks

To set the Admin password

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. In the list of Autonomous Databases, click the display name of the database you want to administer.

4. Go to More Actions, and then click Admin Password. The Admin Password dialog opens.

5. Enter a password for the Autonomous Database. The password must meet the following criteria:
   - Contains from 12 to 30 characters
   - Contains at least one lowercase letter
   - Contains at least one uppercase letter
   - Contains at least one number
   - Does not contain the double quotation mark ("")
   - Does not contain the string "admin", regardless of case
   - Is not one of the last four passwords used for the database
   - Is not a password you previously set within the last 24 hours

6. Enter the password again in the Confirm Password field.

7. Click Update.

To access the Autonomous Database service console for databases on shared Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. In the list of Autonomous Databases, click the display name of the database you want to administer.

4. Click Service Console.

For information on using the Autonomous Transaction Processing service console features, see Managing and Monitoring Performance of Autonomous Transaction Processing. For information on using the Autonomous Data Warehouse service console features, see Managing and Monitoring Performance of Autonomous Data Warehouse Cloud.

To change the license type of an Autonomous Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. In the list of Autonomous Databases, click the display name of the database you want to administer.

4. Go to More Actions, and then click Update License Type.

   The dialog displays the options with your current license type selected.

5. Select the new license type.

6. Click Update.

See Known Issue.
To rename an Autonomous Database on shared Exadata infrastructure

**Note:**
Renaming a database changes the contents of the database wallet and requires that you download a new wallet.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Select the compartment, from the **Compartment** drop-down, that contains the database you want to rename.
3. From the list of Autonomous Databases contained in the compartment, click the display name of the database you want to rename to display the Autonomous Database Details page for that database.
4. Click **More Actions** to display a list of actions.
5. Click **Rename Database** to display the **Rename Database** dialog.
6. Enter a database name that contains only letters and numbers, begins with a letter, and does not exceed 14 characters.
7. Enter the current database name to confirm the name change.
8. Click **Rename Database**.

To change the workload type of an Autonomous Database

You can change the workload type of an Autonomous Database from **JSON** or **APEX** to Transaction Processing if you require additional capabilities offered by Autonomous Transaction Processing.

**Note:**
This change results in billing changes and cannot be reversed.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Click **Autonomous Database** to display a list of Autonomous Databases of all workload types.
3. If you are not in the correct compartment, then select the compartment from the **Compartment** drop-down that contains the database for which you want to change the workload type.
4. Click the display name of the Autonomous Database of either **JSON** or **APEX** workload type for which you want to change the workload type to display the Autonomous Database Details page for that database.
5. Click **More Actions** to display a list of operations. Click **Change Workload Type** to display the **Change Workload Type to Transaction Processing** confirmation dialog.
6. Click **Convert**.

To change the access mode of an Autonomous Database

You can select an operation mode for an Autonomous Database. The default mode is read/write but you can select read-only to limit users to querying the database, only. In addition, for either of these modes you can restrict access to only allow a user with administrator privileges to access the database.

**Note:**
Changing access modes and permission level do not apply to an Autonomous JSON Database.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your compartment from the **Compartment** drop-down.
3. In the list of Autonomous Databases, click the name of the database for which you want to change the access mode to display the details page for that database.

**Note:**
The database you choose must be in the Available state to successfully change the access mode.
4. On the **Autonomous Database Information** tab, click the **Edit** link in the **Mode** field.
5. In the Edit Database Mode dialog, choose either **Read/Write** or **Read-only**, depending on the access mode you want. By default, an Autonomous Database is provisioned in read/write mode.

   You can also restrict access to the ADMIN user or users with administrator privileges by checking **Allow administrator access only**. You can apply this restriction whether the database is in read/write or read-only mode.

6. Click **Confirm** to apply the change.

   **Note:**
   - Changing the permission level requires that users and applications reestablish connections to the database.
   - When the database is in read-only mode:
     - You cannot change the ADMIN user password.
     - You cannot upgrade the database.

To enable or disable Operations Insights on an Autonomous Database

Operations Insights is an Oracle Cloud Infrastructure service that provides analytics that you can use to monitor an Autonomous Database on either dedicated or shared Exadata infrastructure.

   **Note:**
   Enabling Operations Insights for the first time takes a few minutes to complete. Subsequent enabling operations take less time.

To enable Operations Insights:

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse** or **Autonomous Transaction Processing**.
2. If necessary, choose the compartment from the **Compartment** drop-down that contains the Autonomous Database you want to register with Operations Insights.
3. From the list of Autonomous Databases, click the display name of the database to display the details page for that database.
4. In the **Operations Insights** section, click **Enable** or **Disable** to display a confirmation dialog.
   - Once enabled, click the **View** link in the **Operations Insights** section to display the various metrics.
5. Click **Confirm**.

**Networking Management Tasks**

To change the network access type of an Autonomous Database on shared Exadata infrastructure from public endpoint to private endpoint

   Autonomous Databases on shared Exadata infrastructure can use either of the following network access options:
   - **Virtual cloud network**: This option uses a private endpoint within a VCN in your tenancy. The private endpoint connects to the private endpoint in either an Autonomous Database with private endpoint using dedicated Exadata infrastructure or an Autonomous Database with a private endpoint in the Shared Exadata infrastructure.
   - **Allow secure access from everywhere**: This option uses a public endpoint provided by Oracle.

   This topic describes how to switch a database's network access to the **Virtual cloud network** option. See **Autonomous Database with Private Endpoint** on page 1163 more information on this option, including the prerequisites needed to switch.

   **Note:**
   - Your Oracle Database version must be 19c or higher to perform an in-place switch the network access type after provisioning.
To change the network access configuration from a private to a public endpoint, the Autonomous Database must have the **Available** lifecycle state.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Go to **More Actions**, and then click **Update Network Access**.
5. In the **Update Network Access** dialog, select **Virtual cloud network**.

   **Note:**
   
   If Data Safe is enabled,
   
   a. Ensure that you have created a private endpoint in the selected VCN for Autonomous Database with a private endpoint
   
   b. Ensure that you have configured the security rules to allow traffic from Data Safe to Autonomous Database. For more information, see the Data Safe documentation.

6. Specify the following information:
   
   a. **Virtual cloud network**: The VCN in which to launch the Autonomous Database. Click **Change Compartment** to select a VCN in a different compartment.
   
   b. **Subnet**: The subnet to which the Autonomous Database should attach. Click **change compartment** to select a subnet in a different compartment. Oracle recommends that you specify a private subnet.
   
   c. **Hostname prefix**: **Optional.** This specifies a host name prefix for the Autonomous Database and associates a DNS name with the database instance, in the following form:

   
   
   hostname_prefix.**adb.*region.**oraclecloud.com

   
   The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). You can use up to 63 alphanumeric characters for your hostname prefix.

   If you choose not to specify a hostname prefix, Oracle creates a unique DNS name for your database.

   d. **Network security groups**: You must specify at least one network security group (NSG) for your Autonomous Database. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to your database. A maximum of five NSGs can be specified.

   For more information on creating and working with NSGs, see **Network Security Groups** on page 2841.

   Note that if you choose a subnet with a **security list**, the security rules for the database will be a union of the rules in the security list and the NSGs.

7. Click **Update**.

8. In the **Confirm** dialog, type the Autonomous Database name to confirm the change.

   Click **Update**.

**Notes:**

a. After updating the network access type all database users must obtain a new wallet and use the new wallet to access the database. See **About Downloading Client Credentials (Wallets)** for more information.

b. If you had access control list (ACL) rules defined for the public endpoint, the rules do not apply for the private endpoint.

To change the network access of an Autonomous Database on shared Exadata infrastructure from private endpoint to public endpoint

Autonomous Databases on shared Exadata infrastructure can use either of the following network access options:

a. **Virtual cloud network**: This option uses a private endpoint within a VCN in your tenancy.
• **Allow secure access from everywhere**: This option uses a public endpoint provided by Oracle.

This topic describes how to switch a database's network access to the **Allow secure access from everywhere** option.

**Note:**
- Your Oracle Database version must be 19c or higher to perform an in-place switch the network access type after provisioning.
- To change the network access configuration from a private to a public endpoint, the Autonomous Database must have the *Available* lifecycle state.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Go to **More Actions**, and then click **Update Network Access**.
5. In the **Update Network Access** dialog, select **Allow secure access from everywhere**.
6. Click **Update**.
7. In the **Confirm** dialog, type the Autonomous Database name to confirm the change.
8. Click **Update**.

Notes:
- After updating the network access type all database users must obtain a new wallet and use the new wallet to access the database. See **About Downloading Client Credentials (Wallets)** for more information.
- After the update completes, you can define access control rules for the public endpoint by specifying ACLs. See **To manage the access control list of an Autonomous Database on shared Exadata infrastructure** for more information. See **Access Control Lists (ACLs) for Databases on Shared Exadata Infrastructure** on page 1153 for details and restrictions regarding ACLs.

To manage the access control list of an Autonomous Database on shared Exadata infrastructure

This task applies to Autonomous Databases using the **Allow secure access from everywhere** network access option. This option uses a public endpoint provided by Oracle.

An access control list (ACL) provides additional protection for your Autonomous Database by allowing only the IP addresses in the list to connect to the database. An ACL must contain at least one entry representing an IP address or a range of addresses. To create or edit an ACL for an existing database that uses shared Exadata infrastructure, do the following:

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Under **Network** in the database details, find the **Access Control List** field and click **add** (if no ACL currently exists) or **edit** (to update an existing ACL).
5. In the **Access Control List** dialog, add or modify entries, as applicable.

**Note:**
If you are editing an ACL, the ACL's existing entries display in the **Access Control List** dialog. Do not overwrite the existing values unless you intend...
You can specify the following types of addresses in your list by using the IP notation type drop-down selector:

- **IP Address** allows you to specify one or more individual public IP address. Use commas to separate your addresses in the input field.
- **CIDR Block** allows you to specify one or more ranges of public IP addresses using CIDR notation. Use commas to separate your CIDR block entries in the input field.
- **Virtual Cloud Network** allows you to specify an existing VCN. The drop-down listing in the input field allows you to choose from the VCNs in your current compartment for which you have access permissions. Click the **Change Compartment** link to display the VCNs of a different compartment.
- **Virtual Cloud Network (OCID)** allows you input the OCID of a VCN in a text box. You can use this input method if the VCN you are specifying is in a compartment which you do not have permission to access.

**Caution:**
If you want to specify multiple IP addresses or CIDR ranges within the same VCN, do not create multiple ACL entries. Use one ACL entry with the values for the multiple IP addresses or CIDR ranges separated by commas.

If you add a Virtual Cloud Network to your ACL, you can limit further by specifying allowed VCN IP addresses or CIDR ranges. Enter those addresses or CIDR blocks in the **IP Addresses or CIDRs** field that is displayed below your Virtual Cloud Network choice. Use commas to separate your VCN addresses and CIDR blocks in the input field. You can specify the following types of IP addresses at the VCN level:

- Private IP addresses within your Oracle Cloud Infrastructure VCN
- Private IP addresses within an on-premises network that have access to your Autonomous Database using a transit routing and a private connection via FastConnect or VPN Connect.

Click **+ Another Entry** to add additional access rules to your list.

**Important:**
If you are using a service gateway, ensure that the CIDR range 240.0.0.0/4 is included in the list to allow clients accessing the database through the service gateway to connect to it.

To remove the ACL, simply delete all entries in the list. This action allows all clients to connect to the database.

6. **Click Update.**

If the Lifecycle State is **Available** when you click **Update**, the Lifecycle State changes to **Updating** until the ACL update is complete. The database is still up and accessible, there is no downtime. When the update is complete the Lifecycle State returns to **Available** and the network ACL rules from the access control list are in effect.

For more information about access control lists, see **Security Considerations** on page 1153.

To update the network configuration of an Autonomous Database on shared Exadata infrastructure that uses a private endpoint

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer. The **Autonomous Database Details** page displays.
4. In the **Autonomous Database Information** tab, the **Network** section displays the names of your database's virtual cloud network (VCN), subnet, and network security groups (NSGs). The following networking configuration changes are possible:

   • Clicking the names of your VCN and subnet will take you to the resource details pages of those resources. While you can edit the configurations of those resources, you cannot assign a different VCN or subnet to your Autonomous Database.

   • You can add or remove NSGs by clicking the **edit** link by the listed NSGs in the Network section on the **Autonomous Database Details** page. Note that your specified NSGs must contain stateless security rules.

   • You can edit the security rules of any of your Autonomous Database's NSGs by clicking the name of the NSG. Clicking the name takes you to the **Network Security Group Details** page of the NSG.

**Management Tasks for the Oracle Cloud Infrastructure Platform**

To view a work request for your Autonomous Database

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse, Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. In the **Resources** section, click **Work Requests**. The status of all work requests appears on the page.
5. To see the log messages, error messages, and resources that are associated with a specific work request, click the operation name. Then, select an option in the **More information** section.

For associated resources, you can click the the Actions icon (three dots) next to a resource to copy the resource's OCID.

For more information, see **Work Requests** on page 258.

To move an Autonomous Database to another compartment

**Note:**

- To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Database resources, see **Details for the Database Service** on page 2240.

- **Security zone considerations:**
  - If your Autonomous Database is in a security zone, the destination compartment must also be in a security zone.
  - If your Autonomous Database uses a public endpoint, you cannot move it to a security zone compartment unless you first switch the networking configuration to use a private endpoint.
  - If your Autonomous Database is not in a security zone and has Data Guard standby database, you cannot move the database into a security zone compartment while the standby remains in a compartment that is not in a security zone.

See the **Security Zone Policies** topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse, Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to move.
4. Go to **More Actions**, and then click **Move Resource**.
5. Select the new compartment.
6. Click **Move Resource**.

For information about dependent resources for Database resources, see *Moving Database Resources to a Different Compartment* on page 1141.

To manage tags for your Autonomous Database

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse, Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to administer.
4. Go to **More Actions**, and then click **Apply Tag(s)** to add new tags. Or click the **Tags** tab to view or edit the existing tags.

For more information, see *Resource Tags* on page 211.

To upgrade an Always Free Autonomous Database to a paid instance

If you are using a paid account, you can upgrade an Always Free/Autonomous Database to a paid instance. Paid instances include the ability to scale the OCPU count and storage.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse, Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click the display name of the database you want to upgrade.
4. Go to **More Actions**, and then click **Upgrade Instance to Paid**.
5. In the **Confirm Upgrade** dialog, confirm that you want to upgrade the instance by clicking the **Upgrade Instance to Paid** button.

The lifecycle state of the Autonomous Database will change to **Updating** while your upgrade is in progress. You database remains online and accessible while the upgrade is in progress. After your instance is upgraded to paid, you will be able to provision a new Always Free/Autonomous Database in place of your upgraded instance.

*Security Management Tasks*

For information on network security management tasks, see *Networking Management Tasks* on page 1174.

To register or deregister an Autonomous Database with Data Safe

To use Oracle Data Safe with an Autonomous Database, you register your database with Data Safe. To discontinue using Data Safe, you deregister the database. For information about using Data Safe, see the Data Safe documentation.

*Prerequisites for Autonomous Databases with private endpoints*

- Data Safe must be enabled in the region containing the Autonomous Database. For information about creating and using Data Safe instances, see the Data Safe documentation.
- Ensure that the Data Safe instance has a private endpoint. Instructions for creating a Data Safe private endpoint are located in the Register DB Systems that have Private IP Addresses topic in this manual.
- Enable communication from the Data Safe private endpoint to your database. To do this, update the security list or network security group (NSG) rules in the database's VCN to allow the Data Safe private endpoint to access the database. See the Access and Security section in this manual for information about network security groups, security rules, and security lists. See To update the network configuration of an Autonomous Database on shared Exadata infrastructure that uses a private endpoint on page 1177 for information on updating NSG rules for Autonomous Databases running on shared Exadata infrastructure. See and To edit the network security groups (NSGs) for your Autonomous Exadata Infrastructure resource on page 1204 for information on updating NSG rules for Autonomous Databases running on dedicated Exadata infrastructure.
Registering and deregistering an Autonomous Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. In the list of Autonomous Databases, click the display name of the database you want to manage.

4. In the Details page, under Data Safe, click register or deregister depending on the status of the database.
   - If the database uses dedicated Exadata infrastructure, enter the ADMIN password and click Confirm to start the registration or deregistration process. The ADMIN password is needed to unlock Data Safe so that it can monitor the database.
   - If the database uses Shared Exadata infrastructure, click Confirm to start the registration or deregistration process.

If the registration fails and the database is using a private endpoint, ensure that the prerequisites listed in this topic for allowing network access have been met.

5. You can optionally use either or both of the following to monitor the registration and deregistration process:
   - Use the work request created by the system to monitor the progress of the registration or deregistration.
   - Click View Console to display the Data Safe user interface for the registered database.

Registering and deregistering an Autonomous Database when Database Vault is enabled

When Database Vault is enabled on the database you are registering or deregistering, complete the following additional steps to register or deregister the database. These are needed to accommodate the additional database security provided by Database Vault.

- The Database Vault account manager must first grant specific access rights to the ADMIN database user before they can register or deregister an Autonomous Database. Otherwise, an "insufficient privileges" error is displayed.
- After the database has been registered or deregistered, the Database Vault account manager can remove the access rights to limit access during normal operations.
- After the database registration is complete, the Database Vault owner must grant specific access rights to the DS $ADMIN database user to enable normal operations. See the Data Safe documentation to learn about the access rights needed.

For more information on using Database Vault with an Autonomous Database, see the following user guides:

- Using Oracle Autonomous Transaction Processing on Shared Exadata Infrastructure
- Using Oracle Autonomous Transaction Processing on Dedicated Exadata Infrastructure
- Using Oracle Autonomous Data Warehouse on Shared Exadata Infrastructure
- Using Oracle Autonomous Data Warehouse on Dedicated Exadata Infrastructure
To rotate the encryption key for an Autonomous Database

Rotating the encryption key creates a new version of the vault key that replaces the current version of the vault key.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your compartment from the Compartment drop-down.

3. Click the display name of the Autonomous Database for which you want to rotate the encryption key to display the details page for that database.

   **Note:**
   The Autonomous Database you choose must be on dedicated Exadata infrastructure and in an Available state.

4. Click the More Actions drop-down.

5. Click Rotate Encryption Key to display a confirmation dialog.

6. Click Rotate Key.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage Autonomous Databases:

- ListAutonomousDatabases
- GetAutonomousDatabase
- UpdateAutonomousDatabase
- ChangeAutonomousDatabaseCompartment
- StartAutonomousDatabase
- RestartAutonomousDatabase
- StopAutonomousDatabase
- DeleteAutonomousDatabase

**For More Information**

- Using Oracle Autonomous Database on Shared Exadata Infrastructure ([full product documentation](#))
- Using Oracle Autonomous Database on Dedicated Exadata Infrastructure ([full product documentation](#))

**Connecting to an Autonomous Database**

This topic describes the following actions related to connecting client applications to an Autonomous Database:

- Obtaining the credentials and information (wallet) you need to create a connection (applies to both shared Exadata infrastructure and dedicated Exadata infrastructure)
- Rotating the keys and credentials (wallet) needed for a connection (applies to shared Exadata infrastructure only)
- Obtaining access URLs for Oracle Application Express (APEX) and Oracle Database Actions

   **Tip:**
   For more information on connecting a client to an Autonomous Database on dedicated Exadata infrastructure, see Connecting to Autonomous Database.

**About Connecting to Autonomous Databases**

Applications and tools connect to Autonomous Databases by using Oracle Net Services (also known as SQL*Net). SQL*Net supports a variety of connection types to Autonomous Databases, including Oracle Call Interface (OCI), ODBC drivers, JDBC OC, and JDBC Thin Driver.

To support connections of any type, you must download the client security credentials and network configuration settings required to access your database. You must also supply the applicable TNS names or connection strings for a connection, depending on the client application or tool, type of connection, and service level. You can view or copy
the TNS names and connection strings in the **DB Connection** dialog for your Autonomous Database. For detailed information about the TNS names, see **Predefined Database Service Names for Autonomous Transaction Processing** and **Predefined Database Service Names for Autonomous Data Warehouse**.

**Connecting to an Autonomous Database**

You can connect to an Autonomous Database that uses shared Exadata infrastructure from a VCN with either a public or private endpoint.

To connect to Autonomous Databases that use a **public endpoint** from a VCN, the VCN must be configured with one of the following gateways:

- **internet gateway**: For access from a public subnet in the VCN
- **service gateway**: For access from a private subnet in the VCN

Make sure to configure the subnet's **route table** with a rule that sends the desired traffic to the specific gateway. Also configure the subnet's **security lists** to allow the desired traffic.

You can also connect to your database from private IP addresses in your on-premises network by using transit routing with an Oracle Cloud Infrastructure VCN. This allows traffic to move directly from your on-premises network to your Autonomous Database without going over the internet. See **Transit Routing: Private Access to Oracle Services** on page 2803 for more information on this method of access.

To connect to Autonomous Databases that use a **private endpoint** from a VCN, you must configure a security rule within one of the database's **network security groups** (NSGs) to allow access to the Autonomous Database endpoint. For more information on private endpoint network configuration, see **Networking Prerequisites Needed for Private Endpoint**.

**About Downloading Client Credentials**

The client credentials .zip that you download contains the following files:

- **cwallet.sso** - Oracle auto-login wallet
- **ewallet.p12** - PKCS #12 wallet file associated with the auto-login wallet
- **sqlnet.ora** - SQL*Net profile configuration file that includes the wallet location and TNSNAMES naming method
- **tnsnames.ora** - SQL*Net configuration file that contains network service names mapped to connect descriptors for the local naming method
- **Java Key Store (JKS)** files - Key store files for use with JDBC Thin Connections

**Important:**

Wallet files, along with the database user ID and password, provide access to data in your Autonomous Database. Store wallet files in a secure location. Share wallet files only with authorized users. If wallet files are transmitted in a way that might be accessed by unauthorized users (for example, over public email), transmit the wallet password separately and securely.

For Autonomous Databases on **shared Exadata infrastructure**, you have the choice of downloading an **instance wallet** file or a **regional wallet** file. The instance wallet contains only credentials and keys for a single Autonomous Database. The regional wallet contains credentials and keys for all Autonomous Databases in a specified region. For security purposes, Oracle recommends that regional wallets be used only by database administrators, and that instance wallets be supplied to other users whenever possible.

For Autonomous Databases on **dedicated Exadata infrastructure**, the wallet file contains only credentials and keys for a single Autonomous Database.

**About Rotating Your Autonomous Database Wallet**

For Autonomous Databases on **shared Exadata infrastructure**, you can rotate an instance or regional wallet for security purposes. When your wallet rotation is complete, you will have a new set of certificate keys and credentials, and the old wallet's keys and credentials will be invalid. Rotating an instance wallet does not invalidate the regional wallet that covers the same database instance. Rotating a regional wallet affects all databases in the specified region. User session termination begins after wallet rotation completes, however this process does not happen immediately.
**Important:**

If you are rotating a wallet to address a security breach and need to reestablish all database connections immediately using the keys and credentials of your newly rotated wallet, stop and restart the database instance.

**Before You Begin**

The Autonomous Database is preconfigured to support Oracle Net Services (a TNS listener is installed and configured to use secure TCPS and client credentials.) The client computer must be prepared to use Oracle Net Services to connect to the Autonomous Database. Preparing your client includes downloading the client credentials. See the following links for steps you might have to perform before you access the client credentials and connection information for your Autonomous Database:

*Shared Exadata Infrastructure*

- Preparing for Oracle Call Interface (OCI), ODBC, and JDBC OCI Connections

* Dedicated Exadata infrastructure

- Preparing for Oracle Call Interface (OCI), ODBC, and JDBC OCI Connections
- Preparing for JDBC Thin Connections

**Using the Oracle Cloud Infrastructure Console**

To download a wallet for an Autonomous Database on shared Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you are interested in.
4. Click DB Connection.
5. In the Download Client Credentials (Wallet) section, select the Wallet Type. You can choose to download an instance wallet or a regional wallet.
6. To obtain the client credentials, click Download Wallet.
   - You will be prompted to provide a password to encrypt the keys inside the wallet. The password must be at least 8 characters long and must include at least 1 letter and either 1 numeric character or 1 special character.
   - Save the client credentials zip file to a secure location. See About Downloading Client Credentials on page 1182 for information about the files included in the download.
7. Take note of or copy the TNS names or connection strings you need for your connection. See About Connecting to Autonomous Databases on page 1181 for information about making connections.

To download a wallet for an Autonomous Database on dedicated Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you are interested in.
4. Click DB Connection.
5. Select the DB Connection option.
6. Click the DB Connection tab.
7. To obtain the client credentials, click Download.
   - You will be prompted to provide a password to encrypt the keys inside the wallet. The password must be at least 8 characters long and must include at least 1 letter and either 1 numeric character or 1 special character.
   - Save the client credentials zip file to a secure location. See About Downloading Client Credentials on page 1182 for information about the files included in the download.
8. Take note of or copy the TNS names or connection strings you need for your connection. See About Connecting to Autonomous Databases on page 1181 for information about making connections.

WHAT NEXT?

Connect to the database - Data Warehouse | Transaction Processing

To rotate the wallet of an Autonomous Database on shared Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you are interested in.
4. Click DB Connection.
5. In the Download Client Credentials (Wallet) section, select the Wallet Type. You can choose to rotate an instance wallet or a regional wallet.
6. Click Rotate Wallet. A confirmation dialog will prompt you to enter the database name to confirm the rotation.
7. Enter the name of the database, then click Rotate Wallet.

The rotation takes a few minutes to complete.

To obtain access URLs for Oracle Application Express (APEX) and Oracle SQL Developer Web for an Autonomous Database on dedicated Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you are interested in.
4. Select the Application Connection option.
5. Application URLs are displayed in plain text in the Application URL field. Copy the URL string using the Copy link.
6. Paste the URL into a browser running on a Compute instance that is inside of the VCN of the Autonomous Database. Alternately, you can use the URL with a compute instance that has a direct connection to the VCN of the Autonomous Database.

Using the API

Use the GenerateAutonomousDatabaseWallet API operation to download the client credentials for your Autonomous Database.

Use the UpdateAutonomousDatabaseWalletDetails API operation to rotate the wallet for your Autonomous Database.

Use the AutonomousDatabase API operation to get the access URLs for Application Express (APEX) and SQL Developer Web.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Backing Up an Autonomous Database Manually

This topic describes how to create manual backups of Autonomous Databases. You can use the Oracle Cloud Infrastructure Console or the API to perform these tasks.

Oracle Cloud Infrastructure automatically backs up your Autonomous Databases and retains these backups for 60 days. Automatic backups are weekly full backups and daily incremental backups. You can also create manual backups to supplement your automatic backups. Manual backups are stored in an Object Storage bucket that you create, and are retained for 60 days.
Prerequisites

- To create or manage Autonomous Database backups, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service. See Let database and fleet admins manage Autonomous Databases on page 2151 for sample Autonomous Database policies. See Details for the Database Service on page 2240 for detailed information on policy syntax.
- To create a manual backup for an Autonomous Database, you must first configure an Object Storage bucket to serve as a destination for your manual backups. See Setting Up a Bucket to Store Manual Backups for instructions.

Using the Console

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, find the database that you want to back up.
4. Click the name of the Autonomous Database to display the Autonomous Database details.
5. In the database details page, click Create Manual Backup.

   The create Manual Backup dialog box is displayed.

   a. If you have properly configured your database for manual backups, continue to step 6.
   b. If the database is not properly configured for manual backups, a message box informs you that you must first configure the database before you can create a manual backup. See Setting Up a Bucket to Store Manual Backups for instructions.
   c. Click Close, configure your database according to the instructions, and click Create Manual Backup again.
6. In the Create Manual Backup dialog box, enter a name for your backup. Avoid entering confidential information.
7. In the Create Manual Backup dialog box, click Create.

   Your backup may take several hours to complete, depending on the size of your database.

8. Optionally, you can check the state of your backup in the list of backups on the database details page. For some states, an information icon (i) is displayed to provide additional details regarding the state or ongoing operations like deletions. The backup has one of the following states:

   - Creating
   - Active
   - Deleting
   - Deleted
   - Failed

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage Autonomous Database backups:
Setting Up a Bucket to Store Manual Backups

You must create an Oracle Cloud Infrastructure Object Storage bucket to hold your Autonomous Database manual backups and configure your database to connect to it. This is a one-time operation.

To set up an object store and user credentials for your manual backups

Some of the steps in this procedure require you to connect to the database by using an Oracle Database client such as SQL Developer. See Connecting with Oracle SQL Developer (18.2 or later) for information and instructions on connecting to an Autonomous Transaction Processing database. See Connecting with Oracle SQL Developer (18.2 or later) for information and instructions on connecting to an Autonomous Data Warehouse database.

1. If you have not already done so, generate an auth token for the Oracle Cloud Infrastructure Object Storage user to access the bucket you create in the next step. See To create an auth token on page 2463 to learn how to do this. (You will need this auth token for the database credential you create in step 4.)

2. In the Oracle Cloud Infrastructure Console, create a bucket in your designated Object Storage Swift compartment to hold the backups.

For example, if your backup bucket is named "backup_database1", the URL would be:

```
Note:
When you create your bucket:
• Pick Standard as the storage tier. Manual backups are only supported with buckets created in the standard storage tier.
• Ensure that you use the database name, and not the display name, as the bucket name.
```

3. Using an Oracle Database client, log in to the database as the administrator set the database DEFAULT_BACKUP_BUCKET property to the URL of your Object Storage bucket. The format of the tenancy URL is https://swiftobjectstorage.region.oraclecloud.com/v1/object_storage_namespace/bucket_name.

   For example:

   ```
   ALTER DATABASE PROPERTY SET default_backup_bucket='https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/ansh8lvrlulzpz/backup_database1';
   ```

   In the example, the Object Storage namespace is ansh8lvrlulzpz.

   Tip:
   • To determine the Object Storage namespace string to use, click View Bucket in the actions (three dots) menu of the bucket you created in the previous step.
   • Do not include the bucket name in the URL.
   • Ensure that you follow the format indicated. Do not use a pre-authenticated request URL.

4. With the tenancy user and the auth token referenced in step 1, create the credential for your Oracle Cloud Infrastructure Object Storage account. Use DBMS_CLOUD.CREATE_CREDENTIAL to create the credential.

   For example:

   ```
   BEGIN
   DBMS_CLOUD.CREATE_CREDENTIAL(
   credential_name => 'DEF_CRED_NAME',
   username => 'db1_user@oracle.com',
   ```
password => '<auth_token>'
);
END;
/

For more information on creating this credential, see CREATE_CREDENTIAL Procedure.

5. Set the database property `default_credential` to the credential you created in the previous step.

For example:

```sql
ALTER DATABASE PROPERTY SET DEFAULT_CREDENTIAL = 'ADMIN.DEF_CRED_NAME';
```

To list the current value for the default bucket, run the following command:

```sql
SELECT PROPERTY_VALUE from database_properties WHERE PROPERTY_NAME='DEFAULT_BUCKET';
```

After completing these steps you can take manual backups any time you want.

**Manual Backup Notes**

Database configuration notes:

- If you previously configured manual backups using the `DEFAULT_BUCKET` property, you do not need to make any changes to perform manual backups with your existing configuration. In this case, the `DEFAULT_BUCKET` property is set to the value of Oracle Cloud Infrastructure Object Storage tenancy URL and the required bucket name is in the format of `backup_databasename`, where databasename is lowercase. However, Oracle recommends that you configure Autonomous Database for manual backups using the `DEFAULT_BACKUP_BUCKET` database property.
- If you previously configured Autonomous Database to use manual backups using the `DEFAULT_BUCKET` property and created backups, then after configuring the `DEFAULT_BACKUP_BUCKET` property to use a new manual backup bucket, the old manual backups in the old bucket are not available for restore. If you want to use the old backups then you must change the value of the `DEFAULT_BACKUP_BUCKET` property to specify the URL of the old manual backup bucket.
- If you previously configured Autonomous Database to use manual backups and you rename your Autonomous Database, then your backups will continue to work without changes.

Manual backup notes:

- Each manual backup creates a full backup on your Oracle Cloud Infrastructure Object Storage bucket and the backup can only be used by the Autonomous Database instance when you initiate a point-in-time-recovery.
- The retention period for manual backups is the same as for automatic backups, which is 60 days.
- While backing up a database, the database is fully functional. However, during the backup the lifecycle management operations, such as stopping the database, are not allowed.

**Restoring an Autonomous Database**

Autonomous Database

This topic describes how to restore an Autonomous Database from a backup. You can use the Oracle Cloud Infrastructure Console or the API to perform this task.

You can use any existing manual or automatic backup to restore your database, or you can restore and recover your database to any point in time in the 60-day retention period of your automatic backups. For point-in-time restores, you specify a timestamp, and your Autonomous Database decides which backup to use for the fastest restore.

**Note:**

Restoring Autonomous Database puts the database in the unavailable state during the restore operation. You cannot connect to a database in that state.
Prerequisites

To restore Autonomous Databases, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service. See Let database and fleet admins manage Autonomous Databases on page 2151 for sample Autonomous Database policies. See Details for the Database Service on page 2240 for detailed information on policy syntax.

Using the Oracle Cloud Infrastructure Console

To restore an Autonomous Database from a backup

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, find the database that you wish to restore.
4. Click the name of the Autonomous Database to display the database details.
5. Click the Restore button to open the restore dialog.
6. Click Select Backup.
7. Specify the date range for a list of backups to display.
8. Select the backup.
9. Click Restore.

To restore an Autonomous Database using point-in-time restore

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, find the database that you wish to restore.
4. Click the name of the Autonomous Database to display the database details.
5. Click the Restore button to open the restore dialog.
6. Click Specify Timestamp.
7. Enter a timestamp. Your Autonomous Database decides which backup to use for faster recovery. The timestamp input allows you to specify precision to the seconds level (YYYY-MM-DD HH:MM:SS GMT).
8. Click Restore.

Using the API

Use the RestoreAutonomousDatabase API operation to restore your Autonomous Database from a backup.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Cloning an Autonomous Database

This topic describes how to clone an existing Autonomous Database using the Oracle Cloud Infrastructure Console or the API. You can use the cloning feature to create a point-in-time copy of your Autonomous Database for purposes such as testing, development, or analytics. To clone only the database schema of your source database, choose the metadata clone option.

Note:

- You can clone any existing Autonomous Database (including those provisioned with preview version software) using a preview version of Autonomous Database. However, preview-version databases cannot be
cloned using the regular (general-availability) Autonomous Database software.

- You cannot clone an Autonomous Database from one Autonomous Container Database to another Autonomous Container Database if one of the Autonomous Container Databases has different encryption management configured. Encryption management must be the same for both Autonomous Container Databases, either Oracle-managed or customer-managed.

### Clone Types

The clone feature offers the following types of Autonomous Database clones:

- **Full clone**: This option creates a database that includes the metadata and data from the source database.
- **Metadata clone**: This option creates a database that includes only the metadata from the source database.
- **Refreshable clone**: This option creates a clone that can be easily updated with changes from the source database. For information about creating and using refreshable clones, see Using Refreshable Clones with Autonomous Database.

### Clone Sources

You can use a running database to create a clone. For databases running on shared Exadata infrastructure, you can also use a backup as the source of your clone. When using a backup, you can select a listed backup to clone from, or create a point-in-time clone. Point-in-time clones contain all data up to a specified timestamp. The specified timestamp must be in the past.

**Note:**

When you create a clone from a backup, you must select a backup that is at least two hours old.

### Prerequisites

To clone an Autonomous Database, you must have the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service.

**Note:**

You can’t clone a database in a security zone to create a database that isn't in a security zone. This is true whether the source is a running database or a database backup. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

### Password Requirement for New Databases on Dedicated Exadata Infrastructure

When cloning a database on dedicated Exadata infrastructure, the password you set for the target database cannot be one of the three most recently used passwords of the source database.

### Using the Oracle Cloud Infrastructure Console

**Note:**

See Create a Refreshable Clone for an Autonomous Database Instance for instructions for creating a refreshable clone.

To clone an Autonomous Database to shared Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. If you are not already in the correct compartment, then choose one from the Compartment drop-down in the List Scope section that contains the database you want to clone.
3. In the list of Autonomous Databases, click the display name of the database you want to clone.

4. Go to More Actions, and then click Create Clone.

In the Create Autonomous Database Clone dialog, enter the following:

**Clone Type**
Select the type of clone you want to create. Choose either Full Clone or Metadata Clone.

**Clone Source**
The clone source selection allows you to specify whether the clone is created from a running database or from a database backup. Select one of the following options:

- **Clone from running database**: Creates a clone of a running database as it exists at the current moment.
- **Clone from a backup**: Creates a clone from a database backup. If you choose this option, select one of the following options:
  - **Specify a timestamp**: Creates a point-in-time clone.
  - **Select from a list of backups**: Creates a clone using all data from the specified backup. To limit your list of backups to a specific date range, enter the starting date in the From field and the ending date in the To field.

**Note:** You must select a backup that is at least 2 hours old, or the clone operation will fail.

**Database Information**

- **Compartment**: Your current compartment is the default selection.
- **Display Name**: A user-friendly description or other information that helps you easily identify the resource. The display name does not have to be unique, and you can change it whenever you like. Avoid entering confidential information.
- **Database Name**: The database name must consist of letters and numbers only, starting with a letter. The maximum length is 14 characters. Avoid entering confidential information.
- **Choose database version**: Select a database version from the available versions.
- **CPU Core Count**: You can enable up to 128 cores for your Autonomous Database. The actual number of available cores is subject to your tenancy's service limits.

**Auto Scaling**: allows Autonomous Databases to automatically increase the number of CPU cores by up to three times the assigned CPU core count value, depending on demand for processing. The auto scaling feature reduces the number of CPU cores when additional cores are not needed. For databases with up to 42 assigned cores, you can increase the maximum number of cores available through auto scaling by increasing the CPU core count value.

**Note:**
The maximum number of cores that are available to any Autonomous Database database not using dedicated Exadata infrastructure is 128, regardless of whether auto scaling is enabled or not. This means that a database with a CPU core count of 64 could auto scale up to two times the assigned number of cores (2 x 64 = 128). A database with 42 cores (or fewer) could auto scale up to three times the assigned number (3 x 42 = 126). For billing purposes, the database service determines the average number of CPUs used per hour.

- **Storage**: Specify the storage you wish to make available to your Autonomous Database database, in terabytes. You can make up to 128 TB available. For full clones, the size of the source database determines the minimum amount of storage you can make available.
- **Enable Preview Version**: (This option only displays during periods when a preview version of Autonomous Database is available) Select this option to provision the database with an Autonomous Database preview version. Preview versions of Autonomous Database are made available for limited periods for testing.
purposes. Do not select this option if you are provisioning a database for production purposes or if you will need the database to persist beyond the limited availability period of the preview version.

**Administrator Credential**

Set the password for the Autonomous Database Admin user by entering a password that meets the following criteria. You use this password when accessing the Autonomous Database service console and when using an SQL client tool.

- Password cannot be one of the three most recently used passwords of the source database
- Contains from 12 to 30 characters
- Contains at least one lowercase letter
- Contains at least one uppercase letter
- Contains at least one number
- Does not contain the double quotation mark ("")
- Does not contain the string "admin", regardless of casing

**License Type**

The type of license you want to use for the Autonomous Transaction Processing database. Your choice affects metering for billing. You have the following options:

- **My Organization Already Owns Oracle Database Software Licenses**: This choice is used for the Bring Your Own License (BYOL) license type. If you choose this option, make sure you have proper entitlements to use for new service instances that you create.
- **Subscribe to New Database Software Licenses and the Database Cloud Service**: This is used for the License Included license type. With this choice, the cost of the cloud service includes a license for the Database service.

5. Click **Create Autonomous Database Clone**.

The Console displays the details page for the new clone of your database and the service begins provisioning the Autonomous Database. Note the following:

- The new clone displays the **Provisioning** lifecycle state until the provisioning process completes.
- The source database remains in the **Available** lifecycle state.
- Backups associated with the source database are not cloned for either the full clone or the metadata clone option.
- Oracle recommends that you evaluate the security requirements for the new database and implement them, as applicable. See Security Considerations on page 1153 for details.

**WHAT NEXT?**

- Modify the access control list
- Manage database users - Data Warehouse | Transaction Processing
- Load data into the database - Data Warehouse | Transaction Processing
- Connect applications that use the database - Data Warehouse | Transaction Processing
- Create APEX applications that use the database - Data Warehouse | Transaction Processing
- Register the database with Data Safe
- Set up Object Storage for manual backups
- Connect to the database

To clone an Autonomous Database to dedicated Exadata infrastructure

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. If you are not already in the correct compartment, then choose one from the **Compartment** drop-down in the **List Scope** section that contains the database you want to clone.
3. In the list of Autonomous Databases, click the display name of the database you want to clone.
4. Click **More Actions** to display a list of actions.
5. Click **Create Clone** to display the Create Autonomous Database Clone page.

In the **Clone Type** section, select the **type of clone** you want to create. Choose either **Full Clone** or **Metadata Clone**.

**Provide basic information for the Autonomous Database**

- **Create in Compartment**: Your current compartment is the default selection but you can select a different compartment in which to create the clone from the drop-down list.
- The name of the source database displays in the read-only **Source database name** field.
- **Display Name**: Enter a description or other information to identify the database clone. You can change the display name any time and it does not have to be unique. Avoid entering confidential information.
- **Database Name**: Enter a database name for the clone that contains only letters and numbers, begins with a letter, and does not exceed 14 characters. Avoid entering confidential information.
- **Autonomous Container Database in compartment**: You can choose to create the database clone in the same compartment and container database as the source database, or you can choose a different compartment by clicking **Change compartment**, and a different container database by choosing one from the drop-down list.

**Configure the database**

- **OCPU Count**: You can enable up to 92 cores for your cloned Autonomous Database.
- **Storage**: Specify the amount of storage, in terabytes, that you want to make available to your cloned Autonomous Database database, up to 128 TB. For full clones, the size of the source database determines the minimum amount of storage you can make available.

**Create administrator credentials**

Set the password for the Autonomous Database administrator user by entering a password that meets the following criteria.

- Password cannot be one of the three most recently used passwords of the source database
- Between 12 and 30 characters long
- Contains at least one lowercase letter
- Contains at least one uppercase letter
- Contains at least one number
- Does not contain the double quotation mark ("")
- Does not contain the string "admin", regardless of casing

Use this password when accessing the service console and when using a SQL client tool.

6. Click **Create Autonomous Database Clone**.

The Console displays the details page for the new clone of your database and the service begins provisioning the Autonomous Database. Note the following:

- The new clone displays the **Provisioning** lifecycle state until the provisioning process completes.
- The source database remains in the **Available** lifecycle state.
- Backups associated with the source database are not cloned for either the full-clone or the metadata-clone option.
- Oracle recommends that you evaluate the security requirements for the new database and implement them, as applicable. See **Network Security Groups for Databases Resources That Use Private Endpoints** on page 1154 for details.

**WHAT NEXT?**

- Manage database users - Data Warehouse | Transaction Processing
- Load data into the database - Data Warehouse | Transaction Processing
- Create applications that use the database - Data Warehouse | Transaction Processing
- Connect to the database - Data Warehouse | Transaction Processing

**Using the API**

Use the **CreateAutonomousDatabase** API operation to clone an Autonomous Database.
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

**For More Information**

For information about optimizer statistics, resource management rules and performance data for a cloned database, see Using Oracle Autonomous Database on Shared Exadata Infrastructure, which has full product documentation for Autonomous Database.

**Maintenance Updates for Autonomous Databases with Shared Exadata Infrastructure**

Autonomous Databases perform maintenance updates and database patching for you. Your database remains available throughout the maintenance process. This topic describes Autonomous Database maintenance for shared Exadata infrastructure.

For information on maintenance for dedicated Exadata infrastructure, see Overview of Dedicated Exadata Infrastructure Maintenance on page 1196.

**Maintenance Duration**

For Autonomous Databases with shared Exadata infrastructure, Oracle performs regular maintenance updates that generally take no more than two hours.

**Checking the Scheduling of Maintenance Updates**

To see when your next scheduled maintenance update is, navigate to the Autonomous Database details page in the Console for the database you are interested in. The Next Maintenance metadata field displays the beginning and ending times of the next database maintenance. You can also use the GetAutonomousDatabase API operation to determine the time of your next maintenance update.

**Overview of Autonomous Database on Dedicated Exadata Infrastructure**

This topic describes the database system architecture, features, user roles and hardware shapes for Autonomous Database on dedicated Exadata infrastructure. For a general overview of Autonomous Databases that covers the basics common to both infrastructure options, see Overview of Autonomous Databases on page 1149.

**Database System Architecture Overview**

Autonomous Databases on dedicated Exadata infrastructure have a three-level database architecture model that makes use of Oracle multitenant database architecture.

**Database System Resource types**

Each level of the architecture model corresponds to one of the following resources types:

- An **Autonomous Exadata Infrastructure** resource. This is a hardware rack which includes compute nodes and storage servers, tied together by a high-speed, low-latency InfiniBand network and intelligent Exadata software. On dedicated Exadata infrastructure, you have exclusive use of the Exadata infrastructure and hardware on which your Autonomous Transaction Processing databases run.

For a list of the hardware and Oracle Cloud resource characteristics of Autonomous Exadata Infrastructure resources, see Characteristics of Autonomous Exadata Infrastructure Resources.
• An **Autonomous Container Database**, which provides a container for multiple user databases. This resource is sometimes referred to as a CDB, and is functionally equivalent to the multitenant container databases found in Oracle 12c and higher databases.

Multitenant architecture offers many advantages over non-CDB architecture. For example, it does the following:

• Allows you to easily manage multiple individual user databases
• Makes more efficient use of database hardware, as individual databases may use only a fraction of the server hardware capacity
• Allows for easier and more rapid movement of data and code
• Allows for easier testing, as development databases can be housed within the same container as production databases
• Allows for the separation of duties between database administrators, who manage only the individual Autonomous Database instances to which they are granted privileges, and fleet managers, who manage infrastructure resources and container databases.

• An **Autonomous Database**. You can create multiple Autonomous Databases within the same container database. This level of the database architecture is analogous to the pluggable databases (PDBs) found in non-Autonomous Exadata systems. Your Autonomous Database can be configured for either transaction processing or data warehouse workloads.

**Database System Resource Deployment Order**

You must create the dedicated Exadata infrastructure resources in the following order:

1. **Autonomous Exadata Infrastructure.** See [Creating an Autonomous Exadata Infrastructure Resource](#) on page 1198 for more information.

2. **Autonomous Container Database.** See [Creating an Autonomous Container Database](#) on page 1205 for more information.

3. **Autonomous Database.** See [Creating an Autonomous Database on Dedicated Exadata Infrastructure](#) on page 1167 for more information.

**Related Database System Resources**

Related resources and prerequisites include:

• A **Virtual Cloud Network (VCN)** and a **Subnet**, which you create using Oracle Cloud Infrastructure's Networking service. You must have at least one VCN and one subnet available to provision an Autonomous Database with dedicated Exadata infrastructure.

For more information, see the following topics:

• [Network Isolation](#) (from Fleet Administrator’s Guide to Oracle Autonomous Transaction Processing on Dedicated Exadata Infrastructure)

• [Networking Overview](#) on page 2748

• [To create a VCN](#) on page 2825

• [To create a subnet](#) on page 2825

• **Autonomous Backups**, created for you automatically by the Autonomous Database service. By default, backups are stored for 60 days. Using the Console, you can choose to change the retention period to 7, 15, or 30 days.

• **Manual Backups**. Optionally, you can create on-demand manual backups. Manual backups are subject to the retention policy you have in place for the Autonomous Container Database.

**User Roles**

Your organization may choose to split the administration of the Autonomous Database on dedicated Exadata infrastructure into the following roles:

• **Fleet Administrator**. Fleet administrators create, monitor and manage Autonomous Exadata Infrastructure and Autonomous Container Database resources. A fleet administrator must have permissions for using the networking
resources required by the dedicated Exadata infrastructure, and permissions to manage the infrastructure and container database resources.

See Fleet Administrator’s Guide to Oracle Autonomous Transaction Processing on Dedicated Exadata Infrastructure for a complete overview of the fleet administrator role.

- **Database Administrator.** Database administrators create, monitor and manage Autonomous Databases. They also create and manage users within the database. Database administrators must have permissions for using container databases, for managing Autonomous Transaction Processing databases and backups, and for using the related networking resources. For manual backups, they must have permissions to use the designated Object Storage bucket. At the time of provisioning an Autonomous Database, the administrator provides user credentials for the automatically created ADMIN account, which provides administrative rights to the new database.

See Using Oracle Autonomous Transaction Processing on Dedicated Exadata Infrastructure for a complete overview of the database administrator role.

- **Database User.** Database users are the developers who write applications that connect to and use an Autonomous Database to store and access the data. Database users do not need Oracle Cloud Infrastructure accounts. They gain network connectivity to and connection authorization information for the database from the database administrator.

### CPU Provisioning, CPU Scaling, and Storage Scaling

You can scale the CPU count and the storage capacity of the database at any time without impacting availability or performance. Autonomous Database on dedicated Exadata infrastructure does not currently support over-provisioning, the ability for multiple Autonomous Databases to share a single CPU core. Therefore, an Autonomous Exadata Infrastructure resource can currently support, across all its Autonomous Container Databases, up to as many Autonomous Databases as it has CPU cores. This maximum number will increase when Oracle Autonomous Database supports over-provisioning.

### Available Exadata Infrastructure Hardware Shapes

Oracle Cloud Infrastructure currently offers Autonomous Database with the following dedicated Exadata infrastructure system models and configurations:

- **System Models:** X7 and X8
- **Configurations:** quarter rack, half rack, and full rack

The subsections that follow provide the details for each shape's configuration.

**Exadata X8 Shapes**

<table>
<thead>
<tr>
<th>Property</th>
<th>Quarter Rack</th>
<th>Half Rack</th>
<th>Full Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shape Name</strong></td>
<td>Exadata.Quarter3.100</td>
<td>Exadata.Half3.200</td>
<td>Exadata.Full3.400</td>
</tr>
<tr>
<td><strong>Number of Compute Nodes</strong></td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total Maximum Number of Enabled CPU Cores</strong></td>
<td>100</td>
<td>200</td>
<td>400</td>
</tr>
<tr>
<td><strong>Total RAM Capacity</strong></td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
</tr>
<tr>
<td><strong>Number of Exadata Storage Servers</strong></td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td><strong>Total Raw Flash Storage Capacity</strong></td>
<td>76.8 TB</td>
<td>179.2 TB</td>
<td>358.4 TB</td>
</tr>
<tr>
<td><strong>Total Usable Storage Capacity</strong></td>
<td>149 TB</td>
<td>298 TB</td>
<td>596 TB</td>
</tr>
</tbody>
</table>
**Exadata X7 Shapes**

<table>
<thead>
<tr>
<th>Property</th>
<th>Quarter Rack</th>
<th>Half Rack</th>
<th>Full Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shape Name</td>
<td>Exadata.Quarter2.92</td>
<td>Exadata.Half2.184</td>
<td>Exadata.Full2.368</td>
</tr>
<tr>
<td>Number of Compute Nodes</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Total Maximum Number of Enabled CPU Cores</td>
<td>92</td>
<td>184</td>
<td>368</td>
</tr>
<tr>
<td>Total RAM Capacity</td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
</tr>
<tr>
<td>Number of Exadata Storage Servers</td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>Total Raw Flash Storage Capacity</td>
<td>76.8 TB</td>
<td>153.6 TB</td>
<td>307.2 TB</td>
</tr>
<tr>
<td>Total Usable Storage Capacity</td>
<td>106 TB</td>
<td>212 TB</td>
<td>424 TB</td>
</tr>
</tbody>
</table>

**Using the Oracle Cloud Infrastructure Console to Manage Dedicated Exadata Infrastructure**

For information on provisioning, managing, and backing up dedicated Exadata infrastructure resources in the Oracle Cloud Infrastructure Console, see the following topics:

**For Database Fleet Administrators**
- Creating an Autonomous Exadata Infrastructure Resource on page 1198
- Creating an Autonomous Container Database on page 1205
- Managing an Autonomous Exadata Infrastructure Resource on page 1201
- Managing an Autonomous Container Database on page 1208
- Fleet Administrator’s Guide to Oracle Autonomous Database on Dedicated Exadata Infrastructure (complete fleet administrator guide)

**For Database Administrators**
- Creating an Autonomous Database on Dedicated Exadata Infrastructure on page 1167
- Managing an Autonomous Database on page 1169
- Connecting to an Autonomous Database on page 1181
- Backing Up an Autonomous Database Manually on page 1184
- Restoring an Autonomous Database on page 1187
- Using Oracle Autonomous Database on Dedicated Exadata Infrastructure (complete database administrator guide)

**Additional Information**

For known issues, see Known Issues for Oracle Autonomous Database on Dedicated Exadata Infrastructure.

**Overview of Dedicated Exadata Infrastructure Maintenance**

Autonomous Database systems on dedicated Exadata infrastructure have separate regularly scheduled maintenance runs for both Autonomous Exadata Infrastructure resources and Autonomous Container Databases. You can choose to set the scheduling for your maintenance runs, or let the system schedule maintenance. You can view the maintenance history for infrastructure instances and container databases in the Oracle Cloud Infrastructure Console. Additionally, one-off patching is available for certain resources on dedicated Exadata infrastructure when you file a service request for an eligible resource with My Oracle Support.
Autonomous Exadata Infrastructure Maintenance

Exadata infrastructure maintenance takes place at least once each quarter and is mandatory. You can schedule a maintenance window to control the time, day of the week, and week of the month for Exadata infrastructure maintenance. Exadata infrastructure maintenance patches the Exadata infrastructure (including patching of the Exadata grid infrastructure code and operating systems updates), and do not include database patching. Oracle notifies you about upcoming Exadata infrastructure maintenance in the weeks before quarterly Exadata infrastructure patching occurs. You can also view scheduled maintenance runs in the Oracle Cloud Infrastructure console. The following tasks explain how to view scheduled and past maintenance updates, and how to edit the maintenance schedule for an Exadata infrastructure instance:

- To configure the automatic maintenance schedule for an Autonomous Exadata Infrastructure resource on page 1201
- To view the next scheduled maintenance for an Autonomous Exadata Infrastructure resource on page 1202
- To view the maintenance history of an Autonomous Exadata Infrastructure resource on page 1202

You can use the GetMaintenanceRun, ListMaintenanceRun, and UpdateAutonomousExadataInfrastructure API operations to view details about scheduled and past maintenance updates, and to update the maintenance schedule of your infrastructure instance.

Autonomous Container Database Maintenance

Container database maintenance updates include Oracle Database software patches and take place at least once each quarter. You can configure a maintenance window to control the time, day of the week, and week of the month that your maintenance update run will begin. Otherwise, Oracle will schedule container database maintenance runs for you so that they are coordinated with the maintenance runs of the associated Exadata infrastructure.

- Tip:
  Container database maintenance runs must be scheduled to take place after quarterly Exadata infrastructure maintenance runs occur.

If a scheduled container database maintenance run cannot take place (because of changes made to infrastructure maintenance scheduling or other reasons), Oracle will automatically reschedule the container database maintenance for the following quarter. You can change your container database maintenance window or reschedule a single container database maintenance run to ensure that your container database maintenance runs follow infrastructure maintenance within the same quarter.

Autonomous Database offers two container database maintenance choices:

- Release Update (RU): Autonomous Database installs only the most current release update.
- Release Update Revision (RUR): Autonomous Database installs the release update plus additional fixes.

The following tasks explain how to view and edit maintenance updates information for Autonomous Container Databases:

- To configure the automatic maintenance schedule for an Autonomous Container Database on page 1209
- To view the maintenance history of an Autonomous Container Database on page 1210
- To reschedule or skip scheduled maintenance for an Autonomous Container Database on page 1210
- To configure the type of maintenance patching for an Autonomous Container Database on page 1209

Use the UpdateAutonomousContainerDatabase API operation to change the patching type for an Autonomous Container Database. Use the ListMaintenanceRun API operation to see past maintenance update information. Use the UpdateMaintenanceRun API operations to skip a container database maintenance update. You can skip maintenance runs for up to 2 consecutive quarters if needed.
Notifications for Maintenance of Autonomous Exadata Infrastructure and Autonomous Container Database Resources

Autonomous Database emits events for Autonomous Exadata Infrastructure and Autonomous Container Database maintenance runs. Using the Notifications service (which consumes events), you can create and subscribe to a Notifications topic, allowing you to receive notifications about your maintenance runs by email, PagerDuty alert, Slack, or https.

You can set up notifications based on the following events:

- A new maintenance run is scheduled
- A maintenance reminder email is sent
- A maintenance run begins
- A maintenance run ends.

See Getting Started with Events on page 1786 to learn about creating and subscribing to an Events topic. See Services that Produce Events for a full list of Database service events. See Managing Topics and Subscriptions on page 3356 to learn how to create and subscribe to a Notifications topic.

Managing One-off Patches as Part of Dedicated Exadata Infrastructure Maintenance

Oracle generates one-off patches when a user files a service request with My Oracle Support. If appropriate to resolve the service request, and Oracle and the user agree that a one-off patch is the best solution, then the service team generates a one-off patch and makes it available to the user that filed the service request. One-off patches are separate from scheduled maintenance patches.

If you enable Oracle Cloud Notifications and Oracle Cloud Events with a subscription to receive notifications regarding new updates, then when one-off patches become available, Oracle sends a notification that contains the OCID of the product to be patched. Otherwise, you can find the update in the My Oracle Support portal for the service request that you filed.

You can edit the scheduled start time or choose to install the one-off patch, immediately. By default, Oracle schedules a one-off patch to be applied within 72 hours of the patch becoming available and, if no action to change the schedule occurs, then the patch is automatically applied.

1. Copy the OCID from the notification and paste it into the Search field on the Oracle Cloud Infrastructure Console to navigate to the correct product.
2. On the product details page, in the Maintenance section, click the View link in the Next Maintenance field to display the Maintenance page for the product that you want to patch.
3. One-off patches are displayed in the Unplanned maintenance section and are denoted as one-off patches in the Type field. If the scheduled start time for the patch interferes with enterprise operations or is otherwise inconvenient, then click Edit to change the scheduled time to install the patch. Click Patch Now to immediately install the one-off patch.
4. Click Run Maintenance to start the patching operation.

Creating an Autonomous Exadata Infrastructure Resource

This topic describes how to provision an Autonomous Exadata Infrastructure resource for Autonomous Databases using the Oracle Cloud Infrastructure Console or the API. For an overview of dedicated Exadata infrastructure, see Overview of Autonomous Database on Dedicated Exadata Infrastructure on page 1193.

The infrastructure resource includes the physical Exadata hardware and intelligent Exadata software. Once you have provisioned an infrastructure instance, you can provision one or more Autonomous Container Databases to run on your infrastructure. To provision an Autonomous Database, you must have both an infrastructure resource and at least one container database available.

Note:

This topic is not applicable to Autonomous Databases on shared Exadata infrastructure.
Prerequisites

• To create an Autonomous Exadata Infrastructure resource, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service.

| Tip: |
| See Let database and fleet admins manage Autonomous Databases on page 2151 for sample Autonomous Database policies. See Details for the Database Service on page 2240 for detailed information on policy syntax. |

• You will also need a Virtual Cloud Network and a Subnet, which you create using Oracle Cloud Infrastructure's Networking service. For information on creating and managing these resources, see VCNs and Subnets on page 2821.

• If you are creating an Autonomous Exadata Infrastructure resource in a security zone compartment, your networking configuration must use a subnet that is also in a security zone compartment. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

Using the Oracle Cloud Infrastructure Console

To create an Autonomous Exadata Infrastructure resource

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. Click Autonomous Exadata Infrastructure.
4. Click Create Autonomous Exadata Infrastructure.
5. In the Create Autonomous Exadata Infrastructure dialog, enter the following general information:
   • Compartment: Specify the compartment in which the Autonomous Exadata Infrastructure will be created.
   • Display Name: A user-friendly description or other information that helps you easily identify the infrastructure resource. The display name does not have to be unique. Avoid entering confidential information.
   • Availability Domain: Select an availability domain for the Autonomous Exadata Infrastructure.
   • System Model: Select a system model, either the X7 or X8. See Available Exadata Infrastructure Hardware Shapes on page 1195 for detailed information on available system models.
   • System Configuration: Select Quarter Rack, Half Rack, or Full Rack. Total available OCPUs and storage are displayed on the system configuration buttons. Total available OCPU and storage values are determined by the specified system model.
6. Enter the following network information:
   • Virtual cloud network compartment: The compartment containing the VCN you wish to use for the Autonomous Exadata Infrastructure. The default value is the user's current compartment. Click change compartment to select a VCN in a different compartment.
   • Virtual cloud network: The VCN in which to launch the Autonomous Exadata Infrastructure.
   • Subnet compartment: The compartment containing the subnet you wish to use for the Autonomous Exadata Infrastructure. The default value is the user's current compartment. Click change compartment to select a subnet in a different compartment.
   • Subnet: The subnet to which the Autonomous Exadata Infrastructure should attach.
   • Use network security groups to control traffic: Optional. You can specify up to five network security groups (NSGs) for your Autonomous Exadata Infrastructure resource by selecting this option. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to your infrastructure resource. A maximum of five NSGs can be specified. To add an NSG, select the compartment containing the...
NSG using the **Network security group compartment** selector, then select the NSG itself using the **Network security group** selector.

For more information on creating and working with NSGs, see Network Security Groups on page 2841.

Note that if you choose a subnet with a security list, the security rules for the infrastructure resource will be a union of the rules in the security list and the NSGs.

7. Optionally, you can specify the date and start time for the Autonomous Exadata Infrastructure quarterly maintenance:

   a. Click **Modify Schedule**.
   b. In the Automatic Maintenance Schedule dialog, select **Specify a Schedule**.
   c. In the **Maintenance months** selector, specify at least one month for each quarter during which infrastructure maintenance will take place.
   d. For **Week of the Month**, select a week during the month that the maintenance will take place. Weeks start on the 1st, 8th, 15th, and 22nd days of the month, and have a duration of 7 days. Weeks start and end based on calendar dates, not days of the week. For example, to allow maintenance during the 2nd week of the month (from the 8th day to the 14th day of the month), use the value 2. Maintenance cannot be scheduled for the fifth week of months that contain more than 28 days.
   e. For **Day of the Week**, select the day of the week that the maintenance will take place.
   f. For **Start Hour**, select one of the six start time windows available. The maintenance will begin during the 4 hour time window that you specify and may continue beyond the end of the period chosen. The start time window is specified in universal coordinated time (UTC).
   g. Click **Update Maintenance Schedule**.

   **Tip:**

   Oracle recommends that you define the acceptable maintenance times for your Autonomous Exadata Infrastructure resources and Autonomous Container Databases. Doing so will prevent maintenance runs from occurring at times that would be disruptive to regular database operations.

8. Choose the license type you wish to use. Your choice affects metering for billing. You have the following options:
   - **Bring your own license**: If you choose this option, make sure you have proper entitlements to use for new service instances that you create.
   - **License included**: With this choice, the cost of the cloud service includes a license for the Database service.

9. The following **Advanced Options** are available:

   **Tags** - If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

10. Click **Create Autonomous Exadata Infrastructure**.

**WHAT NEXT?**

After creating an Autonomous Exadata Infrastructure resource, you can create one or more Autonomous Container Databases on your infrastructure. You must have provisioned both an infrastructure resource and at least one container database before you can create your first Autonomous Database in Oracle Cloud Infrastructure.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the LaunchAutonomousExadataInfrastructure API operation to create an Autonomous Exadata Infrastructure resource.
Managing an Autonomous Exadata Infrastructure Resource

This topic describes the Autonomous Exadata Infrastructure management tasks for Autonomous Databases that you complete using the Oracle Cloud Infrastructure Console or the API. Autonomous Databases use Autonomous Exadata Infrastructure resources on dedicated Exadata infrastructure. See Overview of Autonomous Database on Dedicated Exadata Infrastructure on page 1193 for more information.

**Note:**

This topic is not applicable to Autonomous Databases on shared Exadata infrastructure.

Using the Oracle Cloud Infrastructure Console

You can perform the following management operations on Autonomous Exadata Infrastructure resources in Oracle Cloud Infrastructure:

- Configuring the automatic maintenance schedule
- Rescheduling maintenance
- Viewing the next scheduled maintenance date and maintenance history
- Immediately patching an Autonomous Exadata Infrastructure
- Copying the Autonomous Exadata Infrastructure endpoint
- Terminating the Autonomous Exadata Infrastructure resource

**Tip:**

Oracle recommends that you define the acceptable maintenance times for your Autonomous Exadata Infrastructure resources and Autonomous Container Databases. Doing so will prevent maintenance runs from occurring at times that would be disruptive to regular database operations.

*To configure the automatic maintenance schedule for an Autonomous Exadata Infrastructure resource*

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you are interested in.
5. On the Autonomous Exadata Infrastructure details page, under Maintenance, click the edit link in the Maintenance Schedule field.
6. In the Automatic Maintenance Schedule dialog, select Specify a schedule.
7. Under Maintenance months, specify at least one month for each maintenance quarter during which you want Autonomous Exadata Infrastructure maintenance to occur.

**Note:**

Maintenance quarters begin in February, May, August, and November, with the first maintenance quarter of the year beginning in February.

8. Under Week of the month, specify which week of the month maintenance will take place. Weeks start on the 1st, 8th, 15th, and 22nd days of the month, and have a duration of 7 days. Weeks start and end based on calendar dates, not days of the week. Maintenance cannot be scheduled for the fifth week of months that contain more than 28 days.
9. Under Day of the week, specify the day of the week on which the maintenance will occur.
10. Under Start hour, specify the hour during which the maintenance run will begin.
11. Click Update Maintenance Schedule.
To view the next scheduled maintenance for an Autonomous Exadata Infrastructure resource

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you are interested in.
5. On the Autonomous Exadata Infrastructure details page, under Maintenance, click the view link in the Next Maintenance field.
6. On the Maintenance page, scheduled maintenance events are listed under the Regular Autonomous Exadata Infrastructure maintenance heading.

To reschedule maintenance of Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your compartment from the Compartment drop-down.
3. In the Dedicated Infrastructure section, click Autonomous Exadata Infrastructure.
4. In the list of Autonomous Exadata Infrastructures, click the display name of the Exadata infrastructure for which you want to reschedule maintenance.
5. On the Autonomous Exadata Infrastructure Details page, in the Maintenance section, click the View link in the Next Maintenance field.
6. The Maintenance page displays any Exadata infrastructure maintenance events planned for the next 15 days in the list of maintenance events.
7. To reschedule maintenance, click the Edit link in the Scheduled Start Time field to display the Edit Maintenance Start Time dialog.
8. Click the calendar icon and choose a date and time on which to run maintenance.
9. Click Save Changes.

To view the maintenance history of an Autonomous Exadata Infrastructure resource

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you are interested in.
5. On the Autonomous Exadata Infrastructure details page, under Maintenance, click the view link in the Next Maintenance field.
6. On the Maintenance page, under Autonomous Database Maintenance, click History. In the list of past maintenance events, you can click on an individual event title to read the details of the maintenance that took place. Maintenance event details include the following:
   • The category of maintenance (quarterly software maintenance, hardware maintenance, or a critical patch)
   • Whether the maintenance was scheduled or unplanned
   • The OCID of the maintenance event. (Go to More Actions, then choose Copy OCID.)
   • The start time and date of the maintenance

To immediately patch an Autonomous Exadata Infrastructure

After you schedule maintenance for your Autonomous Exadata Infrastructures, you can patch the component, immediately, at any time before scheduled maintenance occurs. If you choose to patch your Autonomous Exadata Infrastructure, immediately, while another component is in the process of maintenance, then this maintenance operation gets queued and will begin, in turn.

1. Open the navigation menu. Under Database, click Autonomous Transaction Processing or Autonomous Data Warehouse.
2. Choose your compartment from the **Compartment** drop-down list.

3. In the **Dedicated Infrastructure** section, click **Autonomous Exadata Infrastructure** to display a list of Autonomous Exadata Infrastructures for your selected compartment.

4. Click the display name of the Autonomous Exadata Infrastructure that you want to patch.

5. On the Autonomous Exadata Infrastructure Details page, in the **Maintenance** section, click the **View** link in the **Next Maintenance** field to display the Maintenance page for the Autonomous Exadata Infrastructure that you want to patch.

6. In the **Autonomous Exadata Infrastructure** section, click the **Patch Now** link in the **Scheduled Start Time** field to display the **Run Maintenance** dialog.

7. Click **Run Maintenance** to start the patching operation.

---

**To view or copy the Autonomous Exadata Infrastructure endpoint**

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.

2. Choose your **Compartment**.

3. Under **Autonomous Database**, click **Autonomous Exadata Infrastructure**.

4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you are interested in.

5. On the Autonomous Exadata Infrastructure Information tab, click **Show** or **Copy** in the **DB Infrastructure Endpoint Name field**.

---

**To manage security certificates in an Autonomous Exadata Infrastructure**

To maintain security compliance within an Autonomous Exadata Infrastructure, you must periodically rotate the security certificates for Oracle REST Data Services (ORDS) and Secure Sockets Layer (SSL).

**Note:**

Rotating the ORDS and SSL security certificates is not currently supported for Autonomous Exadata Infrastructure with Autonomous Data Guard enabled.

To rotate security certificates:

1. Open the navigation menu and click **Oracle Database**.

2. Click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.

3. Choose your compartment from the **Compartment** drop-down list.

4. In the **Dedicated Infrastructure** section, click **Autonomous Exadata Infrastructure** to display a list of Autonomous Exadata Infrastructures for your selected compartment.

5. Click the display name of the Autonomous Exadata Infrastructure for which you want to rotate security certificates.

6. Click **Manage Certificates** to display the **Manage Certificates** dialog.

7. Click either **Rotate ORDS Certificate** or **Rotate SSL Certificate**, depending on which operation you want to perform.

   If you are rotating the Oracle REST Data Services certificate, then click **Apply**.

   If you are rotating the SSL certificate, then you must enter the name of the Autonomous Exadata Infrastructure in which you are working to confirm the operation. Click **Apply**.

**Note:**

After you rotate an SSL certificate, you must download wallets for all of the Autonomous Databases in the Autonomous Exadata Infrastructure in which you are working.
To edit the network security groups (NSGs) for your Autonomous Exadata Infrastructure resource

Your Autonomous Exadata Infrastructure instance can use up to five network security groups (NSGs). Note that if you choose a subnet with a security list, the security rules for the infrastructure instance will be a union of the rules in the security list and the NSGs. For more information, see Network Security Groups on page 2841.

1. Open the navigation menu. Under Oracle Database, click Autonomous Transaction Processing.
2. Choose your Compartment.
4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you are interested in.
5. In the Network details, click the Edit link to the right of the Network Security Groups field.

To change an assigned NSG, click the drop-down menu displaying the NSG name, then select a different NSG.

To remove an NSG from your DB system, click the X icon to the right of the displayed NSG name.

7. Click Save.

To move an Autonomous Exadata Infrastructure resource to another compartment

Note:

- To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Database resources, see Details for the Database Service on page 2240.
- If your Autonomous Exadata Infrastructure is in a security zone compartment, the destination compartment must also be in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you wish to move.
5. Click Move Resource.
6. Select the new compartment.
7. Click Move Resource.

For information about dependent resources for Database resources, see Moving Database Resources to a Different Compartment on page 1141.

To terminate an Autonomous Exadata Infrastructure resource

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
4. In the list of Autonomous Exadata Infrastructure resources, click on the display name of the resource you are interested in.
5. Go to More Actions, and then click Terminate.
6. Confirm that you wish to terminate your Autonomous Exadata Infrastructure in the confirmation dialog.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the UpdateAutonomousExadataInfrastructure API operation to configure the automatic maintenance schedule for your infrastructure resource.

Use the GetMaintenanceRun API to view the details of a maintenance run that is scheduled, in progress, or that has ended.

Use the ListMaintenanceRun API to get a list of maintenance runs in a specified compartment.

Use the ChangeAutonomousExadataInfrastructureCompartment API operation to move an Autonomous Exadata Infrastructure resource to another compartment.

Use the TerminateAutonomousExadataInfrastructure API operation to delete an Autonomous Exadata Infrastructure resource.

For More Information

Create and Manage Autonomous Exadata Infrastructure Resources (Fleet Administrator’s Guide to Oracle Autonomous Transaction Processing on Dedicated Exadata Infrastructure)

Creating an Autonomous Container Database

This topic describes how to provision a new Autonomous Container Database using the Oracle Cloud Infrastructure Console or the API. Container databases are only necessary for Autonomous Databases on dedicated Exadata infrastructure. For a brief overview, see Overview of Autonomous Database on Dedicated Exadata Infrastructure on page 1193.

Note:

This topic is not applicable to Autonomous Databases on shared Exadata infrastructure.

Prerequisites

• To create an Autonomous Container Database, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service.

Tip:

See Let database and fleet admins manage Autonomous Databases on page 2151 for sample Autonomous Database policies. See Details for the Database Service on page 2240 for detailed information on policy syntax.

• To create an Autonomous Container Database, you must have an available Autonomous Exadata Infrastructure resource. For information on creating an infrastructure instance, see Creating an Autonomous Exadata Infrastructure Resource on page 1198.

• If you want to create your Autonomous Container Database in a security zone, the Autonomous Exadata Infrastructure that runs the container database must be in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

Using the Oracle Cloud Infrastructure Console

To create an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse or Autonomous Transaction Processing.

2. Under Dedicated Infrastructure, click Autonomous Container Database.
3. Click **Create Autonomous Container Database**.

4. In the **Create Autonomous Container Database** dialog, enter the following database information:
   - **Select a compartment**: Specify the compartment in which you want to create the container database, if different from the default.
   - **Display name**: Enter a description or other information that helps you identify the resource. The display name does not have to be unique. Avoid entering confidential information.
   - **Autonomous Exadata Infrastructure in compartment**: From the drop-down, choose an Autonomous Exadata Infrastructure for your container database. See Creating an Autonomous Exadata Infrastructure Resource on page 1198 for more information.
     
     You can change the compartment containing the Autonomous Exadata Infrastructure you want to use for your container database by clicking the **Change Compartment** link.

5. You can enable Autonomous Data Guard on your primary Autonomous Container Database to create a standby Autonomous Container Database.
   a. Select **Enable Autonomous Data Guard** to provision a peer Autonomous Container Database as a standby database.
   b. Select a compartment in which you want to provision a peer Autonomous Container Database from the **Select peer Autonomous Container Database compartment** drop-down.
   c. You can enter a display name in the **Peer Autonomous Container Database display name** field or accept the default display name. Avoid entering confidential information.
   d. Select a region in which you want to locate the peer Autonomous Container Database from the **Region** drop-down.
   e. Select an Autonomous Exadata Infrastructure to apply to the peer Autonomous Container Database.

   **Note:**
   You must provision the standby Autonomous Container Database with a different Autonomous Exadata Infrastructure from that of the primary database.

   You can change the compartment containing the Autonomous Exadata Infrastructure you want to use for your peer Autonomous Container Database by clicking the **Change Compartment** link.

   f. Select a protection mode for the peer Autonomous Container Database from the **Protection mode** drop-down:
      - **Maximum Availability**: Provides the highest level of data protection that is possible without compromising the availability of a primary database.
      - **Maximum Performance**: Provides the highest level of data protection that is possible without affecting the performance of a primary database. This is the default protection mode.

      See Oracle Data Guard Concepts and Administration for more information about protection modes.

   After you complete this task, the database you initially created is labeled in the Oracle Cloud Infrastructure console database list view as "Primary" and the peer database is labeled as "Standby".

6. Optionally, you can change the default scheduling and maintenance patching type for your Autonomous Container Database maintenance. The patch type choices are Release Update (RU) and Release Update Revision (RUR). The Release Update setting installs only the most current release update, while the Release Update Revision installs the release update plus additional fixes. For information about Release Updates (RUs) and Release Update Revisions (RURs), see Release Update Introduction and FAQ (Doc ID 2285040.1) in the My Oracle Support online help portal *(MOS login required)*.

   **Note:**
   - The patch type you choose for the primary Autonomous Container Database is also applied to the standby database.
   - Scheduled maintenance for a standby Autonomous Container Database must be between one and seven days before scheduled maintenance for a primary Autonomous Container Database.
7. Click **Show Advanced Options** to display the following:

- **Management**: Optionally, you can specify the backup retention policy, which controls the length of time you retain backups in the Autonomous Container Database. The choices are 7 days, 15 days, 30 days, and 60 days. The default setting is 60 days.

  \[
  \text{Note:} \\
  \text{The backup retention policy you specify also applies to the standby Autonomous Container Database.}
  \]

- **Encryption Key**: You can choose encryption based on either Oracle-managed encryption keys or encryption keys that you manage.

  If you choose encryption based on encryption keys that you manage, then you must have access to a valid encryption key.

  \[
  \text{Note:} \\
  \text{Customer-managed encryption keys are not applicable to Autonomous Data Guard-enabled Autonomous Container Databases.}
  \]

  - Select a vault that contains the encryption key you want to use. You can change the compartment containing the vault you want to use by clicking the **Change Compartment** link.
  - Select an encryption key. You can change the compartment containing the encryption key you want to use by clicking the **Change Compartment** link.

  \[
  \text{Note:} \\
  \begin{align*}
  &\text{You cannot change the vault or vault key once the Autonomous Container Database is provisioned.} \\
  &\text{Oracle supports using 256-bit and hardware security module (HSM) encryption keys for Autonomous Container Database encryption.}
  \end{align*}
  \]

  See **Managing Keys** on page 3962 for more information about encryption keys

- **Tagging**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

8. Click **Create Autonomous Container Database**.

**WHAT NEXT?**

After creating an Autonomous Container Database, you can create one or more Autonomous Databases within the container database.

**To configure the Autonomous Container Database maintenance type and scheduling**

1. Click **Configure Maintenance**. In the **Edit Automatic Maintenance** dialog that opens, you can configure both the maintenance schedule and the patch type.

2. For **Maintenance Type**, select either **Release Update (RU)** or **Release Update Revision (RUR)**. Learn more.

3. To configure the maintenance schedule, select **Specify a schedule** in the **Configure the automatic maintenance schedule** section. Choose your preferred month, week, weekday, and start time for container database maintenance. Autonomous Container Database maintenance should be scheduled so that it follows after the maintenance scheduled for the associated Autonomous Exadata Infrastructure. To see the scheduling of the associated Autonomous Exadata Infrastructure, you can click **Show Autonomous Exadata Infrastructure maintenance schedule**. If you have not specified an infrastructure maintenance schedule (and Oracle is
scheduling infrastructure maintenance), your infrastructure maintenance will be scheduled to precede your container database maintenance.

- Under **Maintenance months**, specify at least one month for each quarter during which Autonomous Exadata Infrastructure maintenance will take place.
- Under **Week of the month**, specify which week of the month maintenance will take place. Weeks start on the 1st, 8th, 15th, and 22nd days of the month, and have a duration of 7 days. Weeks start and end based on calendar dates, not days of the week. Maintenance cannot be scheduled for the fifth week of months that contain more than 28 days.
- Under **Day of the week**, specify the day of the week on which the maintenance will occur.
- Under **Start hour**, specify the hour during which the maintenance run will begin.

4. Click **Save Changes**.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the CreateAutonomousContainerDatabase API operation to create an Autonomous container database.

**Managing an Autonomous Container Database**

This topic describes the database management tasks for Autonomous Container Databases that you complete using the Oracle Cloud Infrastructure Console or the API. Container databases are used by Autonomous Databases on dedicated Exadata infrastructure. See Overview of Autonomous Database on Dedicated Exadata Infrastructure on page 1193 for more information.

**Note:**

This topic is not applicable to Autonomous Databases on shared Exadata infrastructure.

The following management operations can be performed on Autonomous Container Databases in Oracle Cloud Infrastructure:

- Edit the backup retention policy. By default, database backups are retained for 60 days. You have the option of retaining backups for 7, 15, 30, or 60 days. The current backup retention policy for an Autonomous Container Database is displayed on the Autonomous Container Database details page.
- Configure the type of database maintenance. You can choose to use Release Update (RU) or Release Update Revision (RUR) updates for your Autonomous Container Database maintenance. Release Update (RU): Autonomous Database installs only the most current release update. Release Update Revision (RUR): Autonomous Database installs the release update plus additional fixes.
  For information about Release Updates (RUs) and Release Update Revisions (RURs), see Release Update Introduction and FAQ (Doc ID 2285040.1) in the My Oracle Support online help portal (MOS login required).
- Configure the scheduling for your Autonomous Container Database.
- View the Autonomous Container Database next scheduled maintenance and maintenance history.
- Immediately patch an Autonomous Container Database.
- Skip a scheduled maintenance run. For container databases, you can skip maintenance runs for up to two consecutive quarters, if necessary.
- Edit the maintenance patch version of your Autonomous Container Database.
- Perform a rolling restart of databases within an Autonomous Container Database. You can perform a “rolling restart” on all the Autonomous Databases in an Autonomous Container Database to ensure that the current memory allocation is optimized. During a rolling restart, each node of an Autonomous Database is restarted separately while the remaining nodes continue to be available. No interruption of service occurs during a rolling restart. You cannot perform a container database restart if a backup is in progress.
- Rotate encryption keys for an Autonomous Container Database.
- Terminate an Autonomous Container Database. Note that you must terminate all Autonomous Databases within a container database before you can terminate the container database itself.
Using the Oracle Cloud Infrastructure Console

To set the backup retention policy for an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. Under Autonomous Database, click Autonomous Container Database.
4. In the list of Autonomous Container Databases, click on the display name of the container database you are interested in.
5. On the Autonomous Container Database details page, under Backup, click the Edit link in the Backup Retention Field.
6. Specify a backup retention period from the list of choices.
7. Click Save Changes.

To configure the automatic maintenance schedule for an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. Under Autonomous Database, click Autonomous Container Database.
4. In the list of Autonomous Container Databases, click on the display name of the container database you are interested in.
5. On the Autonomous Container Database details page, under Maintenance, click the edit link in the Maintenance Details field. In the Edit Automatic Maintenance dialog that opens, you can configure both the maintenance schedule and the patch type.
6. Optionally, you can change the maintenance patch type. To edit this setting, select either Release Update (RU) or Release Update Revision (RUR). Learn more.
7. To configure the maintenance schedule, select Specify a schedule in the Configure the automatic maintenance schedule section. Choose your preferred month, week, weekday, and start time for container database maintenance. Autonomous Container Database maintenance should be scheduled so that it follows after the maintenance scheduled for the associated Autonomous Exadata Infrastructure. To see the scheduling of the associated Autonomous Exadata Infrastructure, you can click Show Autonomous Exadata Infrastructure maintenance schedule. If you have not specified an infrastructure maintenance schedule (and Oracle is scheduling infrastructure maintenance), your infrastructure maintenance scheduling will be automatically modified so that it precedes your container database maintenance during each quarter.
   - Under Maintenance months, specify at least one month for each maintenance quarter during which you want Autonomous Exadata Infrastructure maintenance to occur.
   - Under Week of the month, specify which week of the month maintenance will take place. Weeks start on the 1st, 8th, 15th, and 22nd days of the month, and have a duration of 7 days. Weeks start and end based on calendar dates, not days of the week. Maintenance cannot be scheduled for the fifth week of months that contain more than 28 days.
   - Under Day of the week, specify the day of the week on which the maintenance will occur.
   - Under Start hour, specify the hour during which the maintenance run will begin.
8. Click Save Changes.

To configure the type of maintenance patching for an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. Under Autonomous Database, click Autonomous Container Database.
4. In the list of Autonomous Container Databases, click on the display name of the container database you are interested in.

5. On the Autonomous Container Database details page, under Maintenance, click the Edit link in the Maintenance Details field.

6. In the Automatic Maintenance Schedule dialog, under Maintenance Type, select either Release Update (RU) or Release Update Revision (RUR).
   • Release Update (RU): Autonomous Database installs only the most current release update.
   • Release Update Revision (RUR): Autonomous Database installs the release update plus additional fixes.

7. Optionally, you can configure the automatic maintenance schedule as described in To configure the automatic maintenance schedule for an Autonomous Container Database on page 1209.

8. Click Save Changes.

To view the next scheduled maintenance run of an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. Under Autonomous Database, click Autonomous Container Database.
4. In the list of Autonomous Container Databases, click on the display name of the container database you are interested in.
5. On the Autonomous Container Database details page, under Maintenance, click the View link in the Next Maintenance field.
6. On the Maintenance page, under Autonomous Database Maintenance, click Maintenance. In the list of maintenance events, you can the details of scheduled maintenance runs. Maintenance event details include the following:
   • The status of the scheduled maintenance run
   • The type of maintenance run (quarterly software maintenance or a critical patch)
   • The OCID of the maintenance event.
   • The start time and date of the maintenance

To view the maintenance history of an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. Under Autonomous Database, click Autonomous Container Database.
4. In the list of Autonomous Container Databases, click on the display name of the container database you are interested in.
   a. On the Autonomous Container Database details page, under Maintenance, click the View link in the Next Maintenance field.
5. On the Maintenance page, under Autonomous Database Maintenance, click Maintenance History. In the list of past maintenance events, you can click on an individual event title to read the details of the maintenance that took place. Maintenance event details include the following:
   • The category of maintenance (quarterly software maintenance or a critical patch)
   • Whether the maintenance was scheduled or unplanned
   • The OCID of the maintenance event.
   • The start time and date of the maintenance

To reschedule or skip scheduled maintenance for an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the Autonomous Database section, click Autonomous Container Database.
4. In the list of Autonomous Container Databases, click the display name of the container database that you want to manage.
5. On the Autonomous Container Database details page, in the Maintenance section, click the View link in the Next Maintenance field.
6. On the Maintenance page, any container database maintenance events planned for the next 15 days will appear in the list of maintenance events.

To skip scheduled maintenance for a container database, click Skip.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot skip scheduled maintenance more than twice, consecutively.</td>
</tr>
</tbody>
</table>

To reschedule maintenance, click Edit and enter a start time for the update in the Edit Maintenance dialog. Make sure that your specified container database maintenance window is later in the quarter than your scheduled Exadata infrastructure maintenance.

To immediately patch an Autonomous Container Database

After you schedule maintenance for your Autonomous Container Databases, you can patch the component, immediately, at any time before scheduled maintenance occurs. If you choose to patch a Autonomous Container Database, immediately, while another component is in the process of maintenance, then this maintenance operation gets queued and will begin, in turn.

1. Open the navigation menu. Click Oracle Database, click Autonomous Transaction Processing or Autonomous Data Warehouse.
2. Choose your compartment from the Compartment drop-down.
3. In the Dedicated Infrastructure section, click Autonomous Container Database to display a list of Autonomous Container Databases for your selected compartment.
4. Click the display name of the Autonomous Container Database that you want to patch.
5. On the Autonomous Container Database Details page, in the Maintenance section, click the View link in the Next Maintenance field to display the Maintenance page for the Autonomous Container Database that you want to patch.
6. In the Autonomous Container Database section, click the Patch Now link in the Scheduled Start Time field to display the Run Maintenance dialog.
7. Click Run Maintenance to start the patching operation.

To edit the maintenance patch version of an Autonomous Container Database

You can select from a list of available patches of either maintenance type (release update or release update revision) to apply to your Autonomous Container Database during scheduled maintenance.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your compartment from the Compartment drop-down.
3. In the Autonomous Database section, click either Autonomous Container Database or Autonomous Exadata Infrastructure.
4. In the list of Autonomous Container Databases, click the display name of the container database that you want to manage. Alternatively, if you clicked Autonomous Exadata Infrastructure in the previous step, then click the name of the Exadata infrastructure that contains the Autonomous Container Database that you want to edit.
5. On the Autonomous Container Database details page or the Autonomous Exadata Infrastructure Details page, in the Maintenance section, click the View link in the Next Maintenance field.
6. On the Maintenance page, click the Edit link in the Version field to display the Edit Maintenance dialog.
7. Select the database version with which you want to patch your Autonomous Container Database.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You must select a version that is later than the current version of the Autonomous Container Database.</td>
</tr>
</tbody>
</table>
• The list of available versions may contain both release update (RU) and release update revision (RUR) maintenance types. Your configured maintenance policy does not change if you choose a maintenance type other than that for which your Autonomous Container Database maintenance schedule is configured.

8. Click Save Changes.

To perform a rolling restart of databases within an Autonomous Container Database

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. Under Autonomous Database, click Autonomous Container Database.

4. In the list of Autonomous Container Databases, click on the display name of the container database you are interested in.

5. On the Autonomous Container Database details page, click Restart.

6. In the confirmation dialog, type the name of the Autonomous Container Database.

7. Click Restart.

To move an Autonomous Container Database to another compartment

Note:

• To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Database resources, see Details for the Database Service on page 2240.

• If your Autonomous Container Database is in a security zone, the destination compartment must also be in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your Compartment.

3. Under Autonomous Database, click Autonomous Container Database.

4. In the list of Autonomous Container Databases, click on the display name of the container database you wish to move.

5. Click Move Resource.

6. Select the new compartment.

7. Click Move Resource.

For information about dependent resources for Database resources, see Moving Database Resources to a Different Compartment on page 1141.

To rotate the encryption key for an Autonomous Container Database

Rotating the encryption key creates a new version of the vault key that replaces the current version of the vault key.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.

2. Choose your compartment from the Compartment drop-down.

3. In the Dedicated Infrastructure section, click Autonomous Container Database to display a list of Autonomous Container Databases for your selected compartment.

4. Click the display name of the database for which you want to rotate the encryption key to display the details page for that database.

5. Click Rotate Encryption Key to display a confirmation dialog.
6. Click **Rotate Key**.

**To rotate the encryption key for an Autonomous Database**

Rotating the encryption key creates a new version of the vault key that replaces the current version of the vault key.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your compartment from the **Compartment** drop-down.
3. Click the display name of the Autonomous Database for which you want to rotate the encryption key to display the details page for that database.

   **Note:**

   The Autonomous Database you choose must be on dedicated Exadata infrastructure and in an **Available** state.

4. Click the **More Actions** drop-down.
5. Click **Rotate Encryption Key** to display a confirmation dialog.
6. Click **Rotate Key**.

**To terminate an Autonomous Container Database**

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. In the **List Scope** section, if not already selected, then select the compartment that contains the Autonomous Container Database you want to terminate from the **Compartment** drop-down.
3. In the **Dedicated Infrastructure** section, click **Autonomous Container Database** to display a list of Autonomous Container Databases contained in the compartment.
4. Click the display name of the Autonomous Container Database that you want to terminate to display the details page for that database.
   
   If you want to terminate a standby Autonomous Container Database, then click the display name of the database you want to terminate that is labeled "Standby" to display the details page for that database.
5. Click **Terminate** to display a confirmation dialog.
6. You must enter the display name of the Autonomous Container Database to confirm that you want to terminate the database.

   **Note:**

   Terminating a standby Autonomous Container Database disables Autonomous Data Guard and affects high availability and disaster recovery for any associated peer Autonomous Container Databases.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the **UpdateAutonomousContainerDatabase** API operation to perform the following management actions:

- Set the backup retention period for an Autonomous Container Database.
• Set the maintenance patching type of an Autonomous Container Database.

Use the UpdateMaintenanceRun API operation to skip a container database maintenance run.

Use the ListMaintenanceRun API to get a list of maintenance runs in a specified compartment. Can be used to see maintenance history and scheduled maintenance runs.

Use the RestartAutonomousContainerDatabase API operation to perform a rolling restart on a container database.

Use the ChangeAutonomousContainerDatabaseCompartment API operation to move a container database to another compartment.

Use the TerminateAutonomousContainerDatabase API operation to terminate a container database.

Managing a Standby Autonomous Container Database

Enabling Autonomous Data Guard on an Autonomous Container Database creates a standby (peer) Autonomous Container Database that provides data protection, high availability, and facilitates disaster recovery for the primary database.

Once the standby database is provisioned, you can perform various management tasks related to the standby database, including:

• Manually switching over a primary database to a standby database
• Manually failing over a primary database to a standby database
• Reinstating a primary database to standby role after failover
• Terminating a standby database

See

• Creating an Autonomous Container Database on page 1205 for information about enabling Autonomous Data Guard
• To terminate an Autonomous Container Database

Autonomous Data Guard-enabled databases are identified in the Oracle Cloud Infrastructure console as "Primary" and "Standby" depending on the role assigned to a given database, and the status of Autonomous Data Guard is displayed in the Autonomous Data Guard column.

When you view the details page of a particular Autonomous Container Database, the Autonomous Data Guard section displays the status of Autonomous Data Guard and the state of the peer database associated with the database you are viewing. Additionally, in the Resources section of the details page, you can click Autonomous Data Guard to view Autonomous Data Guard configuration details and information, such as transport lag and apply lag, for peer Autonomous Container Databases.

Using the Oracle Cloud Infrastructure Console

Use the Oracle Cloud Infrastructure console to perform the following Autonomous Data Guard management tasks.

To switch over a primary database to a standby database

When you switch a primary Autonomous Container Database over to a standby Autonomous Container Database, you change the roles of the respective databases.

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. If you are not already in the compartment that contains the Autonomous Container Database you want to switch over, then choose the appropriate compartment from the Compartment drop-down in the List Scope section.
3. In the Dedicated Infrastructure section, click Autonomous Container Database to display a list of Autonomous Container Databases for the compartment. Peer databases are labeled as "Primary" and "Standby" in the list.
4. Click the display name of the Autonomous Container Database you want to switch to display the details page for that database.
5. In the **Resources** section click **Autonomous Data Guard Associations** to display a list of peer databases for the Autonomous Container Database you are managing.

The state of each of the databases must be **Available** to perform a switchover.

6. Click the ellipse in the **Created** column and click **Switchover**.

The states of the peer databases become **Role Change in Progress...** until the switchover action is complete.

At the conclusion of the operation, the respective roles of the two Autonomous Container databases change. The primary database assumes the standby role and the standby database assumes the primary role.

*To fail over a primary database to a standby database*

In the event that a primary Autonomous Container Database becomes unavailable, you can fail over the primary database to the standby Autonomous Container Database.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse, Autonomous JSON Database**, or **Autonomous Transaction Processing**.

2. If you are not already in the compartment that contains the Autonomous Container Database you want to switch over, then choose the appropriate compartment from the **Compartment** drop-down in the **List Scope** section.

3. In the **Dedicated Infrastructure** section, click **Autonomous Container Database** to display a list of Autonomous Container Databases for the compartment. Peer databases are labeled as "Primary" and "Standby" in the list.

4. Click the display name of the standby Autonomous Container Database associated with the primary Autonomous Container Database that you want to fail over to display the details page for that database.

5. In the **Resources** section click **Autonomous Data Guard Associations** to display a list of peer databases for the primary database you are managing.

6. For the primary Autonomous Container Database you are failing over, click the ellipse in the **Created** column and click **Failover**.

7. Confirm that you want to perform the failover operation.

**Caution:**

Fail over to a standby Autonomous Container Database only in the event of a catastrophic failure of the primary database, when there is no possibility of recovery. Failover can result in data loss, depending on the protection mode in effect at the time the primary database fails.

The states of the peer databases become **Role Change in Progress...** until the failover action is complete.

At the conclusion of the operation, the respective roles of the two Autonomous Container databases change. The primary database is labeled as "Disabled Standby" and the standby database assumes the primary role.

*To reinstate a primary database to its former standby role*

After a failover has occurred and the failed primary Autonomous Container Database assumes a disabled, standby role, you can reinstate the failed database to an enabled, standby role.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse, Autonomous JSON Database**, or **Autonomous Transaction Processing**.

2. If you are not already in the compartment that contains the Autonomous Container Database you want to switch over, then choose the appropriate compartment from the **Compartment** drop-down in the **List Scope** section.

3. In the **Dedicated Infrastructure** section, click **Autonomous Container Database** to display a list of Autonomous Container Databases for the compartment. The primary database that you failed over is labeled as "Disabled Standby" in the list.

4. Click the display name of the disabled standby Autonomous Container Database that you want to reinstate.

5. In the **Resources** section click **Autonomous Data Guard Associations** to display a list of peer databases for the primary database you are managing.
6. For the Autonomous Container Database you are reinstating, click the ellipsis in the **Created** column and click **Reinstate**.

   The states of the peer databases become **Role Change in Progress**... until the reinstate action is complete.

At the conclusion of the operation, the role of the original primary database changes from disabled standby to standby. You can now perform a switchover operation to revert the respective databases to their original roles.

See **To manually switch over a primary database to a standby database**

**Autonomous Database Tools**

**Autonomous Database Development and Administration Tools**

This topic describes the Oracle Database tools available for Autonomous Database using the Console and how to access them using the Console. The following tools can be accessed directly from the Oracle Cloud Infrastructure Console:

- **Oracle Database Actions** on page 1216
- **Oracle Application Express** on page 1217
- **Oracle Machine Learning User Administration** on page 1217 (available on shared Exadata infrastructure only)

**Tip:**

Autonomous Database supports a range of other Oracle and third-party tools and applications. See **Autonomous Data Warehouse Tools and Application Test Matrix** to learn about other tools you can use with your Autonomous Database.

For Autonomous Databases on shared Exadata infrastructure, additional tools can be accessed through the **Service Console**.

**Oracle Database Actions**

Database Actions is a web-based interface that uses Oracle REST Data Services to provide development, data tools, administration and monitoring features for Oracle Autonomous Database. Database is available for databases with both the dedicated Exadata infrastructure and shared Exadata infrastructure deployment options.

The main features of are:

**Development**

- **SQL**: Enter and execute SQL and PL/SQL commands, and create database objects.
- **Data Modeler**: Create diagrams from existing database schemas, generate DDL statements, and create reports.
- **APEX**: Link to the Oracle Application Express sign-in page. Application Express is a rapid web application development platform for the Oracle database.
- **REST**: Develop RESTful web services and ensure secure access.
- **JSON**: Manage and query JSON collections. JSON is available only if you are signed in as a database user with the SODA_APP role.

**Data Tools**

- **Data Load**: Load or access data from local files or remote databases.
- **Catalog**: Understand data dependencies and the impact of changes.
- **Data Insights**: Discover anomalies, outliers, and hidden patterns in your data.
- **Business Models**: Create business models for performance and analysis.
- **Data Transforms**: Design your data flows and workflows graphically. Data Transforms is available only to an Oracle Data Integrator on Oracle Cloud Marketplace user that has connectivity enabled from Database Actions in the Oracle Data Integrator user interface.


Administration

- **Database Users**: Perform user management tasks such as create, edit, and REST enable users. Database Users is available only if you are signed in as a database user with administrator rights.

Monitoring

- Monitor database activity and performance using various tools. Monitoring is available only on dedicated Exadata infrastructure and only if you are signed in as a database user with administrator rights.

Complete product information can be found in About Database Actions.

Oracle Application Express

Oracle Application Express (APEX) is a low-code development platform that enables you to build scalable, secure enterprise applications with world-class features that can be deployed anywhere. APEX provides you with an easy-to-use browser-based environment to load data, manage database objects, develop REST interfaces, and rapidly build applications for both desktop and mobile devices.

Oracle Application Express is available for databases with both the dedicated Exadata infrastructure and shared Exadata infrastructure deployment options.

See Oracle Application Express

For complete information, see the APEX topics in the Autonomous Transaction Processing and the Autonomous Data Warehouse user guides. Use the following links:

- Using Oracle Autonomous Transaction Processing
- Using Oracle Autonomous Data Warehouse

Oracle Machine Learning User Administration

Oracle Machine Learning is a collaborative web-based interface that provides a development environment to create data mining notebooks where you can perform data analytics, data discovery and data visualizations. Using the Oracle Cloud Infrastructure Console, you can quickly get to the Oracle Machine Learning User Administration interface to create and manage users.

Machine Learning is currently available for databases with shared Exadata infrastructure only.

Using the Oracle Cloud Infrastructure Console

For Autonomous Databases on Shared Exadata Infrastructure

To access Oracle Database Actions

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you want to work with.
4. Click the Tools tab on the Autonomous Database Details page.
5. Click Open Database Actions

To access Oracle Application Express from an Autonomous Database

To access the Oracle Application Express (Oracle APEX) development environment from an Autonomous Database with the APEX workload type:

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Click Autonomous Database to display a list of Autonomous Databases of all workload types.
3. If you are not in the correct compartment, then select the compartment from the Compartment drop-down that contains the database for which you want to change the workload type.
4. Click the display name of the Autonomous Database of APEX workload type from which you want to access Oracle Application Express to display the Autonomous Database Details page for that database.
5. Click the **Tools** tab to display administration and developer tools available for the database.

6. Click **Open APEX** to access the Oracle APEX sign-in page.

   Additionally, you can access Oracle APEX from the APEX Instance details page, as follows:
   
   a. On the Autonomous Database Details page click the instance name in the **APEX Instance** section.
   
   b. Click **Launch APEX**.

7. Sign into Oracle APEX using the ADMIN password for the Autonomous Database.

**WHAT NEXT?**

- Create an APEX Workspace - Data Warehouse | Transaction Processing
- Access APEX App Builder - Data Warehouse | Transaction Processing
- Use web services with APEX - Data Warehouse | Transaction Processing

**To switch between database details and Oracle APEX instance details**

When you create an Autonomous Database of the APEX workload type, you create a database instance that is optimized for working with Oracle Application Express (Oracle APEX). Oracle APEX-related activities are displayed on a details page separate from that of the database.

To view the Oracle APEX instance details page:

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Click **Autonomous Database** to display a list of Autonomous Databases of all workload types.
3. If you are not in the correct compartment, then select the compartment from the **Compartment** drop-down that contains the database for which you want to view the details.
4. Click the display name of the Autonomous Database of APEX workload type to display the Autonomous Database Details page for that database.
5. In the **APEX Instance** section, click the instance name link to display the APEX Instance Details page.

You can switch back to the database details page by clicking the database name in the **APEX Instance Information** tab.

**To access Oracle Machine Learning's User Administration Interface**

To use Oracle Machine Learning with your Autonomous Database, you must first create a user account within the application. The following steps explain how to navigate to the User Administration interface for Machine Learning from the Autonomous Database details page within the Console.

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose your **Compartment**.
3. In the list of Autonomous Databases, click on the display name of the database you want to work with.
4. Click the **Tools** tab on the Autonomous Database Details page.
5. Click **Open Oracle ML User Administration**

**For Autonomous Databases on Dedicated Exadata Infrastructure**

The Console provides access URLs for Application Express (APEX) and SQL Developer Web that you can use to connect to these applications. The URLs only work from browsers within the same VCN as the Autonomous Database being accessed by the applications. Therefore, to use these URLs, you will need to open a browser running on a computer that meets one of the following conditions:

- The computer is a Compute instance is provisioned in the VCN of the Autonomous Database.
- The computer has a direct connection to the VCN of the Autonomous Database

To access APEX or SQL Developer Web, paste the appropriate access URL into the browser's address field, and then provide the Autonomous Database username and password when prompted. For more information on APEX, see the APEX documentation. For more information on SQL Developer Web, see Oracle SQL Developer Web.
The following tasks explain how to obtain an access URLs for APEX and SQL Developer Web.

To obtain the access URL for Oracle Database Actions for an Autonomous Database on dedicated Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you want to work with.
4. Click the Tools tab on the Autonomous Database Details page.
5. Click Open Database Actions

To obtain the access URLs for Oracle Application Express (APEX) for an Autonomous Database on dedicated Exadata infrastructure

1. Open the navigation menu. Under Oracle Database, click Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click on the display name of the database you want to work with.
4. Click the Tools tab on the Autonomous Database Details page.
5. Click Open APEX

Using Your Autonomous Database

The topics listed in this section provide detailed information and instructions on how to use your Autonomous Database database on shared Exadata infrastructure and dedicated Exadata infrastructure.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Exadata Infrastructure Type</th>
</tr>
</thead>
</table>
| How to Create a Database Link                       | Explains how to use database links to Oracle databases that are accessible from an Autonomous Database | Shared
| Database Link Required Privileges                  | Details the privileges required for a non-admin user to use database links | Shared
| Manage Optimizer Statistics                         | Describes commands for gathering optimizer statistics or enabling optimizer hints | Shared
| Manage Automatic Workload Repository (AWR) Retention | Includes information about controlling the retention time period for Autonomous Database performance data | Shared
| Predefined Database Service Names Resources and Connections | Details the database service names for an Autonomous Database | Shared
| Predefined Job Classes with Oracle Scheduler        | Explains how to control the priority of user requests in an Autonomous Database | Shared
| Managing Concurrency and Priorities Idle Time Limits and MAX_IDLE_TIME | Explains how to control session time limits in an Autonomous Database | Shared
| Perform Manual Backups                              | Explains how to manually back up Autonomous Databases to Object Storage    | Shared
|                                                    |                                                                             | Dedicated                   |
Overview of the Always Free Autonomous Database

Oracle Cloud Infrastructure's Always Free Autonomous Database is part of Oracle Cloud Infrastructure's Free Tier of services. You can provision up to two Always Free Autonomous Databases in the home region of your tenancy. These databases are provided free of charge, and they are available to users of both free and paid accounts. You can use these Autonomous Databases for small-scale applications, for development, or testing purposes, or for learning about and exploring Oracle Cloud Infrastructure.

Always Free Autonomous Database versions

Always Free Autonomous Databases support only a single Oracle Database version.

- You can see only the installed Always Free database version on the details page.
- If your Always Free database is not the latest version, Oracle automatically migrates it to the latest version at a preselected date about which you will be notified several weeks in advance. You can also update the database by selecting the version on the database details page. See To create an Always Free Autonomous Database on page 1159 for more information.

Note:

- You can provision Autonomous Databases only in your Home Region.
- Not all regions support the same database version. The supported version may be 19c-only or 21c-only, depending on the region.
- You cannot create an Always Free Autonomous Database in any Home Region where Always Free Autonomous Databases are not supported. To learn which regions support them, see Data Regions for Platform and Infrastructure Services.

Always Free Autonomous Database Specifications

- **Processor:** 1 Oracle CPU processor (cannot be scaled)
- **Memory:** 8 GB RAM
- **Database Storage:** 20 GB storage (cannot be scaled)
- **Workload Type:** Your choice of either the transaction processing or data warehouse workload type
  - The **Autonomous Transaction Processing** workload type configures the database for a transactional workload, with a bias towards high volumes of random data access.
    - For a complete product overview of Autonomous Transaction Processing, see Autonomous Transaction Processing. For Autonomous Transaction Processing tutorials, see Quick Start tutorials.
  - The **Autonomous Data Warehouse** workload type configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
    - For a complete product overview of Autonomous Data Warehouse, see Autonomous Data Warehouse. For Autonomous Data Warehouse tutorials, see Quick Start tutorials.
- **Database Version:** Oracle Database 19c or Oracle Database 21c.
- **Infrastructure Type:** Shared Exadata infrastructure
- **Maximum Simultaneous Database Sessions:** 20

Lifecycle for Always Free Autonomous Databases

After provisioning, you can continue using your Always Free Autonomous Database for as long as you want at no charge. You can terminate the database at any time.

Lifecycle Management for Inactive Always Free Autonomous Databases

If your Always Free Autonomous Database has no activity for a period of 7 consecutive days, the Database service will stop the database automatically. If this happens, restart the database and continue using it. If your Always Free Autonomous Database remains in a stopped state for 3 consecutive months, the database will be reclaimed (automatically terminated) by the Database service.
Using Events and Notifications to Stay Informed About Inactive Always Free Autonomous Databases

You can use Oracle Cloud Infrastructure's Events service to send structured JSON messages about your Always Free Autonomous Database lifecycle events to applications used for automation. For example, you can create automatic email, Slack, PagerDuty, or HTTPS notifications (using the Notifications service) to be alerted if a database is going to be stopped or terminated in the next 48 hours. You can also set up notifications to be alerted when a database is automatically stopped or and terminated.

See the following topics for more information:

- Getting Started with Events on page 1786 for details on working with Events messages.
- Autonomous Database Event Types for details on the currently available Always Free Autonomous Database lifecycle events messages.
- How Notifications Works for an overview of setting up automated notifications based on the JSON messages emitted by the Events service.

Exadata Cloud Service

Exadata Cloud Service allows you to leverage the power of Exadata in the cloud. You can provision flexible X8M systems that allow you to add database compute servers and storage servers to your system as your needs grow. X8M systems offer RDMA over Converged Ethernet (RoCE) networking for high bandwidth and low latency, persistent memory (PMEM) modules, and intelligent Exadata software. X8M systems can be provisioned using an shape equivalent to a quarter rack X8 system, and then database and storage servers can be added at any time after provisioning. For more information on X8M systems, see Overview of X8M Scalable Exadata Infrastructure on page 1227.

X8 and X7 systems are also available in fixed-shapes (quarter, half, and full rack systems). These systems use InfiniBand networking, and do not have the ability to scale database and storage servers. You can also provision an Exadata base system, which has a smaller capacity than a quarter rack system.

For all Exadata Cloud Service instances, you can configure automatic backups, optimize for different workloads, and scale the OCPU and storage allocations as needed.

Note:

Exadata Cloud Service instances launched on or after March 14, 2019 run Oracle Linux 7. Previously launched systems are running Oracle Linux 6. See OS Updates on page 1274 for important information about updating existing Exadata DB system operating systems.

Supported Database Edition and Versions

Exadata Cloud Service instances require Enterprise Edition - Extreme Performance. This edition provides all the features of Oracle Database Enterprise Edition, plus all the database enterprise management packs and all the Enterprise Edition options, such as Oracle Database In-Memory and Oracle Real Application Clusters (RAC).

Exadata Cloud Service instances support the following software releases:

- Oracle Database 19c (19.0)
- Oracle Database 18c (18.0)
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1)
- Oracle Database 11g Release 2 (11.2)

Note:

- If you plan to run Oracle Database 19c on a cloud VM cluster or DB system in the Exadata Cloud Service, you must specify version 19c when you create the resource. Earlier database versions are supported on a 19c cloud VM cluster or DB system, and can be created at anytime.
Cloud VM clusters and DB systems created with earlier Oracle Database versions will not automatically support Oracle Database 19c.

- For information on upgrading an existing 18c or earlier database to Oracle Database 19c, see Upgrading Exadata Databases on page 1301.

Subscription Types

The only subscription type available for Exadata Cloud Service instances is the Monthly Flex purchase model under Universal Credit Pricing. See the Universal Credit Pricing FAQ for more information.

Metering Frequency and Per-Second Billing

For each Exadata Cloud Service instance you provision, you are billed for the infrastructure for a minimum of 48 hours, and then by the second after that. Each OCPU you add to the system is billed by the second, with a minimum usage period of 1 minute. For X8M systems, if you terminate the cloud VM cluster and do not terminate the cloud Exadata infrastructure resource, billing will continue for the infrastructure resource.

Scaling Options

Three kinds of scaling operations are supported for an Exadata Cloud Service:

- For all Exadata Cloud Service instances, you can scale the compute node processing power within the provisioned system, adding or subtracting CPU cores as needed.
- For X8M systems, the flexible shape allows you to add additional database and storage servers to the cloud Exadata infrastructure resource as you need them.
- For X6, X7 and X8 Exadata DB systems, you can scale by moving the system to a different shape configuration, for example, from a quarter rack to a half rack.

For more information on each type of scaling, see Scaling an Exadata Cloud Service Instance on page 1229.

Scaling CPU Cores Within an Exadata Cloud Service Instance

If an Exadata Cloud Service instance requires more compute node processing power, you can scale up the number of enabled CPU cores symmetrically across all the nodes in the system as follows:

**X8M flexible infrastructure systems:** You can scale CPU cores in multiples of the number of database servers currently provisioned for the cloud VM cluster. For example, if you have 6 database servers provisioned, you can add CPU cores in multiples of 6. At the time of provisioning, X8M systems have 2 database servers. For more information on adding compute and storage resources to an X8M system, see Scaling Exadata X8M Compute and Storage on page 1230.

**Non-X8M fixed-shape systems:** For a base system or an X7 or X8 quarter rack, you can scale in multiples of 2 across the 2 database compute nodes. For an X7 or X8 half rack, you can scale in multiples of 4 across the 4 database compute nodes. For an X7 or X8 full rack, you can scale in multiples of 8 across the 8 database compute nodes.

For a non-metered service instances, you can temporarily modify the compute node processing power (bursting) or add compute node processing power on a more permanent basis. For a metered service instance, you can simply modify the number of enabled CPU cores.

You can provision an Exadata Cloud Service instance with zero CPU cores, or scale the service instance down to zero cores after you provision it. With zero cores, you are billed only for the infrastructure until you scale up the system. For detailed information about pricing, see Exadata Cloud Service Pricing.

Tip:

OCPUs scaling activities are done online with no downtime.

For information on CPU cores per configuration, see Exadata Shape Configurations on page 1223. To learn how to scale a system, see To scale CPU cores in an Exadata Cloud Service cloud VM cluster or DB system on page 1258.
Scaling X6, X7 and X8 Exadata DB System Configurations

Scaling an Exadata X6, X7, or X8 Exadata Cloud Service instance by moving to a shape with more capacity enables you to meet the needs of your growing workload. This is useful when a database deployment requires:

- Processing power that is beyond the capacity of the current system configuration.
- Storage capacity that is beyond the capacity of the current system configuration.
- A performance boost that can be delivered by increasing the number of available compute nodes.
- A performance boost that can be delivered by increasing the number of available Exadata Storage Servers.

You can move your workloads to a larger fixed shape (X7 and X8 hardware shapes), or move to the flexible X8M shape that allows for easy expansion of compute and storage resources as your workloads grow.

To assist with moving your database deployments between Exadata Cloud Service instances, you can restore a backup to a different service instance that has more capacity, or create a Data Guard association for your database in a service instance with more capacity, and then perform a switchover so that your new standby database assumes the primary role. To start the process, contact Oracle and request a service limit increase so that you can provision the larger service instance needed by your database.

Exadata Shape Configurations

Each Exadata Cloud Service instance consists of compute nodes and storage servers. The compute nodes are each configured with a Virtual Machine (VM). You have root privilege for the compute node VMs, so you can load and run additional software on them. However, you do not have administrative access to the Exadata infrastructure components, including the physical compute node hardware, network switches, power distribution units (PDUs), integrated lights-out management (ILOM) interfaces, or the Exadata Storage Servers, which are all administered by Oracle.

For X8M systems, the Exadata hardware is administered through two resource types, the cloud Exadata infrastructure resource and the cloud VM cluster. See The New Exadata Cloud Service Resource Model on page 1228 for more details.

For X6, X7, and X8 systems, the Exadata hardware is administered through the DB system resource.

For all hardware models, you have full administrative privileges for your databases, and you can connect to your databases by using Oracle Net Services from outside the Oracle Cloud Infrastructure. You are responsible for database administration tasks such as creating tablespaces and managing database users. You can also customize the default automated maintenance set up, and you control the recovery process in the event of a database failure.

For full details on the available shape configurations, see Exadata Fixed Hardware Shapes: X6, X7, X8 and Exadata Base on page 1351

Customer-Managed Keys in Exadata Cloud Service

Customer-managed keys for Exadata Cloud Service is a feature of Oracle Cloud Infrastructure Vault service that enables you to encrypt your data using encryption keys that you control. The Vault service provides you with centralized key management capabilities that are highly available and durable. This key-management solution also offers secure key storage using isolated partitions (and a lower-cost shared partition option) in FIPS 140-2 Level 3-certified hardware security modules, and integration with select Oracle Cloud Infrastructure services. Use customer-managed keys when you need security governance, regulatory compliance, and homogenous encryption of data, while centrally managing, storing, and monitoring the life cycle of the keys you use to protect your data.

You can:

- Enable customer-managed keys when you create databases in Exadata Cloud Service
- Switch from Oracle-managed keys to customer-managed keys on databases that are not enabled with Oracle Data Guard
- Rotate your keys to maintain security compliance

Related Topics

- To create a database in an existing Exadata Cloud Service instance on page 1307
### Storage Configuration

When you launch an Exadata Cloud Service instance, the storage space inside the Exadata storage servers is configured for use by Oracle Automatic Storage Management (ASM). By default, the following ASM disk groups are created:

- The DATA disk group is intended for the storage of Oracle Database data files.
- The RECO disk group is primarily used for storing the Fast Recovery Area (FRA), which is an area of storage where Oracle Database can create and manage various files related to backup and recovery, such as RMAN backups and archived redo log files.
- The `/acfs` file systems contain system files that support various operations. You should not store custom files, Oracle Database data files, or backups inside the ACFS disk groups. Custom ACFS mounts can be created using the DATA ASM disk group for files that are not service-related.

The disk group names contain a short identifier string that is associated with your Exadata Database machine environment. For example, the identifier could be C2, in which case the DATA disk group would be named DATAC2, the RECO disk group would be named RECOC2, and so on.

In addition, you can create a SPARSE disk group. A SPARSE disk group is required to support Exadata snapshots. Exadata snapshots enable space-efficient clones of Oracle databases that can be created and destroyed very quickly and easily. Snapshot clones are often used for development, testing, or other purposes that require a transient database.

Note that you cannot change the disk group layout after service creation.

### Impact of Configuration Settings on Storage

If you choose to perform database backups to the Exadata storage, or to create a sparse disk group, or to do both, your choices profoundly affect how storage space in the Exadata storage servers is allocated to the ASM and sparse disk groups.

The table that follows shows the approximate percentages of storage allocated for DATA, RECO, and SPARSE disk groups for each possible configuration.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
<th>DATA Disk Group</th>
<th>RECO Disk Group</th>
<th>SPARSE Disk Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database backups on Exadata storage: No</td>
<td>80 %</td>
<td>20 %</td>
<td>0 %</td>
</tr>
<tr>
<td>Sparse disk group: No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database backups on Exadata storage: Yes</td>
<td>40 %</td>
<td>60 %</td>
<td>0 %</td>
</tr>
<tr>
<td>Sparse disk group: No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database backups on Exadata storage: No</td>
<td>60 %</td>
<td>20 %</td>
<td>20 %</td>
</tr>
<tr>
<td>Sparse disk group: Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Database Configuration Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>DATA Disk Group</th>
<th>RECO Disk Group</th>
<th>SPARSE Disk Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database backups on Exadata storage: Yes</td>
<td>35 %</td>
<td>50 %</td>
<td>15 %</td>
</tr>
<tr>
<td>Sparse disk group: Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Moving Databases to Oracle Cloud Exadata Systems Using Zero Downtime Migration

Oracle now offers the **Zero Downtime Migration** service, a quick and easy way to move on-premises Oracle Databases and Oracle Cloud Infrastructure Classic databases to Oracle Cloud Infrastructure. You can migrate databases to the following types of Oracle Cloud Infrastructure systems: Exadata, Exadata Cloud@Customer, bare metal, and virtual machine.

Zero Downtime Migration leverages Oracle Active Data Guard to create a standby instance of your database in an Oracle Cloud Infrastructure system. You switch over only when you are ready, and your source database remains available as a standby. Use the Zero Downtime Migration service to migrate databases individually or at the fleet level. See **Move to Oracle Cloud Using Zero Downtime Migration** for more information.

Exadata Shape Configurations

This topic describes the available Exadata Cloud Service instance shapes in Oracle Cloud Infrastructure.

See the following sections for shape specifications:

- Exadata X8M on page 1225
- Exadata Base System on page 1226
- Exadata X8 Shapes on page 1226
- Exadata X7 Shapes on page 1227
- Exadata X6 Shapes on page 1227

**Exadata X8M**

After provisioning, the X8M shape is expandable, unlike X6, X7, and X8 shapes. The values in the table that follows represent the specifications for an X8M cloud service instance that has not been expanded. The initial configuration of 2 database servers and 3 storage servers is similar to the quarter rack shape offered for X6, X7 and X8 infrastructure resources.

**X8M Capacity at Provisioning**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shape Name</td>
<td>Exadata X8M-2</td>
</tr>
<tr>
<td>Number of Compute Nodes</td>
<td>2 (value can increased after provisioning)</td>
</tr>
<tr>
<td>Total Minimum Number of Enabled CPU Cores</td>
<td>0</td>
</tr>
<tr>
<td>Total Maximum Number of Enabled CPU Cores</td>
<td>100 (for 2 initial database servers)</td>
</tr>
<tr>
<td>Total RAM Capacity</td>
<td>2780 GB (initial value)</td>
</tr>
<tr>
<td>Number of Exadata Storage Servers</td>
<td>3 (value can increased after provisioning)</td>
</tr>
<tr>
<td>Total Raw Flash Storage Capacity</td>
<td>76.8 TB (for 3 initial storage servers)</td>
</tr>
<tr>
<td>Total Usable Storage Capacity</td>
<td>149 TB (for 3 initial storage servers)</td>
</tr>
</tbody>
</table>

**X8M Expansion Server Capacity**

When you add additional database or storage servers to an X8M system, the expansion servers have the following capacity.
Database

Database Servers

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum OCPUs</td>
<td>50 OCPUs</td>
</tr>
<tr>
<td>Total memory available</td>
<td>1,390 GB</td>
</tr>
</tbody>
</table>

Storage Servers

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total usable disk capacity</td>
<td>49.9 TB</td>
</tr>
<tr>
<td>Persistent memory</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Total flash capacity</td>
<td>25.6 TB</td>
</tr>
</tbody>
</table>

**Exadata Base System**

An Exadata base system is a fixed shape similar in size to a *quarter rack*, with some differences in capacity.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shape Name</td>
<td>Exadata.Base.48</td>
</tr>
<tr>
<td>Number of Compute Nodes</td>
<td>2</td>
</tr>
<tr>
<td>Total Minimum Number of Enabled CPU Cores</td>
<td>0</td>
</tr>
<tr>
<td>Total Maximum Number of Enabled CPU Cores</td>
<td>48</td>
</tr>
<tr>
<td>Total RAM Capacity</td>
<td>720 GB</td>
</tr>
<tr>
<td>Number of Exadata Storage Servers</td>
<td>3</td>
</tr>
<tr>
<td>Total Raw Flash Storage Capacity</td>
<td>38.4 TB</td>
</tr>
<tr>
<td>Total Usable Storage Capacity</td>
<td>74 TB</td>
</tr>
</tbody>
</table>

**Exadata X8 Shapes**

<table>
<thead>
<tr>
<th>Property</th>
<th>Quarter Rack</th>
<th>Half Rack</th>
<th>Full Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shape Name</td>
<td>Exadata.Quarter3.100</td>
<td>Exadata.Half3.200</td>
<td>Exadata.Full3.400</td>
</tr>
<tr>
<td>Number of Compute Nodes</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Total Minimum Number of Enabled CPU Cores</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total Maximum Number of Enabled CPU Cores</td>
<td>100</td>
<td>200</td>
<td>400</td>
</tr>
<tr>
<td>Total RAM Capacity</td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
</tr>
<tr>
<td>Number of Exadata Storage Servers</td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>Total Raw Flash Storage Capacity</td>
<td>76.8 TB</td>
<td>179.2 TB</td>
<td>358.4 TB</td>
</tr>
<tr>
<td>Total Usable Storage Capacity</td>
<td>149 TB</td>
<td>299 TB</td>
<td>598 TB</td>
</tr>
</tbody>
</table>

Exadata X8 shapes provide 700 GB of user disk space for database homes.
### Exadata X7 Shapes

<table>
<thead>
<tr>
<th>Property</th>
<th>Quarter Rack</th>
<th>Half Rack</th>
<th>Full Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shape Name</strong></td>
<td>Exadata.Quarter2.92</td>
<td>Exadata.Half2.184</td>
<td>Exadata.Full2.368</td>
</tr>
<tr>
<td><strong>Number of Compute Nodes</strong></td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total Minimum Number of Enabled CPU Cores</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total Maximum Number of Enabled CPU Cores</strong></td>
<td>92</td>
<td>184</td>
<td>368</td>
</tr>
<tr>
<td><strong>Total RAM Capacity</strong></td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
</tr>
<tr>
<td><strong>Number of Exadata Storage Servers</strong></td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td><strong>Total Raw Flash Storage Capacity</strong></td>
<td>76.8 TB</td>
<td>153.6 TB</td>
<td>307.2 TB</td>
</tr>
<tr>
<td><strong>Total Usable Storage Capacity</strong></td>
<td>106 TB</td>
<td>212 TB</td>
<td>424 TB</td>
</tr>
</tbody>
</table>

Exadata X7 shapes provide 1 TB of user disk space for database homes.

### Exadata X6 Shapes

<table>
<thead>
<tr>
<th>Property</th>
<th>Quarter Rack</th>
<th>Half Rack</th>
<th>Full Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shape Name</strong></td>
<td>Exadata.Quarter1.84</td>
<td>Exadata.Half1.168</td>
<td>Exadata.Full1.336</td>
</tr>
<tr>
<td><strong>Number of Compute Nodes</strong></td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td><strong>Total Minimum (Default) Number of Enabled CPU Cores</strong></td>
<td>22</td>
<td>44</td>
<td>88</td>
</tr>
<tr>
<td><strong>Total Maximum Number of Enabled CPU Cores</strong></td>
<td>84</td>
<td>168</td>
<td>336</td>
</tr>
<tr>
<td><strong>Total RAM Capacity</strong></td>
<td>1440 GB</td>
<td>2880 GB</td>
<td>5760 GB</td>
</tr>
<tr>
<td><strong>Number of Exadata Storage Servers</strong></td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td><strong>Total Raw Flash Storage Capacity</strong></td>
<td>38.4 TB</td>
<td>76.8 TB</td>
<td>153.6 TB</td>
</tr>
<tr>
<td><strong>Total Usable Storage Capacity</strong></td>
<td>84 TB</td>
<td>168 TB</td>
<td>336 TB</td>
</tr>
</tbody>
</table>

Exadata X6 shapes provide 200 GB of user disk space for database homes.

**Overview of X8M Scalable Exadata Infrastructure**

Oracle Cloud Infrastructure scalable Exadata X8M system model allows you to add additional database and storage servers after provisioning and create a system that matches your capacity needs.
**The New Exadata Cloud Service Resource Model**

Exadata Cloud Service instances can now be provisioned with a new infrastructure resource model that replaces the *DB system* resource. In the new model, the DB system is split into two resources, the *cloud Exadata infrastructure* resource, and the *cloud VM cluster* resource.

The X8M system model is only compatible with the new resource model. For provisioning new X7 and X8 systems, Oracle recommends using the new resource model so that your instance will not have to be switched to the new resource model later.

Oracle will continue to support the Exadata DB system resource for an interim period (for both Exadata instance creation and management) before the DB system resource is deprecated in the Exadata Cloud Service. Existing Exadata DB systems can be easily switched to the new resource model with no downtime. For instructions on switching, see *To switch an Exadata DB system to the new Exadata resource model* on page 1229.

**The Cloud Exadata Infrastructure Resource**

The infrastructure resource is the top-level (parent) resource. At the infrastructure level, you control the number of database and storage servers. You also control Exadata system maintenance scheduling at the Exadata infrastructure level. This resource is created using the *CreateCloudExadataInfrastructure* API.

See *To add compute and storage resources to a flexible cloud Exadata infrastructure resource* on page 1230 for information on scaling the X8M cloud Exadata infrastructure resource. Note that after adding storage or database servers to the infrastructure resource, you must then add them to the system's VM cluster to utilize the new capacity.

**The Cloud VM Cluster Resource**

The VM cluster is a child resource of the infrastructure resource, providing a link between your Exadata cloud infrastructure resource and Oracle Database. Networking, OCPU count, IORM, and Oracle Grid Infrastructure are configured and managed at the VM cluster level. This resource is created using the *CreateCloudVmCluster* API.

See *To add database server or storage server capacity to a cloud VM cluster* on page 1230 for information on adding available storage or database servers to the VM cluster. Note that you must add servers to the infrastructure resource before you can add capacity to the VM cluster.

Exadata Cloud Service instances currently support creating a single cloud VM cluster.

**Additional Exadata Cloud Service Instance Resources**

The new Exadata resource model retains the rest of the resource types found in DB systems: Oracle Databases, database backups, Data Guard Associations, Work Requests, Oracle Database Homes, and database server nodes (also called "virtual machines").

**Note:**

The database server file system for database server nodes (also known as "virtual machines") has changed with the X8M generation of hardware. See *The X8M Virtual Machine File System Structure* on page 1352 for details on the X8M database server node file system.

**Switching an Exadata DB System to the New Resource Model and APIs**

If you have existing Exadata DB systems in Oracle Cloud Infrastructure, you can switch them to the new resource model and APIs. This does not change to the underlying hardware or shape family of your Exadata Cloud Service instance. The existing DB system APIs will be deprecated for Exadata by Oracle Cloud Infrastructure for all users following written notification and a transition period allowing you to switch to the new API and Console interfaces. Note that this change will not affect bare metal and virtual machine DB systems.

Switching to the new resource model does not impact the DB system's existing Exadata databases or client connections. If you have created automation that uses the existing DB system API, your applications may need to be updated to use the new API.
Important! Support for the Exadata DB system APIs will end on May 15, 2021. Oracle recommends that you migrate your Exadata Cloud Service instances to the new resource model APIs as soon as possible. Converting to the new resource model does not involve any system downtime.

After converting your DB system, you will have two new resources in place of the DB system resource: a cloud Exadata infrastructure resource, and a cloud VM cluster resource.

What to Expect After Switching

- Your new cloud Exadata infrastructure resource and cloud VM cluster are created in the same compartment as the DB system they replace
- Your new cloud Exadata infrastructure resource and cloud VM cluster use the same networking configuration as the DB system they replace
- After the switch, you cannot perform operations on the old Exadata DB system resource
- Switching is permanent, and the change cannot be undone
- X6, X7, X8 and Exadata base systems retain their fixed shapes after the switch, and cannot be expanded

To switch an Exadata DB system to the new Exadata resource model

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. In the list of DB systems, find the Exadata DB system you want to switch to the new resource model, and click its highlighted name to view the system details.
4. Click More Actions, then Switch to New API.
5. In the displayed confirmation page, read the What to expect after switching section. When you are ready to switch to the new resource model and APIs, click Start.

Caution:

Switching an Exadata DB system to the new resource model and APIs cannot be reversed. If you have automation for your system that utilizes the DB system APIs, you may need to update your applications prior to switching.

Scaling an Exadata Cloud Service Instance

This topic describes the scaling options available for Exadata Cloud Service instances.

Scaling CPU Cores Within an Exadata Cloud Service Instance

If an Exadata Cloud Service instance requires more compute node processing power, you can scale up the number of enabled CPU cores symmetrically across all the nodes in the system as follows:

X8M flexible infrastructure systems: You can scale CPU cores in multiples of the number of database servers currently provisioned for the cloud VM cluster. For example, if you have 6 database servers provisioned, you can add CPU cores in multiples of 6. At the time of provisioning, X8M systems have 2 database servers. For more information on adding compute and storage resources to an X8M system, see Scaling Exadata X8M Compute and Storage on page 1230.

Non-X8M fixed-shape systems: For a base system or an X7 or X8 quarter rack, you can scale in multiples of 2 across the 2 database compute nodes. For an X7 or X8 half rack, you can scale in multiples of 4 across the 4 database compute nodes. For an X7 or X8 full rack, you can scale in multiples of 8 across the 8 database compute nodes.

For a non-metered service instances, you can temporarily modify the compute node processing power (bursting) or add compute node processing power on a more permanent basis. For a metered service instance, you can simply modify the number of enabled CPU cores.

You can provision an Exadata Cloud Service instance with zero CPU cores, or scale the service instance down to zero cores after you provision it. With zero cores, you are billed only for the infrastructure until you scale up the system. For detailed information about pricing, see Exadata Cloud Service Pricing.
Tip:
OCPUs scaling activities are done online with no downtime.

For information on CPU cores per configuration, see Exadata Shape Configurations on page 1223. To learn how to scale a system, see To scale CPU cores in an Exadata Cloud Service cloud VM cluster or DB system on page 1258.

Scaling Exadata X8M Compute and Storage

The flexible X8M system model is designed to be easily scaled in place, with no need to migrate the database using a backup or Data Guard. You can scale an X8M service instance in the Console on the cloud Exadata infrastructure details page. After adding additional database or storage servers to your cloud Exadata infrastructure resource, you must add the increased capacity to the associated cloud VM cluster to utilize the newly-provisioned CPU or storage resources. After adding additional database servers to a VM cluster, you can then allocate the new CPU cores as described in To scale CPU cores in an Exadata Cloud Service cloud VM cluster or DB system on page 1258. After adding additional storage servers to your VM cluster, you do not need to take any further action to utilize the new storage.

Note:
- The Exadata X8M shape does not support removing storage or database servers from an existing X8M instance.
- For OCI Exadata Cloud Service databases configured with either Oracle Data Guard or customer-managed keys (encryption keys stored and managed using the OCI, Vault service), the database cannot currently utilize additional compute nodes added to the Exadata infrastructure.
- For OCI Exadata Cloud Service VM clusters that use node subsetting (meaning the clusters are configured to use only a subset of all nodes available in the dedicated Exadata infrastructure instance), you cannot currently add additional compute nodes to the VM cluster.

See Overview of X8M Scalable Exadata Infrastructure on page 1227 for more information on X8M systems.

To add compute and storage resources to a flexible cloud Exadata infrastructure resource

This task describes how to use the Oracle Cloud Infrastructure Console to scale a flexible cloud Exadata infrastructure resource. Currently, only Exadata X8M systems in Oracle Cloud Infrastructure have the ability to add database (compute) and storage servers to an existing service instance.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Under Exadata at Oracle Cloud, click Exadata Infrastructure.
3. In the list of cloud Exadata infrastructure resources, click the name of the resource you want to scale.
4. Click Scale Infrastructure.
5. Adding database servers: To add compute servers to the infrastructure resource, select the Database Servers radio button, then enter the number of servers you want to add in the Database servers field.

Adding storage servers: To add storage servers to the infrastructure resource, select the Storage Servers radio button, then enter the number of servers you want to add in the Storage servers field.
6. Click Scale.

Tip:
After scaling your infrastructure, you must add the new capacity to the cloud VM cluster before you can use the additional CPU and storage resources in the Exadata Cloud Service instance.

To add database server or storage server capacity to a cloud VM cluster

If you have scaled a flexible cloud Exadata infrastructure resource by adding additional database (compute) or storage servers to the service instance, you must add the additional capacity to the cloud VM cluster to utilize the additional resources. This topic describes how to use the Oracle Cloud Infrastructure (OCI) Console to add the new capacity to your cloud VM cluster.
Database

Note:

• For OCI Exadata Cloud Service databases configured with either Oracle Data Guard or customer-managed keys (encryption keys stored and managed using the OCI, Vault service), the database cannot currently utilize additional compute nodes added to the Exadata infrastructure.
• For OCI Exadata Cloud Service VM clusters that use node subsetting (meaning the clusters are configured to use only a subset of all nodes available in the dedicated Exadata infrastructure instance), you cannot currently add additional compute nodes to the VM cluster.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Under Exadata at Oracle Cloud, click Exadata VM Clusters.
3. In the list of cloud VM clusters, click the name of the cluster to which you want to add capacity.
4. On the VM Cluster Details page, click Scale VM Cluster.
5. If you have additional capacity available as a result of scaling the cloud Exadata infrastructure resource, a banner at the top of the Scale VM Cluster panel provides a message telling you the type and amount of additional capacity available to the VM cluster. Check the Add Capacity box.
6. Select either the Add Database Server or the Add Storage radio button, depending on which type of capacity you want to add to the cloud VM cluster.
7. Click Update. The cloud VM cluster goes into the Updating state. When the capacity has been successfully added, the cluster returns to the Available state.

Tip:

If you have added additional database servers to the cluster, you can allocate the new CPU cores once the cluster is in the Available state by clicking the Scale VM Cluster button again. See To scale CPU cores in an Exadata Cloud Service cloud VM cluster or DB system on page 1258 for more information on adding CPU cores to your cloud VM cluster.

Scaling X6, X7 and X8 Exadata DB System Configurations

Scaling an Exadata X6, X7, or X8 Exadata Cloud Service instance by moving to a shape with more capacity enables you meet the needs of your growing workload. This is useful when a database deployment requires:

• Processing power that is beyond the capacity of the current system configuration.
• Storage capacity that is beyond the capacity of the current system configuration.
• A performance boost that can be delivered by increasing the number of available compute nodes.
• A performance boost that can be delivered by increasing the number of available Exadata Storage Servers.

You can move you workloads to a larger fixed shape (X7 and X8 hardware shapes), or move to the flexible X8M shape that allows for easy expansion of compute and storage resources as your workloads grow.

To assist with moving your database deployments between Exadata Cloud Service instances, you can restore a backup to a different service instance that has more capacity, or create a Data Guard association for your database in a service instance with more capacity, and then perform a switchover so that your new standby database assumes the primary role. To start the process, contact Oracle and request a service limit increase so that you can provision the larger service instance needed by your database.

Best Practices for Exadata Cloud Service Instances

Oracle recommends that you follow these best practice guidelines to ensure the manageability of your Exadata Cloud Service instance:

• Wherever possible, use the Oracle-supplied cloud interfaces such as the Oracle Cloud Infrastructure Console, API, or CLI, or cloud-specific tools such as dbaascli and dbaasapi to perform lifecycle management and administrative operations on your Exadata Cloud Service instance. For example, use the exadbcpatchmulti command to apply Oracle Database patches instead of manually running opatch. In addition, if an operation
can be performed by using the Console as well as a command line utility, Oracle recommends that you use the Console. For example, use the Console instead of using `dbaasapi` to create databases.

- Do not change the compute node OS users or manually manipulate SSH key settings associated with your Exadata DB system.
- Apply only patches that are available through the Database service. Do not apply patches from any other source unless you are directed to do so by Oracle Support.
- Apply the quarterly patches regularly, every quarter if possible.
- Do not change the ports for Oracle Net Listener.

**Network Setup for Exadata Cloud Service Instances**

Before you set up an Exadata Cloud Service instance, you must set up a virtual cloud network (VCN) and other networking service components. This topic describes the recommended configuration for the VCN and several related requirements for the Exadata Cloud Service instance.

**VCN and Subnets**

To launch an Exadata Cloud Service instance, you must have:

- A VCN in the region where you want the Exadata Cloud Service instance
- At least two subnets in the VCN. The two subnets are:
  - Client subnet
  - Backup subnet

**Note:**

For Exadata Cloud Service instances using the new Exadata resource model, networking is configured on the cloud VM cluster resource. For instances using DB system resource model, networking is configured on the DB system resource.

In general, Oracle recommends using regional subnets, which span all availability domains in the region. If you instead use AD-specific subnets, both the client and backup subnets must be in the same availability domain. The important thing to know for your Exadata Cloud Service instance is that the resources you create in the two subnets must be in the same availability domain. For more information, see Overview of VCNs and Subnets on page 2822.

You will create custom route tables for each subnet. You will also create security rules to control traffic to and from the client network and backup network of the Exadata compute notes (for cloud VM clusters, nodes are called virtual machines). More information follows about those items.

**Option 1: Public Client Subnet with Internet Gateway**

This option can be useful when doing a proof-of-concept or development work. You can use this setup in production if you want to use an internet gateway with the VCN, or if you have services that run only on a public network and need access to the database. See the following diagram and description.
You set up:

- **Subnets**:
  - *Public* client subnet (*public* means that the resources in the subnet can have public IP addresses at your discretion).
  - *Private* backup subnet (*private* means that the resources in the subnet cannot have public IP addresses and therefore cannot receive incoming connections from the internet).

- **Gateways for the VCN**:
  - Internet gateway (for use by the client subnet).
  - Service gateway (for use by the backup subnet). Also see Option 1: Service Gateway Access Only to Object Storage on page 1237.

- **Route tables**:
  - Custom route table for the public client subnet, with a route for 0.0.0.0/0, and target = the internet gateway.
  - Separate custom route table for the private backup subnet, with a route rule for the service CIDR label called *OCI <region> Object Storage*, and target = the service gateway. Also see Option 1: Service Gateway Access Only to Object Storage on page 1237.
  - Security rules to enable the desired traffic to and from the Exadata virtual machines compute nodes. See Security Rules for the Exadata Cloud Service instance on page 1239.
  - Static route on the Exadata Cloud Service instance's compute nodes (to enable access to Object Storage by way of the backup subnet).

**Important:**

See this known issue for information about configuring route rules with *service gateway* as the target on route tables associated with public subnets.
Option 2: Private Subnets

Oracle recommends this option for a production system. Both subnets are private and cannot be reached from the internet. See the following diagram and description.

You set up:

- **Subnets:**
  - *Private* client subnet.
  - *Private* backup subnet.

- **Gateways for the VCN:**
  - Dynamic routing gateway (DRG), with a FastConnect or IPSec VPN to your on-premises network (for use by the client subnet).
  - Service gateway (for use by the backup subnet to reach Object Storage, and for use by the client subnet to reach the Oracle YUM repository for OS updates). Also see Option 2: Service Gateway Access to Both Object Storage and YUM Repos on page 1238.
  - NAT gateway (for use by the client subnet to reach public endpoints not supported by the service gateway).

- **Route tables:**
  - Custom route table for the private client subnet, with two rules:
    - A rule for the on-premises network's CIDR, and target = DRG.
    - A rule for the service CIDR label called *All <region> Services in Oracle Services Network*, and target = the service gateway. The *Oracle Services Network* is a conceptual network in Oracle Cloud Infrastructure that is reserved for Oracle services. The rule enables the client subnet to reach the regional Oracle YUM repository for OS updates. Also see Option 2: Service Gateway Access to Both Object Storage and YUM Repos on page 1238.
    - A rule for 0.0.0.0/0, and target = NAT gateway.
  - Separate custom route table for the private backup subnet, with one rule:
    - The same rule as for the client subnet: for the service CIDR label called *All <region> Services in Oracle Services Network*, and target = the service gateway. This rule enables the backup subnet to reach the regional Object Storage for backups.
  - Security rules to enable the desired traffic to and from the Exadata nodes. See Security Rules for the Exadata Cloud Service instance on page 1239.
• **Static route** on the compute nodes (for VM clusters, the virtual machines) to enable access to Object Storage by way of the backup subnet.

**Requirements for IP Address Space**

If you're setting up Exadata Cloud Service instances (and thus VCNs) in more than one region, make sure the IP address space of the VCNs does not overlap. This is important if you want to set up disaster recovery with Oracle Data Guard.

The two subnets you create for the Exadata Cloud Service instance must not overlap with 192.168.128.0/20.

The following table lists the minimum required subnet sizes, depending on the Exadata rack size. For the client subnet, each node requires two IP addresses, and in addition, three addresses are reserved for Single Client Access Names (SCANs). For the backup subnet, each node requires one address.

<table>
<thead>
<tr>
<th>Rack Size</th>
<th>Client Subnet: # Required IP Addresses</th>
<th>Client Subnet: Minimum Size</th>
<th>Backup Subnet: # Required IP Addresses</th>
<th>Backup Subnet: Minimum Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base System or Quarter Rack</td>
<td>(2 addresses * 2 nodes) + 3 for SCANs + 3 reserved in subnet = 10</td>
<td>/28 (16 IP addresses)</td>
<td>(1 address * 2 nodes) + 3 reserved in subnet = 5</td>
<td>/29 (8 IP addresses)</td>
</tr>
<tr>
<td>Half Rack</td>
<td>(2 * 4 nodes) + 3 + 3 = 14</td>
<td>/28 (16 IP addresses)</td>
<td>(1 * 4 nodes) + 3 = 7</td>
<td>/29 (8 IP addresses)</td>
</tr>
<tr>
<td>Full Rack</td>
<td>(2* 8 nodes) + 3 + 3 = 22</td>
<td>/27 (32 IP addresses)</td>
<td>(1 * 8 nodes) + 3 = 11</td>
<td>/28 (16 IP addresses)</td>
</tr>
</tbody>
</table>

**Tip:**

The Networking service reserves three IP addresses in each subnet.

Allocating a larger space for the subnet than the minimum required (for example, at least /25 instead of /28) can reduce the relative impact of those reserved addresses on the subnet's available space.

**VCN Creation Wizard: Not for Production**

The Networking section of the Console includes a handy wizard that creates a VCN along with related resources. It can be useful if you just want to try launching an instance. However, the wizard automatically creates a public subnet and an internet gateway. You may not want this for your production network, so Oracle recommends you create the VCN and other resources individually yourself instead of using the wizard.

**DNS: Short Names for the VCN, Subnets, and Exadata Cloud Service instance**

For the nodes to communicate, the VCN must use the Internet and VCN Resolver. It enables hostname assignment to the nodes, and DNS resolution of those hostnames by resources in the VCN. It enables round robin resolution of the database's SCANs. It also enables resolution of important service endpoints required for backing up databases, patching, and updating the cloud tooling on an Exadata Cloud Service instance. The Internet and VCN Resolver is the VCN's default choice for DNS in the VCN. For more information, see DNS in Your Virtual Cloud Network on page 2910 and also DHCP Options on page 2917.

When you create the VCN, subnets, and Exadata, you must carefully set the following identifiers, which are related to DNS in the VCN:

- VCN domain label
- Subnet domain label
- Hostname prefix for the Exadata Cloud Service instance's cloud VM cluster or DB system resource

These values make up the node's fully qualified domain name (FQDN):
<hostname_prefix>-<subnet_domain_label>.<vcn_domain_label>.oraclevcn.com

For example:

exacs-abcdel.clientpvtad1.acmevcniad.oraclevcn.com

In this example, you assign exacs as the hostname prefix when you create the cloud VM cluster or DB system. The Database service automatically appends a hyphen and a five-letter string with the node number at the end. For example:

- Node 1: exacs-abcdel.clientpvtad1.acmevcniad.oraclevcn.com
- Node 2: exacs-abcdel2.clientpvtad1.acmevcniad.oraclevcn.com
- Node 3: exacs-abcdel3.clientpvtad1.acmevcniad.oraclevcn.com
- And so on

Requirements for the hostname prefix:

- Recommended maximum: 12 characters. For more information, see the example under the following section, "Requirements for the VCN and subnet domain labels".
- Cannot be the string localhost

Requirements for the VCN and subnet domain labels:

- Recommended maximum: 14 characters each. The actual underlying requirement is a total of 28 characters across both domain labels (excluding the period between the labels). For example, both of these are acceptable: subnetad1.verylongvcnphx or verylongsubnetad1.vcnphx. For simplicity, the recommendation is 14 characters each.
- No hyphens or underscores.
- Recommended: include the region name in the VCN's domain label, and include the availability domain name in the subnet's domain label.
- In general, the FQDN has a maximum total limit of 63 characters. Here is a safe general rule:

```
<12_chars_max>-<subnet_domain_label>.<vcn_domain_label>.oraclevcn.com
```

The preceding maximums are not enforced when you create the VCN and subnets. However, if the labels exceed the maximum, the Exadata deployment fails.

**DNS: Between On-Premises Network and VCN**

To enable the use of hostnames when on-premises hosts and VCN resources communicate with each other, you have two options:

- Set up an instance in the VCN to be a custom DNS server. For an example of an implementation of this scenario with the Oracle Terraform provider, see Hybrid DNS Configuration.
- Manage hostname resolution yourself manually.

**Node Access to Object Storage: Static Route**

To be able to back up databases, and patch and update cloud tools on an Exadata Cloud Service instance, you must configure access to Oracle Cloud Infrastructure Object Storage. Regardless of how you configure the VCN with that access (for example, with a service gateway), you may also need to configure a static route to Object Storage on each of the compute nodes in the cluster. This is only required if you are not using automatic backups. If you are using customized backups using the backup APIs, then you must route traffic destined for Object Storage through the backup interface (BONDETH1). This is not necessary if you are using the automatic backups created with the Console, APIs, or CLIs.

**Important:**

You must configure a static route for Object Storage access on each compute node in an Exadata Cloud Service instance if you are not creating automatic backups with the Console, APIs, or CLIs. Otherwise, attempts to back up databases, and patch or update tools on the system, can fail.
Object Storage IP allocations

Oracle Cloud Infrastructure Object Storage uses the CIDR block IP range 134.70.0.0/17 for all regions. This range was introduced in April and May of 2018.

As of June 1, 2018, Object Storage no longer supports the following discontinued IP ranges. Oracle recommends that you remove these older IP addresses from your access-control lists, firewall rules, and other rules after you have adopted the new IP ranges.

The discontinued IP ranges are:

- Germany Central (Frankfurt): 130.61.0.0/16
- UK South (London): 132.145.0.0/16
- US East (Ashburn): 129.213.0.0/16
- US West (Phoenix): 129.146.0.0/16

To configure a static route for Object Storage access

1. SSH to a compute node in the Exadata Cloud Service instance.

   ```
   ssh -i <private_key_path> opc@<node_ip_address>
   ```

2. Log in as opc and then sudo to the root user. Use `sudo su -` with a hyphen to invoke the root user's profile.

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. Identify the gateway configured for the BONDETH1 interface.

   ```
   [root@dbsys ~]# grep GATEWAY /etc/sysconfig/network-scripts/ifcfg-bondeth1 | awk -F=" " '{print $2}'
   ```

   ```
   10.0.4.1
   ```

4. Add the following static rule for BONDETH1 to the /etc/sysconfig/network-scripts/route-bondeth1 file:

   ```
   10.0.X.0/XX dev bondeth1 table 211
   default via <gateway> dev bondeth1 table 211
   134.70.0.0/17 via <gateway_from_previous_step> dev bondeth1
   ```

5. Restart the interface.

   ```
   [root@dbsys ~]# ifdown bondeth1; ifup bondeth1;
   ```

   The file changes from the previous step take effect immediately after the ifdown and ifup commands run.

6. Repeat the preceding steps on each compute node in the Exadata Cloud Service instance.

Service Gateway for the VCN

Your VCN needs access to both Object Storage for backups and Oracle YUM repos for OS updates.

Depending on whether you use option 1 or option 2 described previously, you use the service gateway in different ways. See the next two sections.

Option 1: Service Gateway Access Only to Object Storage

You configure the backup subnet to use the service gateway for access only to Object Storage. As a reminder, here's the diagram for option 1:
In general, you must:

- Perform the tasks for setting up a service gateway on a VCN, and specifically enable the service CIDR label called `OCI <region> Object Storage`.
- In the task for updating routing, add a route rule to the `backup` subnet's custom route table. For the destination service, use `OCI <region> Object Storage` and target = the service gateway.
- In the task for updating security rules in the subnet, perform the task on the `backup` network's network security group (NSG) or custom security list. Set up a security rule with the destination service set to `OCI <region> Object Storage`. See Rule Required Specifically for the Backup Network on page 1242.

**Option 2: Service Gateway Access to Both Object Storage and YUM Repos**

You configure both the `client subnet` and `backup subnet` to use the `service gateway` for access to the Oracle Services Network, which includes both Object Storage and the Oracle YUM repos.

**Important:**

See this known issue for information about accessing Oracle YUM services through the service gateway.

As a reminder, here's the diagram for option 2:
In general, you must:

- Perform the tasks for setting up a service gateway on a VCN, and specifically enable the service CIDR label called **All <region> Services in Oracle Services Network**.
- In the task for updating routing in each subnet, add a rule to each subnet's custom route table. For the destination service, use **All <region> Services in Oracle Services Network** and target = the service gateway.
- In the task for updating security rules for the subnet, perform the task on the backup network's network security group (NSG) or custom security list. Set up a security rule with the destination service set to **OCI <region> Object Storage**. See Rule Required Specifically for the Backup Network on page 1242. Note that the client subnet already has a broad egress rule that covers access to the YUM repos.

Here are a few additional details about using the service gateway for option 2:

- Both the client subnet and backup subnet use the service gateway, but to access different services. You cannot enable both the **OCI <region> Object Storage** service CIDR label and the **All <region> Services in Oracle Services Network** for the service gateway. To cover the needs of both subnets, you must enable **All <region> Services in Oracle Services Network** for the service gateway. The VCN can have only a single service gateway.
- Any route rule that targets a given service gateway must use an enabled service CIDR label and not a CIDR block as the destination for the rule. That means for option 2, the route tables for both subnets must use **All <region> Services in Oracle Services Network** for their service gateway rules.
- Unlike route rules, security rules can use either any service CIDR label (whether the VCN has a service gateway or not) or a CIDR block as the source or destination CIDR for the rule. Therefore, although the backup subnet has a route rule that uses **All <region> Services in Oracle Services Network**, the subnet can have a security rule that uses **OCI <region> Object Storage**. See Rule Required Specifically for the Backup Network on page 1242.

**Security Rules for the Exadata Cloud Service instance**

This section lists the security rules to use with your Exadata Cloud Service instance. Security rules control the types of traffic allowed for the client network and backup network of the Exadata's compute nodes. The rules are divided into three sections.

There are different ways to implement these rules. For more information, see Ways to Implement the Security Rules on page 1242.

**Rules Required for Both the Client Network and Backup Network**

This section has several general rules that enable essential connectivity for hosts in the VCN.
If you use security lists to implement your security rules, be aware that the rules that follow are included by default in the default security list. Update or replace the list to meet your particular security needs. The two ICMP rules (general ingress rules 2 and 3) are required for proper functioning of network traffic within the Oracle Cloud Infrastructure environment. Adjust the general ingress rule 1 (the SSH rule) and the general egress rule 1 to allow traffic only to and from hosts that require communication with resources in your VCN.

**General ingress rule 1: Allows SSH traffic from anywhere**

- **Stateless**: No (all rules must be stateful)
- **Source Type**: CIDR
- **Source CIDR**: 0.0.0.0/0
- **IP Protocol**: SSH
- **Source Port Range**: All
- **Destination Port Range**: 22

**General ingress rule 2: Allows Path MTU Discovery fragmentation messages**

This rule enables hosts in the VCN to receive Path MTU Discovery fragmentation messages. Without access to these messages, hosts in the VCN can have problems communicating with hosts outside the VCN.

- **Stateless**: No (all rules must be stateful)
- **Source Type**: CIDR
- **Source CIDR**: 0.0.0.0/0
- **IP Protocol**: ICMP
- **Type**: 3
- **Code**: 4

**General ingress rule 3: Allows connectivity error messages within the VCN**

This rule enables the hosts in the VCN to receive connectivity error messages from each other.

- **Stateless**: No (all rules must be stateful)
- **Source Type**: CIDR
- **Source CIDR**: Your VCN's CIDR
- **IP Protocol**: ICMP
- **Type**: 3
- **Code**: All

**General egress rule 1: Allows all egress traffic**

- **Stateless**: No (all rules must be stateful)
- **Destination Type**: CIDR
- **Destination CIDR**: 0.0.0.0/0
- **IP Protocol**: All

**Rules Required Specifically for the Client Network**

The following security rules are important for the client network.

**Important:**

- Client ingress rules 1 and 2 only cover connections initiated from within the client subnet. If you have a client that resides outside the VCN, Oracle recommends setting up two additional similar rules that instead have the **Source CIDR** set to the public IP address of the client.
- Client ingress rules 3 and 4 and client egress rules 1 and 2 allow TCP and ICMP traffic inside the client network and enable the nodes to...
communicate with each other. If TCP connectivity fails across the nodes,
the Exadata cloud VM cluster or DB system resource fails to provision.

Client ingress rule 1: Allows ONS and FAN traffic from within the client subnet

The first rule is recommended and enables the Oracle Notification Services (ONS) to communicate about Fast Application Notification (FAN) events.

- **Stateless:** No (all rules must be stateful)
- **Source Type:** CIDR
- **Source CIDR:** Client subnet's CIDR
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 6200
- **Description:** An optional description of the rule.

Client ingress rule 2: Allows SQL*NET traffic from within the client subnet

This rule is for SQL*NET traffic and is required in these cases:

- If you need to enable client connections to the database
- If you plan to use Oracle Data Guard

- **Stateless:** No (all rules must be stateful)
- **Source Type:** CIDR
- **Source CIDR:** Client subnet's CIDR
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 1521
- **Description:** An optional description of the rule.

Client egress rule 1: Allows all TCP traffic inside the client subnet

- **Stateless:** No (all rules must be stateful)
- **Destination Type:** CIDR
- **Destination CIDR:** 0.0.0.0/0
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 22
- **Description:** An optional description of the rule.

Client egress rule 2: Allows all egress traffic (allows connections to the Oracle YUM repos)

Client egress rule 3 is important because it allows connections to the Oracle YUM repos. It is redundant with the general egress rule in Security Rules for the Exadata Cloud Service instance on page 1239 (and in the default security list). It is optional but recommended in case the general egress rule (or default security list) is inadvertently changed.

- **Stateless:** No (all rules must be stateful)
- **Destination Type:** CIDR
- **Destination CIDR:** 0.0.0.0/0
- **IP Protocol:** All
- **Description:** An optional description of the rule.
Database

Rule Required Specifically for the Backup Network

The following security rule is important for the backup network because it enables the DB system to communicate with Object Storage through the service gateway (and optionally with the Oracle YUM repos if the client network doesn't have access to them). It is redundant with the general egress rule in Security Rules for the Exadata Cloud Service instance on page 1239 (and in the default security list). It is optional but recommended in case the general egress rule (or default security list) is inadvertently changed.

Backup egress rule: Allows access to Object Storage

- **Stateless**: No (all rules must be stateful)
- **Destination Type**: Service
- **Destination Service**:
  - The service CIDR label called OCI `<region>` Object Storage
  - If the client network does not have access to the Oracle YUM repos, use the service CIDR label called All `<region>` Services in Oracle Services Network
- **IP Protocol**: TCP
- **Source Port Range**: All
- **Destination Port Range**: 443 (HTTPS)
- **Description**: An optional description of the rule.

Ways to Implement the Security Rules

The Networking service offers two ways to implement security rules within your VCN:

- **Network security groups**
- **Security lists**

For a comparison of the two methods, see Comparison of Security Lists and Network Security Groups on page 2833.

*If you use network security groups*

If you choose to use network security groups (NSGs), here is the recommended process:

1. Create an NSG for the client network. Add the following security rules to that NSG:
   - The rules listed in Rules Required for Both the Client Network and Backup Network on page 1239
   - The rules listed in Rules Required Specifically for the Client Network
2. Create a separate NSG for the backup network. Add the following security rules to that NSG:
   - The rules listed in Rules Required for Both the Client Network and Backup Network on page 1239
   - The rules listed in Rule Required Specifically for the Backup Network on page 1242
3. When the database administrator creates the Exadata Cloud Service instance, they must choose several networking components (for example, which VCN and subnets to use):
   - When they choose the client subnet, they can also choose which NSG or NSGs to use. Make sure they choose the client network's NSG.
   - When they choose the backup subnet, they can also choose which NSG or NSGs to use. Make sure they choose the backup network's NSG.

You could instead create a separate NSG for the general rules. Then when the database administrator chooses which NSGs to use for the client network, make sure they choose both the general NSG and the client network NSG. Similarly for the backup network, they choose both the general NSG and the backup network NSG.

*If you use security lists*

If you choose to use security lists, here is the recommended process:
1. Configure the client subnet to use the required security rules:
   a. Create a custom security list for the client subnet and add the rules listed in Rules Required Specifically for the Client Network on page 1240.
   b. Associate the following two security lists with the client subnet:
      • VCN's default security list with all its default rules. This automatically comes with the VCN. By default it contains the rules in Rules Required for Both the Client Network and Backup Network on page 1239.
      • The new custom security list you created for the client subnet.
2. Configure the backup subnet to use the required security rules:
   a. Create a custom security list for the backup subnet and add the rules listed in Rule Required Specifically for the Backup Network on page 1242.
   b. Associate the following two security lists with the backup subnet:
      • VCN's default security list with all its default rules. This automatically comes with the VCN. By default it contains the rules in Rules Required for Both the Client Network and Backup Network on page 1239.
      • The new custom security list you created for the backup subnet.

Later when the database administrator creates the Exadata Cloud Service instance, they must choose several networking components. When they select the client subnet and backup subnet that you've already created and configured, the security rules are automatically enforced for the nodes created in those subnets.

Caution:
Do not remove the default egress rule from the default security list. If you do, make sure to instead include the following replacement egress rule in the client subnet's security list:
• Stateless: No (all rules must be stateful)
• Destination Type: CIDR
• Destination CIDR: 0.0.0.0/0
• IP Protocol: All

Creating an Exadata Cloud Service Instance

This topic explains how to create an Oracle Exadata Cloud Service instance. It also describes how to configure required access to the Oracle Cloud Infrastructure Object Storage service and set up DNS.

When you create an Exadata Cloud Service instance using the Console or the API, the system is provisioned to support Oracle databases. The service creates an initial database based on the options you provide and some default options described later in this topic.

Resources to Be Created

You will create different Exadata Cloud Service resources depending on which resource model you use to create your Exadata Cloud Service instance.

New Resource Model (Supported for All Exadata Shapes)

If you are using the new Exadata Cloud Service resource model, you will provision the following resources separately:

• Cloud Exadata infrastructure resource: The infrastructure resource is the top-level (parent) resource. At the infrastructure level, you control the number of database and storage servers. You also control Exadata system maintenance scheduling at the Exadata infrastructure level.
• Cloud VM cluster resource: The VM cluster is a child resource of the infrastructure resource, providing a link between your Exadata cloud infrastructure resource and Oracle Database. Networking, OCPU count, IORM, and Oracle Grid Infrastructure are configured and managed at the VM cluster level. To create a cloud VM cluster, you must have an existing cloud Exadata infrastructure resource to house the VM cluster.

Notes:
• Use the new resource model to provision both the flexible X8M shape and fixed-shape systems (X7/X7/Exadata Base System)
• Exadata Cloud Service instance currently support only one cloud VM cluster

| Tip: |
| Oracle recommends using the new resource model to provision Exadata Cloud Service instances, regardless of the hardware shape family you are choosing (X7, X8, or X8M). Doing so will allow you to use the new APIs for these resource types, and you will not have to convert your service instance resources (or any automation associated those resources) at a later time. |

Old Resource Model (X7, X8, and Exadata Base Shape Families Only)
You can use the older Exadata Cloud Service resource model if needed to provision X7 and X8 systems. The old resource model creates a single Exadata DB system resource. See To create an X7 or X8 Exadata DB system on page 1248 for more information.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

Prerequisites
• The public key, in OpenSSH format, from the key pair that you plan to use for connecting to the system via SSH. A sample public key, abbreviated for readability, is shown below.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAA....lo/gKMLVM2xzclxJr/Hc26biw3TXWGEakrK1OQ== rsa-key-20160304
```

For more information, see Managing Key Pairs on Linux Instances on page 693.
• A correctly configured virtual cloud network (VCN) to launch the system in. Its related networking resources (gateways, route tables, security lists, DNS, and so on) must also be configured as necessary for the system. For more information, see Network Setup for Exadata Cloud Service Instances on page 1232.

Default Options for the Initial Database
To simplify launching an Exadata Cloud Service instance in the Console and when using the API, the following default options are used for the initial database:

• Console Enabled: False
• Create Container Database: False for version 11.2.0.4 databases. Otherwise, true.
• Create Instance Only (for standby and migration): False
• Database Home ID: Creates a database home
• Database Language: AMERICAN
• Database Sizing Template: odb2
• Database Storage: Automatic Storage Management (ASM)
• Database Territory: AMERICA
• Database Unique Name: The user-specified database name and a system-generated suffix, for example, dbtst_phx1cs.
• PDB Admin Name: pdbuser (Not applicable for version 11.2.0.4 databases.)
Using the Console

To create a cloud Exadata infrastructure resource

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Under Exadata at Oracle Cloud, click Exadata Infrastructure.
3. Click Create Exadata Infrastructure.
5. Display name: Enter a display name for the Exadata infrastructure. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the cloud Exadata infrastructure resource. Avoid entering confidential information.
7. Select the Exadata system model: Select either a fixed-shape system (quarter, half, or full rack X7-2 or X8-2 shapes), or a scalable system (X8M-2).
   - X8M-2: If you select the flexible X8M-2 system model, your initial Exadata Cloud Service instance will have 2 database servers and 3 storage servers (the equivalents of an X8 quarter rack shape). After provisioning, you can scale the service instance as needed by adding additional storage servers, compute servers, or both.
   - X7 and X8: If you select an X7 or X8 system, you are given the choice of provisioning a quarter, half, or full rack. See Exadata Fixed Hardware Shapes: X6, X7, X8 and Exadata Base on page 1351 for hardware and capacity details.
   - Exadata Base: The Exadata base shape comes in a single configuration, and provides an economical alternative to provisioning a quarter rack system. See Exadata Fixed Hardware Shapes: X6, X7, X8 and Exadata Base on page 1351
8. Configure automatic maintenance: Click this button to specify a schedule for the quarterly automatic infrastructure maintenance. In the Automatic Infrastructure Maintenance Schedule dialog that opens, do the following:
   a. Click the Specify a schedule radio button to choose your preferred month, week, weekday, and start time for infrastructure maintenance.
   b. Under Maintenance months, specify at least one month for each quarter during which Exadata infrastructure maintenance will take place. You can select more than one month per quarter. If you specify a long lead time for advanced notification (for example, 4 weeks), then you may want to specify two or three months per quarter during which maintenance runs can occur. This will ensure that your maintenance updates are applied in a timely manner after accounting for your required lead time. Lead time is discussed in the following steps.
   c. Under Week of the month, specify which week of the month maintenance will take place. Weeks start on the 1st, 8th, 15th, and 22nd days of the month, and have a duration of seven days. Weeks start and end based on calendar dates, not days of the week. Maintenance cannot be scheduled for the fifth week of months that contain more than 28 days.
   d. Optional. Under Day of the week, specify the day of the week on which the maintenance will occur. If you do not specify a day of the week, then Oracle will run the maintenance update on a weekend day to minimize disruption.
   e. Optional. Under Start hour, specify the hour during which the maintenance run will begin. If you do not specify a start hour, then Oracle will choose the least disruptive time to run the maintenance update.
   f. Under Lead Time, specify the number of weeks ahead of the maintenance event you would like to receive a notification message. Your lead time ensures that a newly released maintenance update is scheduled to account for your required period of advanced notification.
   g. Click Update Maintenance Schedule.
9. Click Show Advanced Options to specify advanced options for the initial database.
   In the Tags tab, you can add tags to the database. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
10. Click Create Exadata Infrastructure. The cloud Exadata infrastructure appears in the Exadata Infrastructure list with a status of Provisioning. The infrastructure's icon changes from yellow to green (or red to indicate errors).

WHAT NEXT?
After the cloud Exadata infrastructure resource is successfully provisioned and in the Available status, you can create a cloud VM cluster on your infrastructure. You must provision both an infrastructure resource and a VM cluster before you can create your first database in the new Exadata Cloud Service instance.

To create a cloud VM cluster resource

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To create a cloud VM cluster in an Exadata Cloud Service instance, you must have first created a cloud Exadata infrastructure resource. Exadata Cloud Service instances currently support creating a single cloud VM cluster.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Under Exadata at Oracle Cloud, click Exadata VM Clusters.
3. Click Create Exadata VM Cluster.

   The Create Exadata VM Cluster page is displayed. Provide the required information to configure the VM cluster.

4. Compartment: Select a compartment for the VM cluster resource.
5. Display name: Enter a user-friendly display name for the VM cluster. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system. Avoid entering confidential information.
6. Select Exadata infrastructure: Select the infrastructure resource that will contain the VM cluster. Currently, cloud Exadata infrastructure resources support only one VM cluster, so you must choose an infrastructure resource that does not have an existing VM cluster. Click Change Compartment and pick a different compartment from the one you are working in to view infrastructure resources in other compartments.
7. Configure the VM cluster: Specify the number of OCPU cores you want to allocate to each of the VM cluster's virtual machine compute nodes. The read-only Requested OCPU count for the Exadata VM cluster field displays the total number of OCPU cores you are allocating.
8. Configure Exadata storage: Specify the following:
   - Allocate storage for Exadata sparse snapshots: Select this configuration option if you intend to use snapshot functionality within your VM cluster. If you select this option, the SPARSE disk group is created, which enables you to use VM cluster snapshot functionality for PDB sparse cloning. If you do not select this option, the SPARSE disk group is not created and snapshot functionality will not be available on any database deployments that are created in the environment.
   - Allocate storage for local backups: Select this option if you intend to perform database backups to the local Exadata storage within your Exadata Cloud Service instance. If you select this option, more space is allocated to the RECO disk group, which is used to store backups on Exadata storage. If you do not select this option, more space is allocated to the DATA disk group, which enables you to store more information in your databases.
9. Add SSH key: Add the public key portion of each key pair you want to use for SSH access to the DB system.
   - Upload SSH key files: Select this radio button to browse or drag and drop .pub files.
   - Paste SSH keys: Select this radio button to paste in individual public keys. To paste multiple keys, click + Another SSH Key, and supply a single key for each entry.
10. **Configure the network settings:** Specify the following:

- **Virtual cloud network:** The VCN in which you want to create the VM cluster. Click **Change Compartment** to select a VCN in a different compartment.

- **Client subnet:** The subnet to which the VM cluster should attach. Click **Change Compartment** to select a subnet in a different compartment.

  Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.

- **Backup subnet:** The subnet to use for the backup network, which is typically used to transport backup information to and from Oracle Cloud Infrastructure Object Storage, and for Data Guard replication. Click **Change Compartment** to select a subnet in a different compartment, if applicable.

  Do not use a subnet that overlaps with 192.168.128.0/20. This restriction applies to both the client subnet and backup subnet.

  If you plan to back up databases to Object Storage, see the network prerequisites in Managing Exadata Database Backups on page 1320.

- **Network Security Groups:** Optionally, you can specify one or more network security groups (NSGs) for both the client and backup networks. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress **security rules** to your Exadata Cloud Service VM cluster. A maximum of five NSGs can be specified. For more information, see Network Security Groups on page 2841 and Network Setup for Exadata Cloud Service Instances on page 1232.

  Note that if you choose a subnet with a security list, the security rules for the VM cluster will be a union of the rules in the security list and the NSGs.

  **To use network security groups:**

  - Check the **Use network security groups to control traffic** check box. This box appears under both the selector for the client subnet and the backup subnet. You can apply NSGs to either the client or the backup network, or to both networks. Note that you must have a virtual cloud network selected to be able to assign NSGs to a network.

  - Specify the NSG to use with the network. You might need to use more than one NSG. If you're not sure, contact your network administrator.

  - To use additional NSGs with the network, click **+ Another Network Security Group**.

- **Hostname prefix:** Your choice of host name for the Exadata DB system. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for an Exadata DB system is 12.

  **Important:**

  The host name must be unique within the subnet. If it is not unique, the VM cluster will fail to provision.

- **Host domain name:** The domain name for the VM cluster. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. Hyphens (-) are not permitted.

  If you plan to store database backups in Object Storage, Oracle recommends that you use a VCN Resolver for DNS name resolution for the client subnet because it automatically resolves the Swift endpoints used for backups.

- **Host and domain URL:** This read-only field combines the host and domain names to display the fully qualified domain name (FQDN) for the database. The maximum length is 64 characters.
11. **Choose a license type:** The type of license you want to use for the VM cluster. Your choice affects metering for billing.

   - **License Included** means the cost of the cloud service includes a license for the Database service.
   - **Bring Your Own License (BYOL)** means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premises licenses and cloud licenses.

12. **Click Show Advanced Options** to specify advanced options for the VM cluster:

   - **Time zone:** The default time zone for the DB system is UTC, but you can specify a different time zone. The time zone options are those supported in both the Java.util.TimeZone class and the Oracle Linux operating system. For more information, see [DB System Time Zone](#) on page 1575.

     **Tip:**
     
     If you want to set a time zone other than UTC or the browser-detected time zone, and if you do not see the time zone you want, try selecting the **Select another time zone** option, then selecting “Miscellaneous” in the **Region or country** list and searching the additional **Time zone** selections.

   - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

13. **Click Create Exadata VM Cluster.**

**WHAT NEXT?**

After your VM cluster is successfully created and in the Available state, you can view the VM Cluster Details page by clicking the name of the VM cluster in the list of clusters. From the VM Cluster Details page, you can create your first database in the cluster by clicking **Create Database**. 

*To create an X7 or X8 Exadata DB system*

**Tip:**

Oracle recommends using the new [Exadata Cloud Service resource model](#) when provisioning a new service instance. The new resource model is compatible with all available Exadata shape families (X7, X8, and X8M).

The DB system resource described in this topic will be deprecated after a period where both resource models are supported. If you need to provision a service instance using the DB system resource model, you will be able to switch the instance to the new resource model. See [To switch an Exadata DB system to the new Exadata resource model](#) on page 1229 for more information. Customers with existing Exadata DB systems will be notified in advance regarding the deprecation of the DB system resource model.

1. Open the navigation menu. Under Oracle Database, click **Bare Metal, VM, and Exadata**.
2. Click **Create DB System**.
3. On the **Create DB System** page, provide the basic information for the DB system:

- **Select a compartment:** By default, the DB system launches in your current compartment and you can use the network resources in that compartment.

- **Name your DB system:** A friendly, display name for the DB system. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system. Avoid entering confidential information.

- **Select an availability domain:** The *availability domain* in which the DB system resides.

- **Select a shape type:** The shape type you select sets the default shape and filters the shape options in the next field.

When you select Exadata, you are asked if you would like to use the newer Exadata resource model that replaces the DB system resource with a cloud Exadata infrastructure resource and a cloud VM cluster. These resources are compatible with X7, X8, and X8M hardware generations. Click **Continue Creating DB System** if you do not want to use the new resource model.

- **Select a shape:** The shape determines the type of DB system and the resources allocated to the system. To specify a shape other than the default, click **Change Shape**, and select an available shape from the list. See Exadata Fixed Hardware Shapes: X6, X7, X8 and Exadata Base on page 1351 for available shapes in Oracle Cloud Infrastructure.

Note that the X8M shape is not available when using the DB system resource model.

- **Configure the DB system:** Specify the following:
  
  - **Total node count:** The number of nodes in the DB system. The number depends on the shape you select.
  
  - **Oracle Database software edition:** The database edition supported by the DB system. Exadata DB systems only support Enterprise Edition - Extreme Performance.
  
  - **CPU core count:** The number of CPU cores for the DB system. The text below the field indicates the acceptable values for that shape. The core count is evenly divided across the nodes.

You can increase the CPU cores to accommodate increased demand after you launch the DB system.

For an X8 or X7 Exadata DB system, or an Exadata base system, you can specify zero (0) CPU cores when you launch the system. This will provision the system and immediately stop it. See Scaling CPU Cores Within an Exadata Cloud Service Instance on page 1222 for information about CPU core scaling and the impact on billing. Oracle recommends that if you are not provisioning a stopped system (0 cores), that you specify at least 3 cores per node.

- **Configure storage:** Specify the following:

  - **Cluster Name:** *(Optional)* A unique cluster name for a multi-node DB system. The name must begin with a letter and contain only letters (a-z and A-Z), numbers (0-9) and hyphens (-). The cluster name can be no longer than 11 characters and is not case sensitive. Avoid entering confidential information.

  - **Storage Allocation:** The configuration settings that determine the percentage of storage assigned to DATA, RECO, and optionally, SPARSE disk:

    - **Database Backups on Exadata Storage:** Select this option if you intend to perform database backups to the local Exadata storage within your Exadata DB system environment. If you select this option, more space is allocated to the RECO disk group, which is used to store backups on Exadata storage. If you do not select this option, more space is allocated to the DATA disk group, which enables you to store more information in your databases.

    - **Create Sparse Disk Group:** Select this configuration option if you intend to use snapshot functionality within your Exadata DB system environment. If you select this option, the SPARSE disk group is created, which enables you to use Exadata DB system snapshot functionality for PDB sparse cloning. If you do not select this option, the SPARSE disk group is not created and Exadata DB system snapshot functionality will not be available on any database deployments that are created in the environment.

    **Important:**

    Creating a sparse disk group impacts the storage available for the ASM disk groups (DATA and RECO) and you cannot change the storage allocation configuration after you provision your DB system.
For information about the percentage of storage that will be assigned to DATA, RECO, and SPARSE disk based on your configuration, see Storage Configuration on page 1224. Similar information will display under the options in the Console dialog.

- **Add public SSH keys**: The public key portion of each key pair you want to use for SSH access to the DB system. You can browse or drag and drop .pub files, or paste in individual public keys. To paste multiple keys, click + Another SSH Key, and supply a single key for each entry.

- **Choose a license type**: The type of license you want to use for the DB system. Your choice affects metering for billing.
  - **License Included** means the cost of the cloud service includes a license for the Database service.
  - **Bring Your Own License (BYOL)** means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premises licenses and cloud licenses.

4. Specify the network information:

- **Virtual cloud network**: The VCN in which to launch the DB system. Click Change Compartment to select a VCN in a different compartment.

- **Client subnet**: The subnet to which the Exadata DB system should attach. Click Change Compartment to select a subnet in a different compartment.

  Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.

- **Backup subnet**: The subnet to use for the backup network, which is typically used to transport backup information to and from Oracle Cloud InfrastructureObject Storage, and for Data Guard replication. Click Change Compartment to select a subnet in a different compartment, if applicable.

  Do not use a subnet that overlaps with 192.168.128.0/20. This restriction applies to both the client subnet and backup subnet.

  If you plan to back up databases to Object Storage, see the network prerequisites in Managing Exadata Database Backups on page 1320.

- **Network Security Groups**: Optionally, you can specify one or more network security groups (NSGs) for both the client and backup networks. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to your DB system. A maximum of five NSGs can be specified. For more information,
see Network Security Groups on page 2841 and Network Setup for Exadata Cloud Service Instances on page 1232.

Note that if you choose a subnet with a security list, the security rules for the DB system will be a union of the rules in the security list and the NSGs.

To use network security groups:

- Check the Use Network Security Groups to Control Client Traffic check box. Note that you must already selected a VCN to be able to assign NSGs to the client network.
- Specify the NSG to use with the client network. You might need to use more than one NSG. If you're not sure, contact your network administrator.
- To use additional NSGs with the client network, click + Another Network Security Group.
- Check the Use Network Security Groups to Control Backup Traffic check box.
- Specify the NSG to use with the backup network just as described previously for the client subnet.
- **Hostname prefix:** Your choice of host name for the Exadata DB system. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for an Exadata DB system is 12.

![Important:]

The host name must be unique within the subnet. If it is not unique, the DB system will fail to provision.

- **Host domain name:** The domain name for the DB system. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. Hyphens (-) are not permitted.

If you plan to store database backups in Object Storage, Oracle recommends that you use a VCN Resolver for DNS name resolution for the client subnet because it automatically resolves the Swift endpoints used for backups.

- **Host and domain URL:** Combines the host and domain names to display the fully qualified domain name (FQDN) for the database. The maximum length is 64 characters.

5. Click Show Advanced Options to specify advanced options for the DB system:

- **Disk redundancy:** Exadata DB systems support only high redundancy (3-way mirroring).
- **Time zone:** The default time zone for the DB system is UTC, but you can specify a different time zone. The time zone options are those supported in both the Java.util.TimeZone class and the Oracle Linux operating system. For more information, see DB System Time Zone on page 1575.

![Tip:]

If you want to set a time zone other than UTC or the browser-detected time zone, and if you do not see the time zone you want, try selecting the Select another time zone option, then selecting "Miscellaneous" in the Region or country list and searching the additional Time zone selections.

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. After you completed the network configuration and any advanced options, click Next.
7. Provide information for the initial database:

- **Database name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.

- **Database version:** The version of the initial database created on the DB system when it is launched. After the DB system is active, you can create additional databases on it. You can mix database versions on the DB system.

  **Note:**
  
  If you plan to run Oracle Database 19c on your Exadata DB system, you must specify version 19c when you create the DB system. Earlier database versions are supported on a 19c Exadata DB system and can be created at anytime. Exadata DB systems created with earlier Oracle Database versions will not automatically support Oracle Database 19c. The DB system must be upgraded manually.

- **PDB name:** Not applicable to version 11.2.0.4. The name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of 8 alphanumeric characters. The only special character permitted is the underscore (_).

- **Create administrator credentials:** A database administrator SYS user will be created with the password you supply.
  
  - **Username:** SYS
  
  - **Password:** Supply the password for this user. The password must meet the following criteria:
    
    A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.
  
  - **Confirm password:** Re-enter the SYS password you specified.

- **Select workload type:** Choose the workload type that best suits your application:
  
  - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
  
  - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.

- **Configure database backups:** Specify the settings for backing up the database to Object Storage:
  
  - **Enable automatic backups:** Check the check box to enable automatic incremental backups for this database.
  
  - **Backup retention period:** (Optional) If you enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
  
  - **Backup scheduling (UTC):** If you enable automatic backups, you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default
Database window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See Automatic Incremental Backups for more information.

- Click **Show Advanced Options** to specify advanced options for the initial database.

In the **Management** tab you can specify the following options:

- **Character set**: The character set for the database. The default is AL32UTF8.
- **National character set**: The national character set for the database. The default is AL16UTF16.

In the **Encryption** tab, **Use Oracle-managed keys** is the only selection and cannot be changed during this creation process. You can change encryption management to use encryption keys that you manage after the database is provisioned. See To administer Vault encryption keys on page 1311 for more information.

In the **Tags** tab, you can add tags to the database. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

8. Click **Create DB System**. The DB system appears in the list with a status of Provisioning. The DB system's icon changes from yellow to green (or red to indicate errors).

After the DB system's icon turns green in the list of DB systems and displays the Available status, you can click the highlighted DB system name to see details about the DB system. Note the IP addresses. You'll need the private or public IP address, depending on network configuration, to connect to the DB system.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to create Exadata Cloud Service components.

**APIs for the New Exadata Cloud Service Resource Model**

The new Exadata resource model is compatible with all offered Exadata shape families (X7, X8, and X8M). See The New Exadata Cloud Service Resource Model on page 1228 for more information.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle recommended provisioning new Exadata Cloud Service instances using the new resource model. For Exadata instances, the DB system resource model will be deprecated after a period where both resource models are supported.</td>
</tr>
</tbody>
</table>

Cloud Exadata infrastructure resource:

- GetCloudExadataInfrastructure
- CreateCloudExadataInfrastructure
- ListCloudExadataInfrastructures

Cloud VM cluster resource:

- GetCloudVmCluster
- CreateCloudVmCluster
- ListCloudVmClusters
- GetCloudVmClusterIormConfig
- UpdateCloudVmClusterIormConfig

**APIs for DB System Resource Model (X7 and X8 Shapes Only)**

- GetDbSystem
- LaunchDbSystem
- ListDbSystems
Database Homes

- CreateDbHome
- GetDbHome
- ListDbHomes

Shapes and Database Versions

- ListDbSystemShapes
- ListDbVersions

Configuring a Static Route for Accessing the Object Store

All the traffic in an Exadata Cloud Service instance is, by default, routed through the data network. To route backup traffic to the backup interface (BONDETH1), you need to configure a static route on each of the compute nodes in the cluster. For instructions, see Node Access to Object Storage: Static Route on page 1236.

Setting Up DNS for an Exadata Cloud Service Instance

DNS lets you use host names instead of IP addresses to communicate with an Exadata Cloud Service instance. You can use the Internet and VCN Resolver (the DNS capability built into the VCN) as described in DNS in Your Virtual Cloud Network on page 2910. Oracle recommends using a VCN Resolver for DNS name resolution for the client subnet. It automatically resolves the Swift endpoints required for backing up databases, patching, and updating the cloud tooling on an Exadata instance.

Maintaining an Exadata Cloud Service Instance

User-Managed Maintenance Updates

Maintaining a secure Exadata Cloud Service instance in the best working order requires you to perform the following tasks regularly:

- Patching the Oracle Grid Infrastructure and Oracle Database software on the Exadata compute nodes. See Patching an Exadata Cloud Service Instance Manually on page 1289 and Oracle Clusterware Configuration and Administration for information and instructions.
- Updating the operating system and the tooling on the compute nodes. See Updating an Exadata Cloud Service Instance on page 1274 for information and instructions.

Oracle-Managed Infrastructure Maintenance Updates

In addition to the maintenance tasks you perform, Oracle manages the patching and updating of all other infrastructure components, including the physical compute nodes (Dom0), the Exadata storage servers, and the Exadata InfiniBand switches. This is referred to as DB system infrastructure maintenance.

Overview of the Infrastructure Patching Process

Infrastructure maintenance begins with patching of the Exadata compute nodes. Compute nodes are updated in a rolling fashion, with a single node being shut down, patched, and then brought back online while other nodes remain operational. This process continues until all nodes are patched. After compute node patching completes, Oracle patches the storage nodes. Storage server patching does not impact compute node availability.

Note that while databases are expected to be available during the patching process, Oracle does not verify that all database services and pluggable databases are available after a node is brought back online, as these can depend on the application service definition. Oracle recommends reviewing the documentation on workload management, application continuity, and client failover best practices to reduce the potential for an outage with your applications. By following the guidelines in the documentation, the impact of infrastructure patching will be only minor service degradation due to connection loss as compute nodes are sequentially patched.

Oracle recommends that you follow the Maximum Availability Architecture (MAA) best practices and use Oracle Data Guard to ensure the highest availability for your critical applications. For databases with Oracle Data Guard enabled, Oracle recommends that you separate the patching windows for the infrastructure instances running the
primary and standby databases, and perform a switchover prior to the maintenance operations for the infrastructure instance hosting the primary database, to avoid any impact to your primary database during infrastructure patching.

The approximate time for patching operations is as follows:

- Quarter rack: five hours
- Half rack: 10 hours
- Full rack: 20 hours

Typically, Exadata compute nodes require one and half hours each for patching, and storage servers require one hour each.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not perform major maintenance operations on your databases or applications during the patching window, as these operations could be impacted by the rolling patch operations.</td>
</tr>
</tbody>
</table>

**Scheduling Oracle-Managed Infrastructure Updates**

Exadata Cloud Service infrastructure updates are released on a quarterly basis. You can set a maintenance window to determine the time your quarterly infrastructure maintenance will begin. You can also view scheduled maintenance runs and the maintenance history of your Exadata Cloud Service instance in the Oracle Cloud Infrastructure Console on the Exadata Infrastructure Details or DB System Details page. For more information:

- To set the automatic maintenance schedule for Exadata Cloud Service infrastructure on page 1262
- To view or edit the time of the next scheduled maintenance for Exadata Cloud Service infrastructure on page 1263
- To view the maintenance history of an Exadata Cloud Service infrastructure resource on page 1263

In exceptional cases, Oracle can update your system apart from the regular quarterly updates to apply time-sensitive changes such as security updates. While you cannot opt out of these infrastructure updates, Oracle alerts you in advance through the Cloud Notification Portal to help you plan for them.

**Monitoring Patching Operations Using Lifecycle State Information**

The lifecycle state of your infrastructure resource (either the cloud Exadata infrastructure or the DB system resource) enables you to monitor when the patching of your infrastructure resource begins and ends. In the Oracle Cloud Infrastructure Console, you can see lifecycle state details messages on the Exadata Infrastructure Details or DB System Details page when a tool tip is displayed beside the **Status** field. You can also access these messages using the **ListCloudExadataInfrastructures** API (for cloud Exadata infrastructure resources) or the **ListDbSystems** API (for Exadata DB systems), and using tools based on the API, including SDKs and the **OCI CLI**.

During patching operations, you can expect the following:

- If you specify a maintenance window, then patching begins at your specified start time. The patching process starts with a series of prerequisite checks to ensure that your system can be successfully patched. These checks take approximately 30 minutes to complete. While the system is performing the checks, the infrastructure resource's lifecycle state remains "Available," and there is no lifecycle state message.

  For example, if you specify that patching should begin at 8:00 a.m., then Oracle begins patching operations at 8:00, but the infrastructure resource's lifecycle state does not change from "Available" to "Maintenance in Progress" until approximately 8:30 a.m.

- When Exadata compute node patching starts, the infrastructure resource's lifecycle state is "Maintenance in Progress", and the associated lifecycle state message is "The underlying infrastructure of this system (dbnodes) is being updated."

- When cell storage patching starts, the infrastructure resource's lifecycle state is "Maintenance in Progress", and the associated lifecycle state message is "The underlying infrastructure of this system (cell storage) is being updated and this will not impact Database availability."

- After cell patching is complete, the networking switches are patched one at a time, in a rolling fashion.

- When patching is complete, the infrastructure resource's lifecycle state is "Available", and the Console and API-based tools do not provide a lifecycle state message.
For More Information

For information about the update policy, and details such as the duration and impact on your system's availability and performance, see Oracle Database Cloud Exadata Service Supported Software Versions and Planning for Updates.

Managing an Exadata Cloud Service Instance

This topic describes management operations you can perform on an Exadata Cloud Service instance at the infrastructure level.

Note:

If your instance uses the older DB system resource model, all of the management operations discussed in this topic take place on the DB system resource.

If your instance uses the newer Exadata Cloud Service instance resource model, most of the management operations discussed in this topic take place on the cloud VM cluster resource. However, some operations, including those related to infrastructure maintenance, take place on the cloud Exadata infrastructure resource.

For all of the management tasks, this topic states which resource types the operation takes place on.

You can perform the management tasks discussed in this topic by using the Oracle Cloud Infrastructure Console or the API.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

Using the Console

To check the status of a cloud Exadata infrastructure resource

Note:

This topic only applies to Exadata Cloud Service instances using the new Exadata Cloud Service instance resource model.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Click Exadata Infrastructure under Exadata at Oracle Cloud.
4. In the list of cloud Exadata infrastructure resources, click the name of the infrastructure you're interested in and check its icon. The icon text indicates the status of the system. The following lifecycle states apply to the cloud Exadata infrastructure resource:

- **Provisioning**: Resources are being reserved for the cloud Exadata infrastructure resource. Provisioning can take several minutes. The resource is not ready to use yet.
- **Available**: The cloud Exadata infrastructure was successfully provisioned. You can create a cloud VM cluster on the resource to complete the infrastructure provisioning.
- **Updating**: The cloud Exadata infrastructure is being updated. The resource goes into the updating state during management tasks. For example, when moving the resource to another compartment, or creating a cloud VM cluster on the resource.
- **Terminating**: The cloud Exadata infrastructure is being deleted by the terminate action in the Console or API.
- **Terminated**: The cloud Exadata infrastructure has been deleted and is no longer available.
- **Failed**: An error condition prevented the provisioning or continued operation of the cloud Exadata infrastructure.

**To check the status of a cloud VM cluster**

**Note:**
This topic only applies to Exadata Cloud Service instances using the new Exadata Cloud Service instance resource model.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Click Exadata VM Clusters under Exadata at Oracle Cloud.
4. In the list of cloud VM clusters, find the cluster you're interested in and check its icon. The icon text indicates the status of the system. The following lifecycle states apply to the cloud VM cluster:

- **Provisioning**: Resources are being reserved for the cloud Exadata infrastructure resource. Provisioning can take several minutes. The resource is not ready to use yet.
- **Available**: The cloud Exadata infrastructure was successfully provisioned. You can create a cloud VM cluster on the resource to complete the infrastructure provisioning.
- **Updating**: The cloud Exadata infrastructure is being updated. The resource goes into the updating state during management tasks. For example, when moving the resource to another compartment, or creating a cloud VM cluster on the resource.
- **Terminating**: The cloud Exadata infrastructure is being deleted by the terminate action in the Console or API.
- **Terminated**: The cloud Exadata infrastructure has been deleted and is no longer available.
- **Failed**: An error condition prevented the provisioning or continued operation of the cloud Exadata infrastructure.

To view the status of a virtual machine (database node) in the cloud VM cluster, under Resources, click Virtual Machines to see the list of virtual machines. In addition to the states listed for a cloud VM cluster, a virtual machine's status can be one of the following:

- **Starting**: The database node is being powered on by the start or reboot action in the Console or API.
- **Stopping**: The database node is being powered off by the stop or reboot action in the Console or API.
- **Stopped**: The database node was powered off by the stop action in the Console or API.

**To check the status of an Exadata DB system**

**Note:**
This topic only applies to Exadata Cloud Service instances using the DB system resource model.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.

A list of DB systems is displayed.
3. In the list of DB systems, find the system you're interested in and check its icon. The icon text indicates the status of the system. The following lifecycle states apply to the DB system resource:

- **Provisioning:** Resources are being reserved for the DB system, the system is booting, and the initial database is being created. Provisioning can take several minutes. The system is not ready to use yet.
- **Available:** The DB system was successfully provisioned. A few minutes after the system enters this state, you can SSH to it and begin using it.
- **Terminating:** The DB system is being deleted by the terminate action in the Console or API.
- **Terminated:** The DB system has been deleted and is no longer available.
- **Failed:** An error condition prevented the provisioning or continued operation of the DB system.

To view the status of a database node, under Resources, click **Nodes** to see the list of nodes. In addition to the states listed for a DB system, a node's status can be one of the following:

- **Starting:** The database node is being powered on by the start or reboot action in the Console or API.
- **Stopping:** The database node is being powered off by the stop or reboot action in the Console or API.
- **Stopped:** The database node was powered off by the stop action in the Console or API.

You can also check the status of DB systems and database nodes using the **ListDbSystems** or **ListDbNodes** API operations, which return the `lifecycleState` attribute.

**To start, stop, or reboot an Exadata Cloud Service cloud VM cluster or DB system**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the cloud VM cluster or DB system you want to start, stop, or reboot:

   - **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - **DB systems:** Under **Bare Metal, VM, and Exadata**, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. Under **Resources**, click **Virtual Machines** (for cloud VM clusters) or **Nodes** (for DB systems) to display the compute nodes of the cloud service instance. Click the Actions icon (three dots) for a node and then click one of the following actions:

   - **Start:** Restarts a stopped node. After the node is restarted, the **Stop** action is enabled.
   - **Stop:** Shuts down the node. After the node is powered off, the **Start** action is enabled.
   - **Reboot:** Shuts down the node, and then restarts it.

**Note:**

- For billing purposes, the **Stop** state has no effect on the resources you consume. Billing continues for virtual machines or nodes that you stop, and related resources continue to apply against any relevant quotas. You must **Terminate** a cloud VM cluster or DB system to remove its resources from billing and quotas.
- After you restart or reboot a node, the floating IP address might take several minutes to be updated and display in the Console.

**To scale CPU cores in an Exadata Cloud Service cloud VM cluster or DB system**

**Note:**

For information on adding additional database (compute) and storage servers to **X8M cloud VM clusters**, see **To add compute and storage resources to a flexible cloud Exadata infrastructure resource** on page 1230 and **To add database server or storage server capacity to a cloud VM cluster** on page 1230. Adding additional database servers to your X8M cloud VM cluster will increase the number of CPU cores available for scaling.
If an Exadata Cloud Service instance requires more compute node processing power, you can scale up (increase) the number of enabled CPU cores (OCPUs) in the instance.

You can also scale a cloud VM cluster or DB system (except for X6 systems) down to zero (0) CPU cores to temporarily stop the system and be charged only for the hardware infrastructure. For more information about scaling down, see Scaling Options on page 1222. Oracle recommends that if you are not scaling down to a stopped system (0 cores), that you scale to at least 3 cores per node.

CPU cores must be scaled symmetrically across all nodes in the cloud VM cluster or DB system. Use multiples of two for a base system or quarter rack, multiples of four for a half rack, and multiples of eight for a full rack. The total number of CPU cores in a rack must not exceed the maximum limit for that shape.

| Tip: |
| OCPU scaling activities are done online with no downtime. |

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to scale:
   - **Cloud VM clusters (new resource model):** Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. Click Scale VM Cluster (for cloud VM clusters) or Scale CPU Cores (for DB systems) and then specify a new number of CPU cores. The text below the field indicates the acceptable values, based on the shape used when the DB system was launched.
5. Click Update.

| Note: |
| If you scale a cloud VM cluster or DB system (except for X6 systems) down to zero (0) CPU cores, the floating IP address of the nodes might take several minutes to be updated and display in the Console. |

**To move an Exadata Cloud Service infrastructure resource to another compartment**

| Note: |
| - To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Database resources, see Details for the Database Service on page 2240.
  - If your Exadata Cloud Service instance is in a security zone, the destination compartment must also be in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources. |

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud Exadata infrastructure, cloud VM cluster or DB system you want to move:

**Cloud Exadata infrastructure (new resource model):** Under [Exadata at Oracle Cloud](https://oracle.com), click **Exadata Infrastructure**. In the list of infrastructure resources, find the infrastructure you want to access and click its highlighted name to view its details page.

**Cloud VM clusters (new resource model):** Under [Exadata at Oracle Cloud](https://oracle.com), click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

**DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. Click **Move Resource**.

5. Select the new compartment.

6. Click **Move Resource**.

For information about dependent resources for Database resources, see [Moving Database Resources to a Different Compartment](https://oracle.com) on page 1141.

### To terminate Exadata Cloud Service infrastructure-level resources

This topic describes how to terminate a cloud Exadata infrastructure, cloud VM cluster, or DB system resource in an Exadata Cloud Service instance.

**Note:**

The database data is local to the cloud VM cluster or DB system hosting it and is lost when the system is terminated. Oracle recommends that you back up any data in the cloud VM cluster or DB system before terminating it.

Terminating an Exadata Cloud Service resource permanently deletes it and any databases running on it.

---

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose your **Compartment**.

3. Navigate to the cloud Exadata infrastructure, cloud VM cluster or DB system you want to move:

   **Cloud Exadata infrastructure (new resource model):** Under [Exadata at Oracle Cloud](https://oracle.com), click **Exadata Infrastructure**. In the list of infrastructure resources, find the infrastructure you want to access and click its highlighted name to view its details page.

   **Cloud VM clusters (new resource model):** Under [Exadata at Oracle Cloud](https://oracle.com), click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. For cloud VM clusters and DB systems, click **More Actions**, then **Terminate** on the resource details page. For cloud Exadata infrastructure resources, click **Terminate** on the resource details page.

   Confirm when prompted.

   The resource's icon indicates Terminating.

**Note:**

If you are terminating a cloud Exadata infrastructure resource that contains a cloud VM cluster, you must check the box labelled **Also delete the VM cluster associated with this infrastructure** to confirm that you intend to delete the VM cluster.

At this point, you cannot connect to the system and any open connections are terminated.
To edit the network security groups (NSGs) for your client or backup network

Your client and backup networks can each use up to five network security groups (NSGs). Note that if you choose a subnet with a security list, the security rules for the cloud VM cluster or DB system will be a union of the rules in the security list and the NSGs. For more information, see Network Security Groups on page 2841 and Network Setup for Exadata Cloud Service Instances on page 1232.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to manage:

   Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. In the Network details, click the Edit link to the right of the Client Network Security Groups or Backup Network Security Groups field.
5. In the Edit Network Security Groups dialog, click + Another Network Security Group to add an NSG to the network.

   To change an assigned NSG, click the drop-down menu displaying the NSG name, then select a different NSG.

   To remove an NSG from the network, click the X icon to the right of the displayed NSG name.

6. Click Save.

To manage your BYOL database licenses

If you want to control the number of database licenses that you run at any given time, you can scale up or down the number of OCPUs on the instance. These additional licenses are metered separately.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to scale:

   Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. Click Scale VM Cluster (for cloud VM clusters) or Scale CPU Cores (for DB systems) and then specify a new number of CPU cores. The text below the field indicates the acceptable values, based on the shape used when the DB system was launched.

5. Click Update.

To change the license type of an Exadata Cloud Service cloud VM cluster or DB system

Note:

Updating the license type is not supported for systems running on the X6 shape. The feature is supported for X7 and higher shapes.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to manage:

   * **Cloud VM clusters (new resource model):** Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   * **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. On the resource details page, click Update License Type.

   The dialog displays the options with your current license type selected.

5. Select the new license type.

6. Click Save.

To manage tags for your Exadata Cloud Service resources

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.

2. Choose your Compartment.

3. Find the cloud Exadata infrastructure, cloud VM cluster, DB system or database resource you're interested in, and click the name.

4. Click the Tags tab to view or edit the existing tags. Or click More Actions and then Apply Tags to add new ones.

   For more information, see Resource Tags on page 211.

To view a work request for your Exadata Cloud Service resources

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.

2. Choose your Compartment.

   A list of DB systems is displayed.

3. Find the cloud Exadata infrastructure, cloud VM cluster, DB system or database resource you're interested in, and click the name.

4. In the Resources section, click Work Requests. The status of all work requests appears on the page.

5. To see the log messages, error messages, and resources that are associated with a specific work request, click the operation name. Then, select an option in the More information section.

   For associated resources, you can click the Actions icon (three dots) next to a resource to copy the resource's OCID.

   For more information, see Work Requests on page 258.

To set the automatic maintenance schedule for Exadata Cloud Service infrastructure

This task describes how to set the maintenance schedule for a cloud Exadata infrastructure or Exadata DB system resource. See Oracle-Managed Infrastructure Maintenance Updates on page 1254 for more information on this type of maintenance.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.

2. Navigate to the cloud Exadata infrastructure or DB system you want to access:

   * **Cloud Exadata infrastructure (new resource model):** Under Exadata at Oracle Cloud, click Exadata Infrastructure. In the list of infrastructure resources, find the infrastructure you want to access and click its highlighted name to view its details page.

   * **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

3. On the resource details page, under Maintenance or Infrastructure Maintenance, click the edit link in the Maintenance Schedule field.

4. In the Automatic Maintenance Schedule dialog, select Specify a schedule.

5. Under Maintenance months, specify at least one month for each quarter during which Exadata infrastructure maintenance will take place. You can select more than one month per quarter. If you specify a long lead time for advanced notification (for example, 4 weeks), then you may want to specify two or three months per quarter.
during which maintenance runs can occur. This will ensure that your maintenance updates are applied in a timely manner after accounting for your required lead time. Lead time is discussed in the following steps.

6. **Under Week of the month**, specify which week of the month maintenance will take place. Weeks start on the 1st, 8th, 15th, and 22nd days of the month, and have a duration of seven days. Weeks start and end based on calendar dates, not days of the week. Maintenance cannot be scheduled for the fifth week of months that contain more than 28 days.

7. **Optional.** Under **Day of the week**, specify the day of the week on which the maintenance will occur. If you do not specify a day of the week, then Oracle will run the maintenance update on a weekend day to minimize disruption.

8. **Optional.** Under **Start hour**, specify the hour during which the maintenance run will begin. If you do not specify a start hour, then Oracle will choose the least disruptive time to run the maintenance update.

9. Under **Lead Time**, specify the number of weeks ahead of the maintenance event you would like to receive a notification message. Your lead time ensures that a newly released maintenance update is scheduled to account for your required period of advanced notification.

10. Click **Update Maintenance Schedule**.

To **view or edit the time of the next scheduled maintenance for Exadata Cloud Service infrastructure**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Navigate to the cloud Exadata infrastructure or DB system you want to access:

   * **Cloud Exadata infrastructure (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata Infrastructure**. In the list of infrastructure resources, find the infrastructure you want to access and click its highlighted name to view its details page.

   * **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

3. On the resource details page, under **Maintenance** or **Infrastructure Maintenance**, click the **view** link in the **Next Maintenance** field.

4. On the **Maintenance** page, scheduled maintenance events are listed.

5. **Optional.** To change the time of the next scheduled maintenance, click the Edit link in the **Scheduled Start Time** field.

6. In the **Edit Infrastructure Maintenance Scheduled Start Time** dialog, enter a date and time in the **Scheduled start time** field.

   The following restrictions apply:
   
   - Infrastructure maintenance cannot be rescheduled to occur more than six months after the announcement of the maintenance update's availability. If a new patch is announced prior to your rescheduled maintenance run, the newer patch will be applied on your specified date. You can reschedule your maintenance to take place earlier than it is currently scheduled.
   - Oracle reserves certain dates each quarter for internal maintenance operations, and you cannot schedule your maintenance on these dates. When using the Console, the selection of these dates is disabled.

7. Click **Update Scheduled Start Time**.

To **view the maintenance history of an Exadata Cloud Service infrastructure resource**

This task describes how to view the maintenance history for a cloud Exadata infrastructure or DB system resource. See **Oracle-Managed Infrastructure Maintenance Updates** on page 1254 for more information on this type of maintenance.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Navigate to the cloud Exadata infrastructure or DB system you want to access:

   * **Cloud Exadata infrastructure (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata Infrastructure**. In the list of infrastructure resources, find the infrastructure you want to access and click its highlighted name to view its details page.

   * **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
3. On the resource details page, under **Maintenance** or **Infrastructure Maintenance**, click the **view** link in the **Next Maintenance** field.

4. Click **Maintenance History** to see a list of past maintenance events including details on their completion state.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage Exadata Cloud Service instance components.

**Cloud Exadata infrastructure resource (new resource model):**

- ListCloudExadataInfrastructures
- GetCloudExadataInfrastructure
- ChangeCloudExadataInfrastructureCompartment
- UpdateCloudExadataInfrastructure
- DeleteCloudExadataInfrastructure

**Cloud VM cluster (new resource model)**

- ListCloudVmClusters
- GetCloudVmCluster
- ChangeCloudVmClusterCompartment
- UpdateCloudVmCluster
- GetCloudVmClusterIormConfig
- UpdateCloudVmClusterIormConfig
- DeleteCloudVmCluster

**DB systems (old resource model):**

- ListDbSystems
- GetDbSystem
- ChangeDbSystemCompartment
- UpdateDbSystem
- TerminateDbSystem

**Nodes:**

- DbNodeAction: Use this operation to power cycle a node in the DB system.
- ListDbNodes
- GetDbNode

**Managing Exadata Cloud Service I/O Resource Management (IORM)**

This topic explains the I/O Resource Management (IORM) feature and how to enable it, modify the IORM settings, and disable it by using the Console or the API.

**About IORM**

The I/O Resource Management (IORM) feature allows you to manage how multiple databases share the I/O resources of an Oracle Exadata cloud VM cluster (for systems using the **new resource model**) or DB system.

On an Exadata VM cluster or DB system, all databases share dedicated storage servers which include flash storage. By default, the databases are given equal priority with respect to these resources. The Exadata storage management software uses a first come, first served approach for query processing. If a database executes a major query that overloads I/O resources, overall system performance can be slowed down.

IORM allows you to assign priorities to your databases to ensure critical queries are processed first when workloads exceed their resource allocations. You assign priorities by creating directives that specify the number of shares for each database. The number of shares corresponds to a percentage of resources given to that database when I/O resources are stressed.
Directives work together with an overall optimization objective you set for managing the resources. The following objectives are available:

- **Auto** - Recommended. IORM determines the optimization objective and continuously and dynamically determines the optimal settings, based on the workloads observed, and resource plans enabled.
- **Balanced** - For critical OLTP and DSS workloads. This setting balances low disk latency and high throughput. This setting limits disk utilization of large I/Os to a lesser extent than low latency to achieve a balance between good latency and good throughput.
- **High throughput** - For critical DSS workloads that require high throughput.
- **Low latency** - For critical OLTP workloads. This setting provides the lowest possible latency by significantly limiting disk utilization.

For more information about IORM, see Exadata System Software User's Guide.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

**Using the Console**

*To enable IORM on your Exadata cloud VM cluster*

**Note:**

This topic only applies to Exadata Cloud Service systems using the new infrastructure resource model. If you are enabling IORM for an Exadata DB system, see To enable IORM on your Exadata DB system on page 1266.

Enabling IORM includes specifying an optimization objective and configuring your resource plan directives.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Click Exadata VM Clusters under the Exadata at Oracle Cloud.
4. In the list of VM clusters, find the VM cluster for which you want to enable IORM, and click its highlighted name. The cluster's details are displayed, showing the IORM status as “Disabled.”
5. Click More Actions, then Enable IORM.
   
   It might take a minute for the Enable I/O Resource Management dialog to retrieve the VM cluster information.
6. Select the objective to apply to the resource plan:
   
   - **Auto** - (Recommended) Dynamically changes the objective based on the resource plan and observed workloads.
   - **Balanced** - Weighs high throughput and low latency evenly.
   - **High throughput** - Provides the best throughput for DSS workloads.
   - **Low latency** - Provides the best latency for critical OLTP workloads.
7. Configure the resource plan default directive by setting the number of shares. This number of shares is assigned to each database not associated with a specific directive.
8. In the Resource Plan Directives section, add a directive for each database you want to assign a greater or lesser number of shares than the default directive.

   To add a directive, click + Additional Directive, then specify the database and the number of shares for that database.
9. When you are done adding directives, click **Enable**.

While the IORM configuration settings are being applied, the VM cluster details page shows the IORM status as "Updating." The update might take several minutes to complete but should have no impact on your ability to perform normal operations on your VM cluster. After a successful update, the IORM status shows as "Enabled."

**To modify the IORM configuration on your cloud VM cluster**

**Note:**

This topic only applies to Exadata Cloud Service systems using the new infrastructure resource model. If you are updating an Exadata DB system, see To modify the IORM configuration on your Exadata DB system on page 1267.

Use this procedure to change your IORM settings or to disable IORM.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Click **Exadata VM Clusters** under **Exadata at Oracle Cloud**.
4. In the list of VM clusters, find the VM cluster for which you want to update IORM, and click its highlighted name. The cluster's details are displayed, showing the IORM status as "Enabled."
5. Click **More Actions**, then **Update IORM**.
6. In the Update I/O Resource Management dialog, take one of the following actions:
   - Change your settings - Specify a new objective and adjust your directives, as applicable, and then click **Update**.
   - Disable IORM - Click **Disable IORM**. Disabling IORM removes all your resource plan directives and restores a basic objective for I/O resource management.

While the new IORM configuration settings are being applied, the system details page shows the IORM status as "Updating." The update might take several minutes to complete but should have no impact on your ability to perform normal operations on your DB system. After a successful update, the IORM status shows as "Enabled" or "Disabled," depending on the action you took.

**To enable IORM on your Exadata DB system**

**Note:**

This topic only applies to Exadata Cloud Service instances using the DB system resource model.

Enabling IORM includes specifying an optimization objective and configuring your resource plan directives.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. In the list of DB systems, find the Exadata DB system for which you want to enable IORM, and click its highlighted name.
   
   The system details are displayed, showing the IORM status as "Disabled."
4. Click **More Actions**, then **Enable IORM**.
   
   It might take a minute for the Enable I/O Resource Management dialog to retrieve the DB system information.
5. Select the objective to apply to the resource plan:
   - **Auto** - (Recommended) Dynamically changes the objective based on the resource plan and observed workloads.
   - **Balanced** - Weighs high throughput and low latency evenly.
   - **High throughput** - Provides the best throughput for DSS workloads.
   - **Low latency** - Provides the best latency for critical OLTP workloads.
6. Configure the resource plan default directive by setting the number of shares. This number of shares is assigned to each database not associated with a specific directive.
7. In the Resource Plan Directives section, add a directive for each database you want to assign a greater or lesser number of shares than the default directive.

To add a directive, click **Additional Directive**, then specify the database and the number of shares for that database.

8. When you are done adding directives, click **Enable**.

While the IORM configuration settings are being applied, the system details page shows the IORM status as "Updating." The update might take several minutes to complete but should have no impact on your ability to perform normal operations on your DB system. After a successful update, the IORM status shows as "Enabled."

**To modify the IORM configuration on your Exadata DB system**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This topic only applies to Exadata Cloud Service instances using the DB system resource model.</td>
</tr>
</tbody>
</table>

Use this procedure to change your IORM settings or to disable IORM.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. In the list of DB systems, find the Exadata DB system for which you want to modify the IORM configuration, and click its highlighted name.

The system details are displayed, showing the IORM status as "Enabled."

4. Click **More Actions**, then **Update IORM**.
5. In the Update I/O Resource Management dialog, take one of the following actions:

   - Change your settings - Specify a new objective and adjust your directives, as applicable, and then click **Update**.
   - Disable IORM - Click **Disable IORM**. Disabling IORM removes all your resource plan directives and restores a basic objective for I/O resource management.

While the new IORM configuration settings are being applied, the system details page shows the IORM status as "Updating." The update might take several minutes to complete but should have no impact on your ability to perform normal operations on your DB system. After a successful update, the IORM status shows as "Enabled" or "Disabled," depending on the action you took.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage the I/O resources of an Exadata cloud VM cluster (see **The New Exadata Cloud Service Resource Model** on page 1228 for more information on this resource type).

- **ListCloudVmClusters**
- **GetCloudVmCluster**
- **GetCloudVmClusterIormConfig**
- **UpdateCloudVmClusterIormConfig**

Use these API operations to manage the I/O resources of an Exadata DB system.

- **ListDbSystems**
- **GetDbSystem**
- **GetExadataIormConfig**
- **UpdateExadataIormConfig**
Managing Exadata Resources with Oracle Enterprise Manager Cloud Control

This topic provides a short introduction to Oracle Enterprise Manager Cloud Control, a tool that can be used to manage and monitor Exadata Cloud and Exadata Cloud@Customer resources. For complete documentation and Oracle By Example tutorials, see Additional Information on page 1268 at the end of this topic.

Overview

Oracle Enterprise Manager Cloud Control provides a complete lifecycle management solution for Oracle Cloud Infrastructure's Exadata Cloud and Exadata Cloud@Customer services.

Enterprise Manager Cloud Control discovers Exadata Cloud and Exadata Cloud@Customer services as a single target and automatically identifies and organizes all dependent components. Using Enterprise Manager Cloud Control you can then:

- Monitor and manage all Exadata, Exadata Cloud and Exadata Cloud@Customer systems, along with any other targets, from a single interface
- Visualize storage and compute data
- View performance metrics of your Exadata components

Features

Enterprise Manager Target for Exadata Cloud

The target for Oracle Cloud Infrastructure Exadata resources (which covers both Exadata Cloud and Exadata Cloud@Customer) does the following:

- Automatically identifies and organizes related targets
- Provides a high-level integration point for Enterprise Manager framework features such as incident rules, groups, notifications, and monitoring templates

Improved Performance Monitoring

Enterprise Manager Cloud Control enhances performance monitoring in the following ways:

- Adds Exadata Storage Server and Exadata Storage Grid targets
- Offers visualization of storage and compute performance for your Exadata Cloud and Exadata Cloud@Customer resources
- Enables use of the same Maximum Availability Architecture (MAA) key performance indicators (KPI) developed for Oracle Exadata Database Machine

Scripted CLI-based Discovery

Enterprise Manager Cloud Control uses scripts to discover Oracle Cloud Infrastructure Exadata resources. Scripts comb the existing hosts, clusters, ASM, databases and related targets, as well as adding the storage server targets

"Single Pane of Glass" View of On-Premises and Oracle Cloud Infrastructure Exadata Resources

Enterprise Manager Cloud Control's use of a single Exadata target type provides a consistent Enterprise Manager experience across on-premises, Exadata Cloud, and Exadata Cloud@Customer resources. The common Exadata target menu allows you to easily navigate to, monitor and manage all of your Exadata systems.

Visualization

Enterprise Manager Cloud Control allows you to visualize the database and related targets associated with each Exadata Cloud and Exadata Cloud@Customer system.

Additional Information

For more information on Oracle Enterprise Manager Cloud Control, see the following documentation resources:

- Oracle Enterprise Manager Cloud Control for Oracle Exadata Cloud
Connecting to an Exadata Cloud Service Instance

This topic explains how to connect to an Exadata Cloud Service instance using SSH or SQL Developer. How you connect depends on how your cloud network is set up. You can find information on various networking scenarios in Networking Overview on page 2748, but for specific recommendations on how you should connect to a database in the cloud, contact your network security administrator.

Prerequisites

For SSH access to a compute node in an Exadata Cloud Service instance, you'll need the following:

• The full path to the file that contains the private key associated with the public key used when the system was launched.
• The public or private IP address of the Exadata Cloud Service instance.

Use the private IP address to connect to the system from your on-premises network, or from within the virtual cloud network (VCN). This includes connecting from a host located on-premises connecting through a VPN or FastConnect to your VCN, or from another host in the same VCN. Use the public IP address to connect to the system from outside the cloud (with no VPN). You can find the IP addresses in the Oracle Cloud Infrastructure Console as follows:

• Cloud VM clusters (new resource model): On the Exadata VM Cluster Details page, click Virtual Machines in the Resources list.
• DB systems: On the DB System Details page, click Nodes in the Resources list.

The values are displayed in the Public IP Address and Private Address & DNS Name columns of the table displaying the Virtual Machines or Nodes of the Exadata Cloud Service instance.

Connecting to a Compute Node with SSH

You can connect to the compute nodes in an Exadata DB System by using a Secure Shell (SSH) connection. Most UNIX-style systems (including Linux, Solaris, BSD, and OS X) include an SSH client by default. For Windows, you can download a free SSH client called PuTTY from http://www.putty.org.

To connect from a UNIX-style system

Use the following SSH command to access a compute node:

```
$ ssh -i <private key> opc@<DB System IP address>
```

<private key> is the full path and name of the file that contains the private key associated with the Exadata DB System you want to access.

Use the private or public IP address depending on your network configuration. For more information, see Prerequisites on page 1391.

To connect from a Windows system

1. Open putty.exe.
2. In the Category pane, select Session and enter the following fields:
   • Host Name (or IP address): opc@<ip_address>
     Use the compute node's private or public IP address depending on your network configuration. For more information, see Prerequisites on page 1391.
   • Connection type: SSH
   • Port: 22
3. In the Category pane, expand Connection, expand SSH, and then click Auth, and browse to select your private key.
4. Optionally, return to the Session category screen and save this session information for reuse later.
5. Click Open to start the session.
To access a database after you connect to the compute node

1. Log in as opc and then sudo to the oracle user.

```
login as: opc
[opc@<host_name> ~]$ sudo su - oracle
```

2. Source the database's .env file to set the environment.

```
[oracle@<host_name>]# . <database_name>.env
```

In the following example, the host name is "ed1db01" and the database name is "cdb01".

```
[oracle@ed1db01]# . cdb01.env
ORACLE_SID = [root] ? +ASM1
The Oracle base has been set to /u01/app/grid
```

Connecting to a Database with SQL Developer

You can connect to a database with SQL Developer by using one of the following methods:

- Create a temporary SSH tunnel from your computer to the database. This method provides access only for the duration of the tunnel. (When you are done using the database, be sure to close the SSH tunnel by exiting the SSH session.)

- Open port 1521 for the Oracle default listener by updating the security list used for the cloud VM cluster or DB system resource in the Exadata Cloud Service instance. This method provides more durable access to the database. For more information, see Updating the Security List on page 1305.

After you’ve created an SSH tunnel or opened port 1521 as described above, you can connect to a Exadata Cloud Service instance using SCAN IP addresses or public IP addresses, depending on how your network is set up and where you are connecting from. You can find the IP addresses in the Console, in the Database details page.

To connect using SCAN IP addresses

You can connect to the database using the SCAN IP addresses if your client is on-premises and you are connecting using a FastConnect or VPN connection. You have the following options:

- Use the private SCAN IP addresses, as shown in the following tnsnames.ora example:

  ```
  testdb=
  (DESCRIPTION =
   (ADDRESS_LIST=
    (ADDRESS = (PROTOCOL = TCP)(HOST = <scanIP1>)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = <scanIP2>)(PORT = 1521)))
   (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = <dbservice.subnetname.dbvcn.oraclevcn.com>)
   )
  )
  ```

- Define an external SCAN name in your on-premises DNS server. Your application can resolve this external SCAN name to the DB System's private SCAN IP addresses, and then the application can use a connection string that includes the external SCAN name. In the following tnsnames.ora example, extscanname.example.com is defined in the on-premises DNS server.

  ```
  testdb =
  (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = <extscanname.example.com>)(PORT = 1521))
  )
  ```
To connect using public IP addresses

You can use the node's public IP address to connect to the database if the client and database are in different VCNs, or if the database is on a VCN that has an internet gateway. However, there are important implications to consider:

- When the client uses the public IP address, the client bypasses the SCAN listener and reaches the node listener, so server side load balancing is not available.
- When the client uses the public IP address, it cannot take advantage of the VIP failover feature. If a node becomes unavailable, new connection attempts to the node will hang until a TCP/IP timeout occurs. You can set client side sqlnet parameters to limit the TCP/IP timeout.

The following tnsnames.ora example shows a connection string that includes the CONNECT_TIMEOUT parameter to avoid TCP/IP timeouts.

```sql
TEST=
  (DESCRIPTION =
    (CONNECT_TIMEOUT=60)
    (ADDRESS_LIST=
      (ADDRESS = (PROTOCOL = TCP)(HOST = <publicIP1>)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = <publicIP2>)(PORT = 1521))
    )
  (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = <dbservice.subnetname.dbvcn.oraclevcn.com>)
  )
)
```

Managing Exadata Cloud Service Software Images Using the Dbaascli Utility

You can create custom database software images for your Exadata Cloud Service instances using the Console or API. These images are stored in Object Storage, and can be used to provision a Database Home in your Exadata instance. See Oracle Database Software Images on page 1567 more information.

You can control the version of Oracle binaries that is installed when you provision a new database on an Exadata Cloud Service instance by maintaining the software images on the system. Oracle provides a library of cloud software images that you can view and download onto your instance by using the dbaascli utility.

When you create a new database with a new Oracle Home (Database Home) directory location, the Oracle Database binaries are sourced from a software image that is stored on your Exadata Cloud Service instance. Over time, the software images on your instance become outdated if they are not maintained. Using an outdated software image makes it necessary for you to apply patches to newly installed binaries to bring them up to date. Oracle recommends that you maintain your instance with up-to-date software images to avoid this extra patching step which can be time-consuming and error prone.

Viewing Information About Available Software Images

You can view information about Oracle Database software images that are available to download to your Exadata Cloud Service instance by using the cswlib list subcommand of the dbaascli utility.
To view information about available software images

1. Connect to a compute node as the opc user.
   For detailed instructions, see Connecting to a Compute Node with SSH on page 1269.
2. Start a root-user command shell:
   
   $ sudo -s
   #
3. Execute the dbaascli command with the cswlib list subcommand:
   
   # dbaascli cswlib list

   The command displays a list of available software images, including version and bundle patch information that you can use to download the software image.
4. Exit the root-user command shell:
   
   # exit
   $

Downloading Software Images

You can download available software images onto your Exadata Cloud Service instance by using the cswlib download subcommand of the dbaascli utility.

To downloaded a software image

1. Connect to a compute node as the opc user.
   For detailed instructions, see Connecting to a Compute Node with SSH on page 1269.
2. Start a root-user command shell:
   
   $ sudo -s
   #
3. Execute the dbaascli command with the cswlib download subcommand:
   
   # dbaascli cswlib download [--version <software_version>] [--bp <software_bundle_patch>]

   The command displays a list of software images that are downloaded to your Exadata Cloud Service environment, including version and bundle patch information.

   The optional parameters are:
   
   • **version**: specifies an Oracle Database software version. For example, 19000, 18000, or 12201.
   • **bp**: identifies a bundle patch release. For example, APR2021, JAN2021, or OCT2020.

   If you do not include the optional parameters, the dbaascli cswlib download command downloads the latest available software image for all available Oracle Database software versions.
4. Exit the root-user command shell:
   
   # exit
   $

Updating an Exadata Cloud Service VM Cluster Operating System

Exadata VM Cluster Image Updates is a feature that enables ExaCS customers to update the OS image on their Exadata VM Cluster nodes in an automated manner from their OCI console and APIs.
**Introduction**

Exadata VM Cluster Image Updates allows you to update the OS image on your Exadata VM Cluster nodes in an automated manner from the OCI console and APIs. This automated feature greatly simplifies and speeds up the process, makes it less error prone, and eliminates the need to use Patch Manager.

When you apply a patch, the system runs a precheck operation to ensure your VM cluster, Exadata DB system, or Database Home meets the requirements for that patch. If the precheck is not successful, the patch is not applied, and the system displays a message that the patch cannot be applied because the precheck failed. A separate precheck operation that you can run in advance of the planned update is also available.

**Supported versions**

The following versions and limitations are supported:

- Only Exadata image major versions 19 and above are supported.
- You cannot move to a new major version. For example, if the ExaCS VM Cluster is on major version 20 then you can apply only image updates for version 20.
- Only the latest generation of Exadata VM Cluster images are shown on the console and can be applied.

**Updating the operating system**

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. In the list of DB systems, click the name of the Exadata DB system that you want to patch to display the DB system details.
4. In the Version section, to the right of the Updates Available label, click View Updates to display the Updates/patches page.
5. Review the list of available patches for the DB system.
6. To the right of the Created field, click the Actions icon (three dots) for the patch you are interested in, and then click one of the following actions:
   - **Run Precheck.** Precheck checks the prerequisites to ensure that the patch can be successfully applied. Oracle highly recommends that you run the precheck operation before you apply a patch. The reason is that things can change in a database any time, and the precheck you run just before running a patch may find errors that the previous precheck did not find.
   - **Apply Exadata Image Update.** This link displays the Apply Exadata Image Update dialog box that you use to apply the patch. The dialog box shows the name of the database system you are patching, the current version of the database, and the new version of the database after the patch is applied. To start the process, click Apply Exadata Image Update.
   - **Copy OCID.** This copies the Oracle Cloud ID. This can be used when troubleshooting a patch or to give to Support when contacting them.

**Note:**

If the precheck fails, the system displays a message in the Apply OS Image Update dialog box that the last precheck has failed. Oracle recommends that you run the precheck again.

**Note:**

While the patch is running:

- Run Precheck and Apply OS Image Update are not available. When the patch has completed, these actions are available again.
- If the Exadata infrastructure containing this VM cluster is scheduled for maintenance that conflicts with the timing of the patch, the patch fails and the system displays a message explaining why. After the infrastructure maintenance is complete, run the patch again.

7. Confirm when prompted.
8. The patch list displays the status of the operation in the Version section of the database details page. Click **View Updates** to view more details about an individual patch status and to display any updates that are available to run. If no new updates are available, the system displays a message that says **No Updates Available**.

**Patching and Precheck states, and DB system status**

The following table shows the various states of precheck and patch operations and the status of the DB system during each operation.

<table>
<thead>
<tr>
<th>Operation</th>
<th>DB System Status</th>
<th>Patch State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Available</td>
<td>Available</td>
<td>The update is available to patch a database or database home.</td>
</tr>
<tr>
<td>Precheck</td>
<td>Available</td>
<td>Checking</td>
<td>The precheck is in progress</td>
</tr>
<tr>
<td>Precheck (failed)</td>
<td>Available</td>
<td>Available (Information icon)</td>
<td>The precheck failed but the patch is still available. The reason for the failure is included in the image update history.</td>
</tr>
<tr>
<td>Patching</td>
<td>Updating</td>
<td>Applying Update</td>
<td>The update is in progress. While a patch is being applied, the status of the patch displays as Applying Update and the DB system's status displays as Updating. Life cycle operations on the DB system and its resources might be temporarily unavailable. An entry is made in the update history log.</td>
</tr>
<tr>
<td>Patching (failed)</td>
<td>Available</td>
<td>Available (Information icon)</td>
<td>The update failed. The update information is available in the update history log. The system displays a message asking you to do a rollback before attempting another update.</td>
</tr>
<tr>
<td>Patching (success)</td>
<td>DB System up to date</td>
<td>Applied</td>
<td>The update is successful. The patch name is removed from the update list and an entry is made in the update history log.</td>
</tr>
</tbody>
</table>

**Updating an Exadata Cloud Service Instance**

This topic covers how to update the operating system and the tooling on the compute server nodes (for cloud VM clusters, these are called virtual machines) of an Exadata Cloud Service instance. Review all of the information carefully before you begin the updates.

**OS Updates**

You update the operating systems of Exadata compute nodes by using the `patchmgr` tool. This utility manages the entire update of one or more compute nodes remotely, including running pre-reboot, reboot, and post-reboot steps. You can run the utility from either an Exadata compute node or a non-Exadata server running Oracle Linux. The server on which you run the utility is known as the "driving system." You cannot use the driving system to update itself. Therefore, if the driving system is one of the Exadata compute nodes on a system you are updating, you must run a separate operation on a different driving system to update that server.

The following two scenarios describe typical ways of performing the updates:

**Scenario 1: Non-Exadata Driving System**

The simplest way to run the update the Exadata system is to use a separate Oracle Linux server to update all Exadata compute nodes in the system.

**Scenario 2: Exadata Node Driving System**

You can use one Exadata compute node to drive the updates for the rest of the compute nodes in the system, and then use one of the updated nodes to drive the update on the original Exadata driver node.

For example: You are updating a half rack Exadata system, which has four compute nodes - node1, node2, node3, and node4. First, use node1 to drive the updates of node2, node3, and node4. Then, use node2 to drive the update of node1.

The driving system requires root user **SSH** access to each compute node the utility will update.
Preparing for the OS Updates

**Caution:**

Do not install NetworkManager on the Exadata Cloud Service instance. Installing this package and rebooting the system results in severe loss of access to the system.

- Before you begin your updates, review *Exadata Cloud Service Software Versions* (Doc ID 2333222.1) to determine the latest software version and target version to use.
- Some steps in the update process require you to specify a YUM repository. The YUM repository URL is:


Region identifiers are text strings used to identify Oracle Cloud Infrastructure regions (for example, us-phoenix-1). You can find a complete list of region identifiers in Regions.

You can run the following `curl` command to determine the latest version of the YUM repository for your Exadata Cloud Service instance region:

```
```

This example returns the most current version of the YUM repository for the US West (Phoenix) region:

```
<a href="18.1.4.0.0/">18.1.4.0.0/</a> 01-Mar-2018 03:36 -
```

- To apply OS updates, the system's VCN must be configured to allow access to the YUM repository. For more information, see Option 2: Service Gateway Access to Both Object Storage and YUM Repos on page 1238.

To update the OS on all compute nodes of an Exadata Cloud Service instance

This example procedure assumes the following:

- The system has two compute nodes, node1 and node2.
- The target version is 18.1.4.0.0.180125.3.
- Each of the two nodes is used as the driving system for the update on the other one.

1. Gather the environment details.
   
   a. **SSH to node1 as root** and run the following command to determine the version of Exadata:

      ```
      [root@node1]# imageinfo -ver
      12.2.1.1.4.171128
      ```

   b. **Switch to the grid user, and identify all computes in the cluster.**

      ```
      [root@node1 .ssh]# su - grid
      [grid@node1]$ olsnodes
      node1
      node1
      ```

2. Configure the driving system.
   
   a. **Switch back to the root user on node1, check whether a root ssh key pair (id_rsa and id_rsa.pub) already exists. If not, then generate it.**

      ```
      [root@node1 .ssh]# ls /root/.ssh/id_rsa*
      ls: cannot access /root/.ssh/id_rsa*: No such file or directory
      [root@node1 .ssh]# ssh-keygen -t rsa
      ```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase): Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
root@node1.fraad1client.exadataclientne.oraclevcn.com
The key's randomart image is:

b. Distribute the public key to the target nodes, and verify this step. In this example, the only target node is node2.

```
[root@node1 .ssh]# scp -i ~opc/.ssh/id_rsa ~root/.ssh/id_rsa.pub
opc@node2:/tmp/id_rsa.node1.pub

[root@node2 ~]# ls -al /tmp/id_rsa.node1.pub
-rw-r--r-- 1 opc opc 442 Feb 28 03:33 /tmp/id_rsa.node1.pub

[root@node2 ~]# date
Wed Feb 28 03:33:45 UTC 2018
```
c. On the target node (node2, in this example), add the root public key of node1 to the root authorized_keys file.

```
[root@node2 ~]# cat /tmp/id_rsa.node1.pub >> ~root/.ssh/authorized_keys
```
d. Download dbserver.patch.zip as p21634633_12*_Linux-x86-64.zip onto the driving system (node1, in this example), and unzip it. See dbnodeupdate.sh and dbserver.patch.zip: Updating Exadata Database Server Software using the DBNodeUpdate Utility and patchmgr (Doc ID 1553103.1) for information about the files in this .zip.

```
[root@node1 patch]# mkdir /root/patch
[root@node1 patch]# cd /root/patch
[root@node1 patch]# unzip p21634633_181400_Linux-x86-64.zip
Archive:  p21634633_181400_Linux-x86-64.zip  creating: dbserver_patch_5.180228.2/
creating: dbserver_patch_5.180228.2/ibdiagtools/
inflating: dbserver_patch_5.180228.2/ibdiagtools/cable_check.pl
inflating: dbserver_patch_5.180228.2/ibdiagtools/setup-ssh
inflating: dbserver_patch_5.180228.2/ibdiagtools/VERSION_FILE
extracting: dbserver_patch_5.180228.2/ibdiagtools/xmonib.sh
inflating: dbserver_patch_5.180228.2/ibdiagtools/monitor
inflating: dbserver_patch_5.180228.2/ibdiagtools/checkbadlinks.pl
creating: dbserver_patch_5.180228.2/ibdiagtools/topologies/
inflating: dbserver_patch_5.180228.2/ibdiagtools/topologies/VerifyTopologyUtility.pm
inflating: dbserver_patch_5.180228.2/ibdiagtools/topologies/verifiylib.pm
inflating: dbserver_patch_5.180228.2/ibdiagtools/topologies/Node.pm
inflating: dbserver_patch_5.180228.2/ibdiagtools/topologies/Rack.pm
```
e. Create the `dbs_group` file that contains the list of compute nodes to update. Include the nodes listed after running the `olsnodes` command in step 1 except for the driving system node. In this example, `dbs_group` should include only `node2`.

```
[root@node1 patch]# cd /root/patch/dbserver_patch_5.180228
```
3. Run a patching precheck operation.

```
patchmgr -dbnodes dbs_group -precheck -yum_repo <yum_repository> -target_version <target_version> -nomodify_at_prereq
```

**Important:**

You must run the precheck operation with the `-nomodify_at_prereq` option to prevent any changes to the system that could impact the backup you take in the next step. Otherwise, the backup might not be able to roll back the system to its original state, should that be necessary.

The output should look like the following example:

```
[root@node1 dbserver_patch_5.180228]# ./patchmgr -dbnodes
dbs_group -precheck -yum_repo http://yum-phx.oracle.com/repo/
EngineeredSystems/exadata/dbserver/18.1.4.0.0/base/x86_64 -target_version
18.1.4.0.0.180125.3 -nomodify_at_prereq
************************************************************************************************************
NOTE  patchmgr release: 5.180228 (always check MOS 1553103.1 for the
latest release of dbserver.patch.zip)
NOTE
WARNING Do not interrupt the patchmgr session.
WARNING Do not resize the screen. It may disturb the screen layout.
WARNING Do not reboot database nodes during update or rollback.
WARNING Do not open logfiles in write mode and do not try to alter them.
************************************************************************************************************
node(s)
2018-02-28 21:24:57 +0000        :Working: DO: Check free space and verify
SSH equivalence for the root user to node2
2018-02-28 21:26:15 +0000        :SUCCESS: DONE: Check free space and
verify SSH equivalence for the root user to node2
precheck on node(s).
node(s).
```

4. Back up the current system.

```
patchmgr -dbnodes dbs_group -backup -yum_repo <yum_repository> -target_version <target_version> -allow_active_network_mounts
```

**Important:**

This is the proper stage to take the backup, before any modifications are made to the system.

The output should look like the following example:

```
[root@node1 dbserver_patch_5.180228]# ./patchmgr -dbnodes
dbs_group -backup -yum_repo http://yum-phx.oracle.com/repo/
EngineeredSystems/exadata/dbserver/18.1.4.0.0/base/x86_64 -target_version
18.1.4.0.0.180125.3 -allow_active_network_mounts
************************************************************************************************************
NOTE  patchmgr release: 5.180228 (always check MOS 1553103.1 for the
latest release of dbserver.patch.zip)
NOTE
### Database

**WARNING** Do not interrupt the patchmgr session.

**WARNING** Do not resize the screen. It may disturb the screen layout.

**WARNING** Do not reboot database nodes during update or rollback.

**WARNING** Do not open logfiles in write mode and do not try to alter them.

---

<table>
<thead>
<tr>
<th>Date</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-02-28</td>
<td>Working: DO: Initiate backup on 1 node(s).</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>Working: DO: Initiate backup on node(s)</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>Working: DO: Check free space and verify SSH equivalence for the root user to node2</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>SUCCESS: DONE: Check free space and verify SSH equivalence for the root user to node2</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>Working: DO: dbnodeupdate.sh running a backup on node(s).</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>SUCCESS: DONE: Initiate backup on node(s).</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>SUCCESS: DONE: Initiate backup on 1 node(s).</td>
<td></td>
</tr>
</tbody>
</table>

---

5. Remove all custom RPMs from the target compute nodes that will be updated. Custom RPMs are reported in precheck results. They include RPMs that were manually installed after the system was provisioned.

**Note:**
- If you are updating the system from version 12.1.2.3.4.170111, and the precheck results include krb5-workstation-1.10.3-57.el6.x86_64, remove it. (This item is considered a custom RPM for this version.)
- **Do not** remove exadata-sun-vm-computenode-exact or oracle-ofed-release-guest. These two RPMs are handled automatically during the update process.

6. Run the `nohup` command to perform the update.

```
nohup patchmgr -dbnodes dbs_group -upgrade -nobackup -
yum_repo <yum_repository> -target_version <target_version> -
allow_active_network_mounts &
```

The output should look like the following example:

```
[root@node1 dbserver_patch_5.180228]# nohup ./patchmgr -dbnodes
dbs_group -upgrade -nobackup -
yum_repo http://yum-phx.oracle.com/repo/EngineeredSystems/exadata/dbserver/18.1.4.0.0.180125.3 -target_version
18.1.4.0.0.180125.3 -allow_active_network_mounts &
```

**NOTE** patchmgr release: 5.180228 (always check MOS 1553103.1 for the latest release of dbserver.patch.zip)

**NOTE** Database nodes will reboot during the update process.

**WARNING** Do not interrupt the patchmgr session.

**WARNING** Do not resize the screen. It may disturb the screen layout.

**WARNING** Do not reboot database nodes during update or rollback.

**WARNING** Do not open logfiles in write mode and do not try to alter them.

---

<table>
<thead>
<tr>
<th>Date</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-02-28</td>
<td>Working: DO: Initiate prepare steps on node(s).</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>Working: DO: Check free space and verify SSH equivalence for the root user to node2</td>
<td></td>
</tr>
<tr>
<td>2018-02-28</td>
<td>SUCCESS: DONE: Check free space and verify SSH equivalence for the root user to node2</td>
<td></td>
</tr>
</tbody>
</table>
7. After the update operation completes, verify the version of the kernel on the compute node that was updated.

   [root@node2 ~]# imageinfo -ver
   18.1.4.0.0.180125.3

8. If the driving system is a compute node that needs to be updated (as in this example), repeat steps 2 through 7 of this procedure using an updated compute node as the driving system to update the remaining compute node. In this example update, you would use `node2` to update `node1`.

9. On each compute node, run the `uptrack-install` command as root to install the available ksplice updates.

   uptrack-install --all --y

**Updating Tooling on an Exadata Cloud Service Instance**

You can update the cloud-specific tooling included on an Exadata Cloud Service compute node by downloading and applying an RPM file containing the latest version of the tools.

**Note:**

Oracle highly recommends that you maintain the same version of cloud tooling across your Exadata Cloud Service environment. Perform the following procedure on every compute node in the Exadata Cloud Service instance.

**Prerequisite**

The compute nodes in the Exadata Cloud Service instance must be configured to access the Oracle Cloud Infrastructure Object Storage service. For more information, see [Node Access to Object Storage: Static Route](#) on page 1236.

**Updating the Cloud Tooling on Each Compute Node Manually**

The method for updating the tooling depends on the tooling release that is currently installed on the compute node.
To check the installed tooling release

1. Connect to the compute node as the opc user.
2. Start a root-user command shell.
   
   ```
   $ sudo -s
   #
   ```
3. Use the following command to display information about the installed cloud tooling and note the release label, shown in red in the example that follows.
   
   ```
   # rpm -qa|grep -i dbaastools_exa
   dbaastools_exa-1.0-1+18.1.2.1.0_180511.0801.x86_64
   ```

   In this example, the release version is 18.1.2.1.0_180511.0801.

To update the tooling if the release label is higher than 17430

You use the `patch tools` subcommand of the `dbaascli` utility to update the cloud tooling.

**Important:**

If you are updating the tooling on an Exadata Cloud Service instance that includes a Data Guard configuration, you must perform these steps on both the primary database's system and on the standby database's system.

1. Connect as the opc user to the compute node.
2. Start a root-user command shell:
   
   ```
   $ sudo -s
   #
   ```
3. Check whether any cloud tooling updates are available:
   
   ```
   # dbaascli patch tools list
   ```

   Example output:

   ```
   [root@exacs-node1 ]# dbaascli patch tools list
   DBAAS CLI version 19.4.1.0.0
   Executing command patch tools list
   Checking tools on all nodes
   Current Patchid on stb-elbdc1: 19.4.1.0.0_190822.1034
   Available Patches
   Patchid : 19.4.1.0.0_190827.1034
   Patchid : 19.4.1.0.0_190912.0440 (LATEST)
   Install tools patch using
dbaascli patch tools apply --patchid 19.4.1.0.0_190912.0440 or
dbaascli patch tools apply --patchid LATEST
   All Nodes have the same tools version
   ```
4. In the command response, locate the patch ID of the cloud tooling update. The patch ID is listed as the "Patchid" value. If multiple patches are listed, choose the latest one.
5. Apply the patch containing the latest cloud tooling update by using one of the following methods:
   - Specify the patch ID of the latest patch:
     ```
     # dbaascli patch tools apply --patchid <patch_ID>
     ```
   - Specify the patch ID as LATEST:
     ```
     # dbaascli patch tools apply --patchid LATEST
     ```
   - Run the update process in the background:
     ```
     # dbaascli patch tools apply --patchid LATEST &
     ```

6. Reset the backup configuration:
   ```
   # /var/opt/oracle/ocde/assistants/bkup/bkup
   ```

7. Exit the root-user command shell and disconnect from the compute node:
   ```
   # exit
   $ exit
   ```

8. If you are updating cloud tooling on a DB system hosting a Data Guard configuration, repeat the preceding steps on the compute node of the peer (primary or standby database's) Exadata Cloud Service instance.

   **To update the tooling if the release label is 17430 or lower**

   1. Download the RPM file using the Swift object storage API endpoint URL for your region.
      ```
      wget <swift_API_endpoint>/v1/exadata/patches/dbaas_patch/shome/dbaastools_exa.rpm
      ```
      The following example downloads the RPM file from the US West (Phoenix).
      ```
      wget https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/exadata/patches/dbaas_patch/shome/dbaastools_exa.rpm
      ```
      See [API Reference and Endpoints](#) for the Swift API endpoint for your region.

   2. Apply the RPM file.
      ```
      # rpm -ev dbaastools_exa
      # rpm -ivh dbaastools_exa.rpm
      ```

   3. Repeat the previous steps on each compute node in the Exadata Cloud Service instance.

   **Configuring Automatic Cloud Tooling Updates**

   You can configure automatic cloud tooling updates for Exadata Cloud Service instance. When you configure these updates, an entry is added to the `/etc/crontab` file to regularly check for cloud tooling updates and apply new updates to the compute node when they become available.

   **Note:**
   These procedures apply only if the release label is higher than 17430.

   **To disable automatic cloud tooling updates for an Exadata Cloud Service instance**

   1. Connect to the compute node as the opc user.
   2. Start a root-user command shell:
      ```
      $ sudo -s
      ```
3. Use the following command to disable automatic tooling updates:

```
# dbaascli patch tools auto disable
```

4. Exit the root-user command shell and disconnect from the compute node:

```
# exit
$ exit
```

5. If you are disabling automatic cloud tooling updates on an Exadata Cloud Service instance hosting a Data Guard configuration, repeat the preceding steps on the compute node of the peer (primary or standby database's) system.

**To integrate customer-managed key management into Exadata Cloud Service**

If you choose to encrypt databases in an Exadata Cloud Service instance using encryption keys that you manage, then you may update the following two packages (using Red Hat Package Manager) to enable DBAASTOOLS to interact with the APIs that customer-managed key management uses.

**KMS TDE CLI**

To update the KMS TDE CLI package, you must complete the following task on all nodes in the Exadata Cloud Service instance:

1. Deinstall current KMS TDE CLI package, as follows:

```
rpm -ev kmstdecli
```

2. Install the updated KMS TDE CLI package, as follows:

```
rpm -ivh kms_tde_cli
```

**LIBKMS**

LIBKMS is a library package necessary to synchronize a database with customer-managed key management through PKCS11. When a new version of LIBKMS is installed, any databases converted to customer-managed key management continue to use the previous LIBKMS version, until the database is stopped and restarted.

To update the LIBKMS package, you must complete the following task on all nodes in the Exadata Cloud Service instance:

1. Confirm that the LIBKMS package is already installed, as follows:

```
rpm -qa --last | grep libkmstdepkcs11
```

2. Install a new version of LIBKMS, as follows:

```
rpm -ivh libkms
```

3. Use SQL*Plus to stop and restart all databases converted to customer-managed key management, as follows:

```
shutdown immediate;
startup;
```

4. Ensure that all converted databases are using the new LIBKMS version, as follows:

```
for pid in $(ps aux | grep "<dbname>" | awk '{print $2;}'); do echo $pid;
    sudo lsof -p $pid | grep kms | grep "pkcs11_[0-9A-Za-z.]*" | sort -u;
done | grep pkcs11
```

5. Deinstall LIBKMS packages that are no longer being used by any database, as follows:

```
rpm -ev libkms
```
Patching an Exadata Cloud Service Instance

This topic explains how to perform patching operations on Exadata Cloud Service resources by using the Console, API, or the CLI.

Tip:
Oracle recommends patching databases by moving them to a Database Home that uses the target patching level. See To patch a database by moving it to another Database Home on page 1287 for instructions on this method of database patching.

For information and instructions on patching the system by using the dbaascli utility, see Patching an Exadata Cloud Service Instance Manually on page 1289.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

About Patching Exadata Cloud Service Resources
Patching an Exadata Cloud Service instance updates the components on all the compute nodes in the instance. A VM cluster or DB system patch updates the Oracle Grid Infrastructure (GI) on the resource.

Note:
The cloud Exadata resource model the instance is using determines whether you patch the Grid Infrastructure on a DB system resource or a cloud VM cluster resource. VM clusters are used by the new resource model. DB systems can be easily migrated to the new resource model with no system downtime.

A Database Home patch updates the Oracle Database software shared by the databases in that home. Thus, you patch a database by either moving it to a Database Home that has the correct patch version or you patch the Database Home the database is currently in.

Consider the following best practices:
• Back up your databases before you apply any patches. For information about backing up the databases, see Managing Exadata Database Backups on page 1320.
• Patch a VM cluster or an Exadata DB system before you patch the Databases Homes and databases on that resource.
• Before you apply any patch, run the precheck operation to ensure your VM cluster, Exadata DB system, or Database Home meets the requirements for that patch.
• To patch a database to a version other than the database version of the current home, move the database to a Database Home running the target version. This technique requires less downtime and allows you to easily roll back the database to the previous version by moving it back to the old Database Home. See To patch a database by moving it to another Database Home on page 1287.
• For the Oracle Database and Oracle Grid Infrastructure major version releases available in Oracle Cloud Infrastructure, patches are provided for the current version plus the two most recent older versions (\(N\) through \(N\) - 2). For example, if an instance is using Oracle Database 19c, and the latest version of 19c offered is 19.8.0.0.0, patches are available for versions 19.8.0.0.0, 19.7.0.0 and 19.6.0.0.
Prerequisites

The Exadata Cloud Service instance requires access to the Oracle Cloud Infrastructure Object Storage service, including connectivity to the applicable Swift endpoint for Object Storage. Oracle recommends using a service gateway with the VCN to enable this access. For more information, see these topics:

- Network Setup for Exadata Cloud Service Instances on page 1232: For information about setting up your VCN for the Exadata Cloud Service instance, including the service gateway.
- Object Storage FAQ: For information about the Swift endpoints to use.

Important:

In addition to the prerequisites listed, ensure that the following conditions are met to avoid patching failures:

- The /u01 directory on the database host file system has at least 15 GB of free space for the execution of patching processes.
- The Oracle Clusterware is up and running on the Exadata Cloud Service instance.
- All nodes of the instance are up and running.

Using the Console

You can use the Console to view the history of patch operations on Exadata Cloud Service instances, apply patches, and monitor the status of patch operations.

Patching Exadata Instances That Use the DB System Resource Model

The tasks in this section describe how to apply patches and monitor the status of patch operations on Exadata DB systems and their Database Homes.

To patch the Oracle Grid Infrastructure on an Exadata DB system

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. In the list of DB systems, click the name of the Exadata DB system you want to patch to display the DB system details.
4. Under DB System Version, click the View link beside the Latest Patch Available field.
5. Review the list of available patches for the DB system.
6. Click the Actions icon (three dots) for the patch you are interested in, and then click one of the following actions:
   - Run Precheck: Check for any prerequisites to make sure that the patch can be successfully applied.
   - Apply: Applies the selected patch. Oracle highly recommends that you run the precheck operation for a patch before you apply it.
7. Confirm when prompted.

The patch list displays the status of the operation. While a patch is being applied, the patch's status displays as Patching and the DB system's status displays as Updating. Lifecycle operations on the DB system and its resources might be temporarily unavailable. If patching completes successfully, the patch's status changes to Applied and the status of the DB system changes to Available. You can view more details about an individual patch operation by clicking Patch History.

To patch the Oracle Database software in a Database Home (DB system)

Note:

This patching procedure updates the Oracle Database software for all databases located in the Database Home. To patch an individual database, you can move it to another Database Home that uses the desired Oracle Database software configuration.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. In the list of DB systems, click the name of the Exadata DB system with the Database Home you want to patch to display the DB system details.

4. Under Resources, click Database Homes.

5. Click the name of the Database Home you want to patch to display the Database Home details.


7. Review the list of available patches for the Database Home.

8. Click the Actions icon (three dots) for the patch you are interested in, and then click one of the following actions:
   - **Precheck**: Check for any prerequisites to make sure that the patch can be successfully applied.
   - **Apply**: Applies the selected patch. Oracle highly recommends that you run the precheck operation for a patch before you apply it.

9. Confirm when prompted.

   The patch list displays the status of the operation. While a patch is being applied, the status of the patch displays as **Patching** and the status of the Database Home and the databases in it display as **Updating**. During the operation, each database in the home is stopped and then restarted. If patching completes successfully, the patch's status changes to **Applied** and the Database Home's status changes to **Available**. You can view more details about an individual patch operation by clicking **Patch History**.

   **Patching Exadata Instances That use the New Resource Model**

   The tasks in this section describe how to apply patches and monitor the status of patch operations on cloud VM clusters and their Database Homes.

   **To patch the Oracle Grid Infrastructure on an Exadata cloud VM cluster**

   1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
   2. Choose your **Compartment**.
   3. Click **Exadata VM Clusters**.
   4. In the list of cloud VM clusters, click the name of the cluster you want to patch to display the cluster details.
   5. Under **Version**, click the **View Patches** link beside the **Updates Available** field.
   6. Review the list of available patches for the cloud VM cluster.
   7. Click the Actions icon (three dots) for the patch you are interested in, and then click one of the following actions:
      - **Run Precheck**: Check for any prerequisites to make sure that the patch can be successfully applied.
      - **Update Grid Infrastructure**: Applies the selected patch. Oracle highly recommends that you run the precheck operation for a patch before you apply it.
   8. Confirm when prompted.

      The patch list displays the status of the operation. While a patch is being applied, the patch's status displays as **Patching** and the cloud VM cluster's status displays as **Updating**. Lifecycle operations on the cluster and its resources might be temporarily unavailable. If patching completes successfully, the patch's status changes to **Applied** and the status of the cluster changes to **Available**. You can view more details about an individual patch operation by clicking **Update History**.

   **To patch the Oracle Database software in a Database Home (cloud VM cluster)**

   **Note:**

   This patching procedure updates the Oracle Database software for all databases located in the Database Home. To patch an individual database, you can move it to another Database Home that uses the desired Oracle Database software configuration.

   1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
   2. Choose your **Compartment**.
   3. Click **Exadata VM Clusters**.
   4. In the list of cloud VM clusters, click the name of the cluster you want to patch to display the cluster details.
   5. Under **Resources**, click **Database Homes**.
6. Click the name of the Database Home you want to patch to display the Database Home details.
7. Under **Latest Patch Available**, click **View**.
8. Review the list of available patches for the Database Home.
9. Click the Actions icon (three dots) for the patch you are interested in, and then click one of the following actions:
   - **Precheck**: Check for any prerequisites to make sure that the patch can be successfully applied.
   - **Apply**: Applies the selected patch. Oracle highly recommends that you run the precheck operation for a patch before you apply it.
10. Confirm when prompted.

The patch list displays the status of the operation. While a patch is being applied, the status of the patch displays as **Patching** and the status of the Database Home and the databases in it display as **Updating**. During the operation, each database in the home is stopped and then restarted. If patching completes successfully, the patch’s status changes to **Applied** and the Database Home's status changes to **Available**. You can view more details about an individual patch operation by clicking **Update History**.

**Patching Individual Oracle Databases in an Exadata Cloud Service Instance**

This task explains how to patch a single Oracle Database in your Exadata Cloud Service instance by moving it to another Database Home. For information on patching Database Homes, see To patch the Oracle Database software in a Database Home (cloud VM cluster) on page 1286 and To patch the Oracle Database software in a Database Home (DB system) on page 1285.

To patch a database by moving it to another Database Home

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the cloud VM cluster or DB system that contains the database you want to move.
   - **Cloud VM clusters (new resource model)**: Under Exadata at Oracle Cloud, click **Exadata VM Clusters**. In the list of VM clusters, click the name of the VM cluster that contains the database you want to move.
   - **DB systems**: Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, click the name of the DB system that contains the database you want to move.
4. In the list of databases on the details page of the VM cluster or DB system, click the name of the database you want to move to view the Database Details page.
5. Click **Move to Another Home**.
6. Select the target Database Home.
7. Click **Move Database**.
8. Confirm the move operation.

The database will be stopped in the current home and then restarted in the destination home. While the database is being moved, the Database Home status displays as **Moving Database**. When the operation completes, Database Home is updated with the current home. If the operation is unsuccessful, the status of the database displays as **Failed**, and the Database Home field provides information about the reason for the failure.

**Viewing Patch History**

Each patch history entry represents an attempted patch operation and indicates whether the operation was successful or failed. You can retry a failed patch operation. Repeating an operation results in a new patch history entry.

Patch history views in the Console do not show patches that were applied by using command line tools such as **dbaascli**.

If your service instance uses the **new resource model**, the patch history available by navigating to the VM Cluster Details page. If your service instance uses the DB system resource model, the patch history is available by navigating to the DB System Details page.

To view the patch history of a cloud VM cluster

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Click **Exadata VM Clusters**.
4. In the list of cloud VM clusters, click the name of the cluster you want to patch to display the cluster details.
5. Under **Version**, click the **View Patches** link beside the **Updates Available** field.
6. Click **Update History**.

   The Update History page displays the history of patch operations for that cloud VM cluster and for the Database Homes on that cloud VM cluster.

To view the patch history of a DB system

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. In the list of DB systems, click the name of the Exadata DB system with the information you want to view to display the DB system details.
4. Under **DB System Version**, click the **View** beside the **Latest Patch Available** field.
5. Click **Patch History**.

   The Patch History page displays the history of patch operations for that DB system and for the Database Homes on that DB system.

To view the patch history of a Database Home

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the cloud VM cluster or DB system that contains the Database Home.

   * **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   * **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. Under **Resources**, click **Database Homes**.
5. Click the name of the Database Home you want to view to display the Database Home details.
7. Click **Patch History** (DB systems) or **Update History** (cloud VM clusters).

   The history page displays the history of patch operations for that Database Home and for the cloud VM cluster or DB system to which it belongs.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage patching the following Exadata resources: cloud VM clusters, DB systems, databases, and Database Homes.

**Cloud VM clusters (for systems using the new resource model):**

- ListCloudVmClusterUpdates
- ListCloudVmClusterUpdateHistoryEntries
- GetCloudVmClusterUpdate
- GetCloudVmClusterUpdateHistoryEntry
- UpdateVmCluster

**DB systems:**

- ListDbSystemPatches
- ListDbSystemPatchHistoryEntries
- GetDbSystemPatch
- GetDbSystemPatchHistoryEntry
- **UpdateDbSystem**

**Databases:**
- **UpdateDatabase** - Use this operation to patch a database by moving it to another Database Home

**Database Homes:**
- **ListDbHomePatches**
- **ListDbHomePatchHistoryEntries**
- **GetDbHomePatch**
- **GetDbHomePatchHistoryEntry**
- **UpdateDbHome**

For the complete list of APIs for the Database service, see Database Service API.

### Patching an Exadata Cloud Service Instance Manually

This topic explains how to use the `dbaascli` utility to perform patching operations for Oracle Grid Infrastructure and Oracle Database on an Exadata Cloud Service instance. The utility requires root or sudo administration privileges.

**Note:**
You must update the cloud specific tooling on all the compute nodes in your Exadata Cloud Service instance before performing the following procedures. For more information, see Updating an Exadata Cloud Service Instance on page 1274.

**Prerequisites**

Patches are stored in Oracle Cloud Infrastructure Object Storage, so the Exadata Cloud Service instance requires access to that service. To enable this access, Oracle recommends using a service gateway with the VCN. For more information, see Network Setup for Exadata Cloud Service Instances on page 1232. In that topic, pay particular attention to:

- **Service Gateway for the VCN** on page 1237
- **Node Access to Object Storage: Static Route** on page 1236
- **Backup egress rule: Allows access to Object Storage** on page 1242

**Managing Patches**

To list available patches

You can produce a list of available patches using the `cswlib list` subcommand of the `dbaascli` utility:

- Connect to the compute node as the `opc` user.

For detailed instructions, see Connecting to an Exadata Cloud Service Instance on page 1269.

- Start a root-user command shell:

```bash
$ sudo -s
#
```

- Execute the following command:

```bash
# cswlib list
```

**Example:**

```bash
# dbaascli cswlib list
DBAAS CLI version 20.1.3.3.0
Executing command cswlib list
```
INFO : Log file => /var/opt/oracle/log/list/
list_2020-11-17_18:14:53.802476231267.log
INFO : dbimage fixup executed.

############ List of Available BP ############
-APR2020 (For DB Versions 18000 12201 12102 11204 19000)
-JUL2020 (For DB Versions 18000 12201 12102 11204 19000)
-OCT2020 (For DB Versions 18000 12201 12102 11204 19000)

############ List of Available NONCDB BP #######
-APR2020 (For DB Versions 12102 19000)
-JUL2020 (For DB Versions 12102 19000)
-OCT2020 (For DB Versions 12102 19000)

- Exit the root-user command shell.

# exit
$

To check prerequisites before applying a patch

You can perform the prerequisites-checking operation using the patch db prereq subcommand of the dbaascli utility:

1. Connect to the compute node as the opc user.
2. Start a root-user command shell:

   $ sudo -s
   #

3. Execute the following command:

   # dbaascli dbhome patch --oracleHome <dbhome_path> --targetVersion <Oracle_Database_version> --executePrereqs

where:

• --oracleHome identifies the path of the Database Home to be prechecked.
• --targetVersion specifies the target Oracle Database version to precheck.

Example:

# dbaascli dbhome patch --oracleHome /u02/app/oracle/product/19.0.0.0/dbhome_2 --targetVersion 19.9.0.0 --executePrereqs
DBAAS CLI version 20.1.3.3.0
Executing command dbhome patch --oracleHome /u02/app/oracle/product/19.0.0.0/dbhome_2 --targetVersion 19.9.0.0 --executePrereqs
-----------------
Setting up parameters...
Patch Parameters setup successful.
-----------------
Validating Inputs.
Successfully Validated Inputs.
-----------------
Downloading DB Gold Image. This may take a while...
INFO : dbimage fixup executed.
Successfully downloaded gold image.
-----------------
Loading PILOT...
Session ID of the current execution is: 2
Log file location: /var/opt/oracle/log/dbHomePatch/pilot_2020-11-13_03-49-29-PM
To learn more about the `dbhome patch` subcommand, including available options, execute the following command:

```
# dbaascli dbhome patch ?
```

4. Exit the root-user command shell:

```
# exit
$ 
```

**To apply a patch to a database**

You can apply a patch by using the `dbhome patch` subcommand of the `dbaascli` utility.

The patching operation:

- Can be used to patch some or all of your compute nodes using one command.
- Coordinates multi-node patching in a rolling manner.
- Can execute patch-related SQL after patching all the compute nodes in the cluster.
- Can patch an empty Database Home, or a Database Home containing one or more databases.
Oracle recommends patching an empty Database Home and then moving databases into the home using the `dbaascli db move` command.

To patch a Database Home (dbhome):

1. Connect to the compute node as the `opc` user.
2. Start a root-user command shell:
   
   ```
   $ sudo -s
   #
   ```
3. Execute the following command:

   ```
   # dbaascli dbhome patch --oracleHome <dbhome_path> --targetVersion <Oracle_Database_version>
   ```

   where:
   - `--oracleHome` identifies the path of the Database Home to be patched.
   - `--targetVersion` specifies the target Oracle Database version to use for patching.
   - `--run_datasql 1` instructs the command to execute patch-related SQL commands.

   **Note:**
   - Patch-related SQL should only be executed after all of the compute nodes are patched. Therefore, take care not to specify this argument if you are patching a subset of nodes and further nodes remain to be patched.
   - This argument can only be specified in conjunction with a patching operation on a set of compute nodes. Therefore, if you have patched all of your nodes and you did not specify this argument, you will need to manually execute the SQL commands associated with the patch. Refer to the patch documentation for further details.

**Example:**

```bash
Example (Oracle Database):
# dbaascli dbhome patch --oracleHome /u02/app/oracle/product/19.0.0.0/dbhome_2 --targetVersion 19.9.0.0
DBAAS CLI version 20.1.3.3.0
Executing command dbhome patch --oracleHome /u02/app/oracle/product/19.0.0.0/dbhome_2 --targetVersion 19.9.0.0
----------------- Setting up parameters... Patch Parameters setup successful.
----------------- Validating Inputs. Successfully Validated Inputs.
----------------- Downloading DB Gold Image. This may take a while... INFO : dbimage fixup executed.
Successfully downloaded gold image.
----------------- Loading PILOT... Session ID of the current execution is: 4 Log file location: /var/opt/oracle/log/dbHomePatch/pilot_2020-11-13_04-49-49-PM
----------------- Running initialization job Completed initialization job
```
Running validate_nodes job
Completed validate_nodes job

Running validate_oracle_home job
Completed validate_oracle_home job

Running validate_source_version job
Completed validate_source_version job

Running validate_diag_perm job
Completed validate_diag_perm job

Running validate_backup_loc job
Completed validate_backup_loc job

Running validate_gold_image_url job
Completed validate_gold_image_url job

Running validate_disk_space job
Completed validate_disk_space job

Running download_gold_image job

Running validate_gold_image job
Completed validate_gold_image job

Running validate_patch_across_nodes job
Completed validate_patch_across_nodes job

Running run_installer_prereqs job
Completed run_installer_prereqs job

Running check_patch_conflict job
Completed check_patch_conflict job

Running acquire_lock job
Completed acquire_lock job

Running copy_image-ssexan-42hss1 job
Completed copy_image-ssexan-42hss1 job

Running detach_home-ssexan-42hss1 job
Completed detach_home-ssexan-42hss1 job

Running move_home-ssexan-42hss1 job
Completed move_home-ssexan-42hss1 job

Running move_image_to_home_loc-ssexan-42hss1 job
Completed move_image_to_home_loc-ssexan-42hss1 job

Running setup_db_home-ssexan-42hss1 job
Completed setup_db_home-ssexan-42hss1 job

Running root_script_execution-ssexan-42hss1 job
Completed root_script_execution-ssexan-42hss1 job

Running copy_home_to_backup_loc-ssexan-42hss1 job
Completed copy_home_to_backup_loc-ssexan-42hss1 job

Running copy_config_files-ssexan-42hss1 job
Completed copy_config_files-ssexan-42hss1 job

Running copy_image-ssexan-42hss2 job
To learn more about the dbhome patch subcommand, including available options, execute the following command:

```
# dbaascli dbhome patch ?
```

4. Exit the root-user command shell:

```
# exit
$
```

To apply a patch to the Oracle Grid Infrastructure

You can apply a patch to your Oracle Grid Infrastructure by using the patch db apply subcommand of the dbaascli utility.

To perform the patching operation:

1. Connect to the compute node as the opc user.
2. Start a root-user command shell:

```
$ sudo -s
  #
```

DBHome Patching Successful.

To apply a patch to the Oracle Grid Infrastructure

You can apply a patch to your Oracle Grid Infrastructure by using the patch db apply subcommand of the dbaascli utility.

To perform the patching operation:

1. Connect to the compute node as the opc user.
2. Start a root-user command shell:

```
$ sudo -s
  #
```

DBHome Patching Successful.

To apply a patch to the Oracle Grid Infrastructure

You can apply a patch to your Oracle Grid Infrastructure by using the patch db apply subcommand of the dbaascli utility.

To perform the patching operation:

1. Connect to the compute node as the opc user.
2. Start a root-user command shell:

```
$ sudo -s
  #
```

DBHome Patching Successful.
3. Execute the following command:

```
# dbaascli patch db apply --patchid <patchid> --dbnames grid
```

where:
- `--patchid` identifies the patch to be applied.
- `--dbnames` specifies "grid" to indicate that the Grid Infrastructure is to be patched.

Example:

```
# dbaascli patch db apply --patchid 29708703-GI --dbnames grid
```

To learn more about the `patch db apply` subcommand, including available options, execute the following command:

```
# dbaascli patch db apply ?
```

4. Exit the root-user command shell:

```
# exit
```

To list applied patches
You can produce a list of applied patches to determine which patches have been applied.

You can use the opatch utility to determine the patches that have been applied to an Oracle Database or Grid Infrastructure installation.

To produce a list of applied patches for an Oracle Database installation:

1. Connect to a compute node as the oracle user.
2. Go to the Oracle user's home directory:

```
$ cd
```

3. Ensure that you are in the Oracle user's home directory:

```
$ pwd
/home/oracle
```

4. Source the environment file.

Example (using the environment file for a database named "DB18"):

```
$ . DB18.env
```

5. Execute the opatch command with the `lspatches` option:

```
$ opatch lspatches
```

To produce a list of applied patches for Oracle Grid Infrastructure:

1. Connect to a compute node as the opc user.
2. Become the grid user:

```
$ sudo -s
# su - grid
```
3. Execute the opatch command with the lspatches option:

```shell
$ opatch lspatches
```

To roll back or resume a patching operation

You can roll back a patch by using the dbaascli utility's `dbaascli dbhome patch --rollback` operation. This operation:

- Can be used to roll back a patch on some or all of your compute nodes using one command.
- Coordinates multi-node operations in a rolling manner.
- Can execute rollback-related SQL after rolling back the patch on all the compute nodes in the cluster.

You can resume a patching operation by using the `dbaascli dbhome patch --resume` operation.

To perform a patch roll back operation:

1. Connect to the compute node as the `opc` user.
2. Start a root-user command shell:

```shell
$ sudo -s
#
```
3. Execute the following command:

```shell
dbaascli dbhome patch --oracleHome <dbhome_path> --targetVersion <Oracle_Database_version> --rollBack
```

where:

- `--oracleHome` identifies the path of the Database Home to be patched.
- `--targetVersion` specifies the target Oracle Database version to use for patching.
- `--instanceN` specifies a compute node and one or more Oracle home directories that are subject to the rollback operation. In this context, an Oracle home directory may be an Oracle Database home directory or the Oracle Grid Infrastructure home directory.
- `--dbnames` specifies the name of the database you want to apply the switchback operation to.

Example:

```shell
# dbaascli dbhome patch --oracleHome /u02/app/oracle/product/19.0.0.0/dbhome_2 --targetVersion 19.7.0.0 --rollBack
```

```shell
DBAAS CLI version 20.1.3.3.0
Executing command dbhome patch --oracleHome /u02/app/oracle/product/19.0.0.0/dbhome_2 --targetVersion 19.7.0.0 --rollBack
-----------------
Setting up parameters...
Patch Parameters setup successful.
-----------------
Validating Inputs.
Successfully Validated Inputs.
-----------------
```
Loading PILOT...

Session ID of the current execution is: 5

Log file location: /var/opt/oracle/log/dbHomePatch/pilot_2020-11-13_05-14-30-PM

Running initialization job
Completed initialization job

Running validate_nodes job
Completed validate_nodes job

Running validate_oracle_home job
Completed validate_oracle_home job

Running validate_diag_perm job
Completed validate_diag_perm job

Running validate_backup_loc job
Completed validate_backup_loc job

Running validate_gold_image_url job
Completed validate_gold_image_url job

Running validate_disk_space job
Completed validate_disk_space job

Running download_gold_image job

Running validate_gold_image job
Completed validate_gold_image job

Running validate_patch_across_nodes job
Completed validate_patch_across_nodes job
Running run_installer_prereqs job
Completed run_installer_prereqs job

-----------------
Running acquire_lock job
Completed acquire_lock job

-----------------
Running copy_image-ssexan-42hss1 job
Completed copy_image-ssexan-42hss1 job

-----------------
Running detach_home-ssexan-42hss1 job
Completed detach_home-ssexan-42hss1 job

-----------------
Running move_home-ssexan-42hss1 job
Completed move_home-ssexan-42hss1 job

-----------------
Running move_image_to_home_loc-ssexan-42hss1 job
Completed move_image_to_home_loc-ssexan-42hss1 job

-----------------
Running setup_db_home-ssexan-42hss1 job
Completed setup_db_home-ssexan-42hss1 job

-----------------
Running root_script_execution-ssexan-42hss1 job
Completed root_script_execution-ssexan-42hss1 job

-----------------
Running copy_home_to_backup_loc-ssexan-42hss1 job
Completed copy_home_to_backup_loc-ssexan-42hss1 job

-----------------
Running copy_config_files-ssexan-42hss1 job
Completed copy_config_files-ssexan-42hss1 job

-----------------
Running copy_image-ssexan-42hss2 job
Completed copy_image-ssexan-42hss2 job

Running move_home-ssexan-42hss2 job
Completed move_home-ssexan-42hss2 job

Running setup_db_home-ssexan-42hss2 job
Completed setup_db_home-ssexan-42hss2 job

Running root_script_execution-ssexan-42hss2 job
Completed root_script_execution-ssexan-42hss2 job

Running copy_config_files-ssexan-42hss2 job
Completed copy_config_files-ssexan-42hss2 job

Running release_lock job
Completed release_lock job

Running cleanup job
Completed cleanup job

DBHome Patching Successful.

To learn more about the patch db apply subcommand, including available options, execute the following command:

```
# dbaascli dbhome patch ?
```

To learn more about the dbaascli dbhome patch subcommand, including available options, execute the following command:

```
# dbaascli dbhome patch ?
```

4. Exit the root-user command shell:

```
# exit
$
```

**Upgrading Exadata Grid Infrastructure**

This topic describes how to upgrade the Oracle Grid Infrastructure (GI) on an Exadata cloud VM cluster using the Oracle Cloud Infrastructure Console or API. Upgrading allows you to provision Oracle Database Homes and databases that use the most current Oracle Database software. For more information on Exadata cloud VM clusters and the new Exadata resource model, see [Overview of X8M Scalable Exadata Infrastructure](#) on page 1227.
Database

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

Prerequisites

To upgrade your GI to Oracle Database 19c, you must be using the Oracle Linux 7 operating system for your VM cluster. For more information on upgrading the operating system, see the following documentation:

- How to update the Exadata System Software (DomU) to 19 from 18 on the Exadata Cloud Service in OCI (My Oracle Support Doc ID 2521053.1).

About Upgrading Grid Infrastructure

Upgrading the Oracle Grid Infrastructure (GI) on a VM cluster involves upgrading all the compute nodes in the instance. The upgrade is performed in a rolling fashion, with only one node being upgraded at a time.

- Oracle recommends running an upgrade precheck to identify and resolve any issues that would prevent a successful upgrade.
- You can monitor the progress of the upgrade operation by viewing the associated work requests.
- If you have an Exadata infrastructure maintenance operation scheduled to start within the next 24 hours, the GI upgrade feature is not available.
- During the upgrade, you cannot perform other management operations such as starting, stopping or rebooting nodes, scaling CPU, provisioning or managing Database Homes or databases, restoring a database, or editing IORM settings. The following Data Guard operations are not allowed on the VM cluster undergoing a GI upgrade:
  - Enable Data Guard
  - Switchover
  - Failover to the database using the VM cluster (a failover operation to a standby on another VM cluster is possible)

Using the Console

You can use the Console to perform a precheck prior to upgrading your Oracle Grid Infrastructure (GI), and to perform the GI upgrade operation.

To precheck your cloud VM cluster prior to upgrading

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Click Exadata VM Clusters.
4. In the list of cloud VM clusters, click the name of the cluster you want to patch to display the cluster details.
5. Under Version, click the View Patches link beside the Updates Available field.
6. Click Updates to view the list of available patches and upgrades.
7. Click the Actions icon (three dots) at the end of the row listing the Oracle Grid Infrastructure (GI) upgrade, then click Run Precheck.
8. In the Confirm dialog, confirm you want to upgrade to begin the precheck operation.

To upgrade the Oracle Grid Infrastructure of a cloud VM cluster

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Click Exadata VM Clusters.
4. In the list of cloud VM clusters, click the name of the cluster you want to patch to display the cluster details.

5. Under Version, click the View Patches link beside the Updates Available field.

6. Click Updates to view the list of available patches and upgrades.

7. Click the Actions icon (three dots) at the end of the row listing the Oracle Grid Infrastructure (GI) upgrade, then click Upgrade Grid Infrastructure.

8. In the Upgrade Grid Infrastructure dialog, confirm you want to upgrade the GI by clicking Upgrade Grid Infrastructure. If you haven't run a precheck, you have the option of clicking Run Precheck in this dialog to precheck your cloud VM cluster prior to the upgrade.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225. Use these API operations to upgrade the Oracle Grid Infrastructure in a cloud VM clusters and view the cluster's update history.

- ListCloudVmClusterUpdates
- ListCloudVmClusterUpdateHistoryEntries
- GetCloudVmClusterUpdate
- GetCloudVmClusterUpdateHistoryEntry
- UpdateVmCluster

For the complete list of APIs for the Database service, see Database Service API.

Upgrading Exadata Databases

Note: This topic applies only to Exadata Cloud Service instances using the new resource model. For information on converting an Exadata DB system to the new resource model, see Switching an Exadata DB System to the New Resource Model and APIs on page 1228.

This topic describes the procedures to upgrade an Exadata database instance to Oracle Database 19c (Long Term Release) by using the Console and the API. The upgrade is accomplished by moving the Exadata database to a Database Home that uses the target software version.

Prerequisites

The following are required in order to upgrade an Exadata Oracle Database instance:

- The Exadata Cloud Service instance system software must use Oracle Linux 7 (OL7). See How to update the Exadata System Software (DomU) to 19 from 18 on the Exadata Cloud Service in OCI for instructions on manually updating the operating system.
- The Oracle Grid Infrastructure must be version 19c. See Upgrading Exadata Grid Infrastructure on page 1299 for instructions on using the Oracle Cloud Infrastructure Console or API to upgrade Grid Infrastructure. If patches are available for your Grid Infrastructure, Oracle recommends applying them prior to performing a database upgrade.
- You must have an available Oracle Database Home that uses the two most recent version of Oracle Database 19c available in Oracle Cloud Infrastructure. See To create a new Database Home in an existing Exadata Cloud Service instance on page 1330 for information on creating a Database Home. You can use Oracle-published software images or a custom database software image based on your patching requirements to create Database Homes.
- You must ensure that all pluggable databases in the container database that is being upgraded can be opened. Pluggable databases that cannot be opened by the system during the upgrade can cause an upgrade failure.

Your Oracle database must be configured with the following settings in order to upgrade:

- The database must be in archivelog mode
- The database must have flashback enabled
See the Oracle Database documentation for your database's release version to learn more about these settings.

**About Upgrading a Database**

For database software version upgrades, note the following:

- Database upgrades involve database downtime. Keep this in mind when scheduling your upgrade.
- Oracle recommends that you back up your database and test the new software version on a test system or a cloned version of your database before you upgrade a production database. See To create an on-demand full backup of a database on page 1322 for information on creating an on-demand manual backup.
- Oracle recommends running an upgrade precheck operation for your database prior to attempting an upgrade so that you can discover any issues that need mitigation prior to the time you plan to perform the upgrade. The precheck operation does not affect database availability and can be performed at any time that is convenient for you.
- If your databases uses Data Guard, you will need to disable or remove the Data Guard association prior to upgrading.
- An upgrade operation cannot take place while an automatic backup operation is underway. Before upgrading, Oracle recommends disabling automatic backups and performing a manual backup. See To configure automatic backups for a database on page 1322 and To create an on-demand full backup of a database on page 1322 for more information.
- After upgrading, you cannot use automatic backups taken prior to the upgrade to restore the database to an earlier point in time.
- If you are upgrading an database that uses version 11.2 software, the resulting version 19c database will be a non-container database (non-CDB).

**How the Upgrade Operation Is Performed by the Database Service**

During the upgrade process, the Database service does the following:

- Executes an automatic precheck. This allows the system to identify issues needing mitigation and to stop the upgrade operation.
- Sets a guaranteed restore point, enabling it to perform a flashback in the event of an upgrade failure.
- Moves the database to a user-specified Oracle Database Home that uses the desired target software version.
- Runs the Database Upgrade Assistant (DBUA) software to perform the upgrade.

**Rolling Back an Unsuccessful Upgrade**

If your upgrade does not complete successfully, you have the option of performing a rollback. Details about the failure are displayed on the Database Details page in the Console, allowing you to analyze and resolve the issues causing the failure. A rollback resets your database to the state prior to the upgrade. All changes to the database made during and after the upgrade will be lost. The rollback option is provided in a banner message displayed on the database details page of a database following an unsuccessful upgrade operation. See To roll back a failed database upgrade on page 1303 for more information.

**After Your Upgrade Is Complete**

After a successful upgrade, note the following:

- Check that automatic backups are enabled for the database if you disabled them prior to upgrading. See To configure automatic backups for a database on page 1322 for more information.
- Edit the Oracle Database COMPATIBLE parameter to reflect the new Oracle Database software version. See What Is Oracle Database Compatibility? for more information.
- If your database uses a <database_name>.env file, ensure that the variables in the file have been updated to point to the 19c Database Home. These variables should be automatically updated during the upgrade process.
- If you are upgrading a non-container database to Oracle Database version 19c, you can convert the database to a pluggable database after converting. See How to Convert Non-CDB to PDB (Doc ID 2288024.1) for instruction on converting your database to a pluggable database.
• If your old Database Home is empty and will not be reused, you can remove it. See To delete a Database Home on page 1332 for more information.

**Using the Console**

You can use the Console to:
• Upgrade your database
• Roll back an unsuccessful upgrade
• View the update history of a database that has been upgraded

Oracle recommends that you use the precheck action to ensure that your database has met the requirements for the upgrade operation.

*To upgrade or precheck an Exadata database*

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, click the name of the VM cluster that contains the database you want to upgrade.

**Note:**
If your database is in an Exadata Cloud Service instance that does not use the new Exadata resource model, you will need to switch the instance to the new model before you can upgrade your database.

4. In the list of databases on the details page of the VM cluster, click the name of the database you want to upgrade to view the Database Details page.
5. Click More Actions, then Upgrade.
6. In the Upgrade Database dialogue, select the following:
   • **Oracle Database version:** The drop-down selector lists only Oracle Database versions that are compatible with an upgrade from the current software version the database is using. The target software version must be higher than the database's current version.
   • **Target Database Home:** Select a Database Home for your database. The list of Database Homes is limited to those homes using the most recent versions of Oracle Database 19c software. Moving the database to the new Database Home results in the database being upgraded to the major release version and patching level of the new Database Home.

7. Click one of the following:
   • **Run Precheck:** This option starts an upgrade precheck to identify any issues with your database that need mitigation before you perform an upgrade.
   • **Upgrade database:** This option starts upgrade operation. Oracle recommends performing an upgrade only after you have performed a successful precheck on the database.

*To roll back a failed database upgrade*

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, click the name of the VM cluster that contains the database with the failed upgrade.
4. Find the database that was unsuccessfully upgraded, and click its name to display details about it. The database should display a banner at the top of the details page that includes a Rollback button and details about what issues caused the upgrade failure.
5. Click Rollback. In the Confirm rollback dialog, confirm that you want to initiate a rollback to the previous Oracle Database version by clicking Rollback.

*To view the upgrade history of a database*

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Under Exadata at Oracle Cloud, click **Exadata VM Clusters**. In the list of VM clusters, click the name of the VM cluster that contains the database you want to upgrade.

   **Note:**
   If your database is in an Exadata Cloud Service instance that does not use the new Exadata resource model, you will need to switch the instance to the new model before you can upgrade your database.

4. In the list of databases on the details page of the VM cluster, click the name of the database for which you want to view the upgrade history.

5. On the Database Details page, under **Database Version**, click the View link that is displayed for databases that have been upgraded. This link does not appear for databases that have not been updated.

   The **Updates History** page is displayed. The table displayed on this page shows precheck and upgrade operations performed on the database.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs to manage database upgrades:

- ListDatabaseUpgradeHistoryEntries
- UpgradeDatabase

For the complete list of APIs for the Database service, see Database Service API.

   **Note:**
   When using the UpgradeDatabase API to upgrade an Exadata Cloud Service database, you must specify DB_HOME as the upgrade source.

**Monitoring an Exadata Cloud Service Database**

This topic explains how to access Enterprise Manager Database Express and Enterprise Manager Database Control, which are web-based tools for managing Oracle Database.

**Accessing Enterprise Manager Database Express 12c**

Enterprise Manager Database Express 12c (EM Express) is available on Exadata Cloud Service databases created using Oracle Database 12c Release 1 (12.1) or later.

How you access EM Express depends on whether you want to manage a CDB or PDB.

- **To manage the CDB.** When a database is created, the Database service automatically sets port 5500 on the deployment’s compute nodes for EM Express access to the CDB.
- **To manage a PDB.** For a database using Oracle Database 12.2 or later, a single port (known as the global port) is automatically set on the compute nodes. The global port lets you use EM Express to connect to all of the PDBs in the CDB using the HTTPS port for the CDB.

   For a database using Oracle Database 12.1, you must manually set a port on the compute nodes for each PDB you want to manage using EM Express.

For both CDBs and PDBs, you must add the port to a security list as described in Updating the Security List on page 1305.

To confirm the port that is in use for a specific database, connect to the database as a database administrator and execute the query shown in the following example:

```
SQL> select dbms_xdb_config.getHttpsPort() from dual;
```

```
DBMS_XDB_CONFIG.GETHTTPS_PORT()
```
Setting the Port for EM Express to Manage a PDB (Oracle Database 12.1 Only)

In Oracle Database 12c Release 1, a unique HTTPS port must be configured for the root container (CDB) and each PDB that you manage using EM Express.

To configure a HTTPS port so that you can manage a PDB with EM Express:

1. Invoke SQL*Plus and log in to the PDB as the SYS user with SYSDBA privileges.
2. Execute the `DBMS_XDB_CONFIG.SETHTTPSPORT` procedure.

   ```sql
   SQL> exec dbms_xdb_config.sethttpsport(port-number)
   ```

Accessing EM Express

Before you access EM Express, add the port to the security list. See Updating the Security List on page 1305.

After you update the security list, you can access EM Express by directing your browser to the URL `https://<node-ip-address>:<port>/em`, where `node-ip-address` is the public IP address of the compute node hosting EM Express, and `port` is the EM Express port used by the database.

Accessing Enterprise Manager 11g Database Control

Enterprise Manager 11g Database Control (Database Control) is available on Exadata Cloud Service databases created using Oracle Database 11g Release 2. Database Control is allocated a unique port number for each database deployment. By default, access to Database Control is provided using port 1158 for the first deployment. Subsequent deployments are allocated ports in a range starting with 5500, 5501, 5502, and so on.

You can confirm the Database Control port for a database by searching for `REPOSITORY_URL` in the `$ORACLE_HOME/host_sid/sysman/config/emd.properties` file.

Before you access Database Control, add the port for the database to the security list associated with the Exadata DB system's client subnet. For more information, see Updating the Security List on page 1305.

After you update the security list, you can access Database Control by directing your browser to the URL `https://<node-ip-address>:<port>/em`, where `node-ip-address` is the public IP address of the compute node hosting Database Control, and `port` is the Database Control port used by the database.

Updating the Security List

Before you can access EM Express or Database Control, you must add the port for the database to the security list associated with the data (client) subnet used by the cloud VM cluster (for systems using the new resource model) or the DB system. To update an existing security list, complete the following steps using the Console:

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system contains the security list you want to update:
   - **Cloud VM clusters (new resource model):** Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster in which you want to manage and click its highlighted name to view the details page for the cluster.
   - **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system in which you want to manage, and then click its name to display details about it.
4. Note Client Subnet name of the cloud VM cluster or the DB system and click its Virtual Cloud Network.
5. Locate the subnet in the list, and then click its security list under Security Lists.
6. Click Edit All Rules and add an ingress rule with source type=CIDR, source CIDR=<source CIDR>, protocol=TCP, and port=<port number or port range>.

The source CIDR should be the CIDR block that includes the ports you open for the client connection.
Creating and Managing Exadata Databases

This topic describes creating and managing Oracle Databases on an Exadata Cloud Service instance.

When you create a Exadata Cloud Service instance, an initial Database Home and database are created. You can create additional Database Homes and databases at any time by using the Console or the Oracle Cloud Infrastructure API.

When you add a database to a VM cluster or a DB system resource on an Exadata instance, the database versions you can select from depend on the current patch level of that resource. You may have to patch your VM cluster or DB system to add later database versions.

After you provision a database, you can move it to another Database Home. Consolidating databases under the same home can facilitate management of these resources. All databases in a given Database Home share the Oracle Database binaries and therefore, have the same database version. The Oracle-recommended way to patch a database to a version that is different from the current version is to move the database to a home running the target version. For information about patching, see Patching an Exadata Cloud Service Instance on page 1284.

**Note:**

When provisioning databases, make sure your VM cluster or DB system has enough OCPUs enabled to support the total number of database instances on the system. Oracle recommends the following general rule: for each database, enable 1 OCPU per node. See To scale CPU cores in an Exadata Cloud Service cloud VM cluster or DB system on page 1258 for information on scaling your OCPU count up or down.

When you create an Exadata database, you can choose to encrypt the database using your own encryption keys that you manage. You can rotate encryption keys, periodically, to maintain security compliance and, in cases of personnel changes, to disable access to a database.

**Note:**

- The encryption key you use must be AES-256.
- To ensure that your Exadata database uses the most current versions of the Vault encryption key, rotate the key from the database details page on the Oracle Cloud Infrastructure Console. Do not use the Vault service.
- You can only use Oracle-managed encryption keys if your database is enabled with Oracle Data Guard.

If you want to use your own encryption keys to encrypt a database that you create, then you must create a dynamic group and assign specific policies to the group for customer-managed encryption keys. See Managing Dynamic Groups on page 2422 and Let security admins manage vaults, keys, and secrets on page 2151. Additionally, see To integrate customer-managed key management into Exadata Cloud Service on page 1283 if you need to update customer-managed encryption libraries for the Vault service.

You can also add and remove databases, and perform other management tasks on a database by using command line utilities. For information and instructions on how to use these utilities, see Creating and Managing Exadata Databases Manually on page 1313.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.
To enable management of customer-managed encryption keys, you must create a policy in the tenancy that allows a particular dynamic group to do so, similar to the following:

```
allow dynamic-group dynamic_group_name to manage keys in tenancy
```

If you are new to policies, then see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want more information about writing policies for databases, then see Details for the Database Service on page 2240.

**Using the Console**

*To create a database in an existing Exadata Cloud Service instance*

**Note:**

If IORM is enabled on the Exadata Cloud Service instance, the default directive will apply to the new database and system performance might be impacted. Oracle recommends that you review the IORM settings and make applicable adjustments to the configuration after the new database is provisioned.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to create the database in:

   *Cloud VM clusters (new resource model):* Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   *DB systems:* Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. Click Create Database.
5. In the Create Database dialog, enter the following:

   - **Database name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
   - **Database version:** The version of the database. You can mix database versions on the Exadata DB system.
   - **PDB name:** *(Optional)* For Oracle Database 12c (12.1.0.2) and later, you can specify the name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of eight alphanumeric characters. The only special character permitted is the underscore (_).
   - **Database Home:** The Oracle Database Home for the database. Choose the applicable option:

     - **Select an existing Database Home:** The Database Home display name field allows you to choose the Database Home from the existing homes for the database version you specified. If no Database Home with that version exists, you must create a new one.

     - **Create a new Database Home:** A database home will be created using the database version and the Database Home display name you specified.

   - **Create administrator credentials:** A database administrator SYS user will be created with the password you supply.
     - **Username:** SYS
     - **Password:** Supply the password for this user. The password must meet the following criteria:

       - A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The
special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.

- **Confirm password:** Re-enter the SYS password you specified.
- **Select workload type:** Choose the workload type that best suits your application:
  - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
  - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
- **Configure database backups:** Specify the settings for backing up the database to Object Storage:
  - **Enable automatic backup:** Check the check box to enable automatic incremental backups for this database. If you are creating a database in a security zone compartment, you must enable automatic backups.
  - **Backup retention period:** If you enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
  - **Backup Scheduling:** If you enable automatic backups, you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See Automatic Incremental Backups for more information.

6. Click **Show Advanced Options** to specify advanced options for the database:

   - **Character set:** The character set for the database. The default is AL32UTF8.
   - **National character set:** The national character set for the database. The default is AL16UTF16.
   - If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
   - If you are creating a database in an Exadata Cloud Service VM cluster, then you can choose to use encryption based on encryption keys that you manage. By default, the database is configured using Oracle-managed encryption keys. To configure the database with encryption based on encryption keys you manage:
     a. Click the Encryption tab.
     b. Select Use customer-managed keys. You must have a valid encryption key in Oracle Cloud Infrastructure Vault service. See Let security admins manage vaults, keys, and secrets on page 2151.

       **Note:**

       Oracle only supports AES-256 encryption keys.

     c. Choose a vault from the Vault in compartment drop-down. You can change the compartment by clicking the CHANGE COMPARTMENT link.
     d. Select an encryption key from the Master encryption key in compartment drop-down. You can change the compartment containing the encryption key you want to use by clicking the CHANGE COMPARTMENT link.
     e. If you want to use an encryption key that you import into your vault, then select Choose the key version and enter the OCID of the key you want to use in the Key version OCID field.

       **Note:**

       - Oracle supports customer-managed keys on databases after Oracle Database 11g release 2 (11.2.0.4).
       - If you choose to provide an OCID for the valid key version, then ensure that the OCID corresponds to the key version you want to use.

7. Click **Create Database**.

After database creation is complete, the status changes from **Provisioning** to **Available**, and on the database details page for the new database, the Encryption section displays the encryption key name and the encryption key OCID.
Caution:
Do not delete the encryption key from the vault. This causes any database protected by the key to become unavailable.

To create a database from a backup
Before you begin, note the following:

• When you create a database from a backup, the availability domain is the same as the availability domain that hosts the backup.
• The Oracle Database software version you specify must be the same or later version as that of the backed-up database.
• If you are creating a database from an automatic backup, then you can choose any level 0 weekly backup, or a level 1 incremental backup created after the most recent level 0 backup. For more information on automatic backups, see Using the Console on page 1321
• If the backup being used to create a database is in a security zone compartment, the database cannot be created in a compartment that is not in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to a backup.
   • Standalone backups: Click Standalone Backups under Bare Metal, VM, and Exadata.
   • Automatic backups: Navigate to the Database Details page of the database associated with the backup:
     • Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
     • DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

   Click the name of the database associated with the backup that you will use to create the new database. Locate the backup in the list of backups on the Database Details page.
4. Click the Actions icon (three dots) for the backup you chose.
5. Click Create Database. On the Create Database from Backup page, configure the database as follows.
6. In the Configure your DB system section:
   • Backups created in cloud VM clusters: Choose a cloud VM cluster to run the database from the Select a VM cluster drop-down list.
   • Backups created in DB systems: Choose a shape from the Select a shape drop-down list, then choose a DB system to run the database from the Select a DB system drop-down list.
7. In the Configure Database Home section:
   • Select an existing Database Home: If you choose this option, make a selection from the Select a Database Home drop-down list.
   • Create a new Database home: If you choose this option, enter a name for the new Database Home in the Database Home display name field.
8. In the Configure database section:
   • In the Database name field, accept the default name or name the database.
     The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
   • In the Password and Confirm password fields, enter and re-enter a password.
     A strong password for SYS administrator must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password
must not contain the user name (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reverse order and regardless of casing.

9. In the **Enter the source database’s TDE wallet or RMAN password** field, enter a password that matches either the Transparent Data Encryption (TDE) wallet password or RMAN password for the source database.

10. Click **Create Database**.

To navigate to a list of backups for a particular database:

1. Click the DB system name that contains the specific database to display the DB System Details page.
2. From the list of databases, click the database name associated with the backup you want to use to display a list of backups on the database details page. You can also access the list of backups for a database by clicking **Backups in the Resources section**.

To navigate to the list of standalone backups for your current compartment:

1. Click **Standalone Backups** under **Bare Metal, VM, and Exadata**.
2. In the list of standalone backups, find the backup you want to use to create the database.

**To move a database to another Database Home**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the database:
   
   - **Cloud VM clusters (new resource model)**: Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   
   - **DB systems**: Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. Click **Move to Another Home**.
5. Select the target Database Home.
6. Click **Move Database**.
7. Confirm the move operation.

The database will be stopped in the current home and then restarted in the destination home. While the database is being moved, the Database Home status displays as **Moving Database**. When the operation completes, Database Home is updated with the current home. If the operation is unsuccessful, the status of the database displays as **Failed**, and the Database Home field provides information about the reason for the failure.

**To terminate a database**

You'll get the chance to back up the database prior to terminating it. This creates a standalone backup that can be used to create a database later. We recommend that you create this final backup for any production (non-test) database.

**Note:**

Terminating a database removes all automatic incremental backups of the database from Oracle Cloud Infrastructure Object Storage. However, all full backups that were created on demand, including your final backup, will persist as standalone backups.

You cannot terminate a database that is assuming the primary role in a Data Guard association. To terminate it, you can switch it over to the standby role.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the database.

   **X8M systems**: Under Exadata at Oracle Cloud, click **Exadata VM Clusters**. In the list of cloud VM clusters, find the VM cluster containing the database you want to manage and click its highlighted name to view the details page for the cluster.

   In the list of databases, click the highlighted name of the database you wish to manage. The Database Details page is displayed.

   **X6, X7, or X8 systems**: Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system containing the database you want to manage and click its highlighted name to view the details page for the DB system.

   In the list of databases, click the highlighted name of the database you wish to manage. The Database Details page is displayed.

4. Click **More Actions**, and then click **Terminate**.

5. In the confirmation dialog, indicate whether you want to back up the database before terminating it, and type the name of the database to confirm the termination.

6. Click **Terminate Database**.

   The database's status indicates Terminating.

### To administer Vault encryption keys

After you provision a database in an Exadata DB system or VM cluster, you can rotate the Vault encryption key or change the encryption management configuration for that database.

**Note:**

- To ensure that your Exadata database uses the most current version of the Vault encryption key, rotate the key from the database details page on the Oracle Cloud Infrastructure Console. Do not use the Vault service.
- You can rotate Vault encryption keys only on databases that are configured with customer-managed keys.
- You can change encryption key management from Oracle-managed keys to customer-managed keys but you cannot change from customer-managed keys to Oracle-managed keys.
- If the database for which you are changing encryption key management is using Oracle-managed keys and is enabled with Oracle Data Guard, then you cannot change to customer-managed keys.
- Oracle supports administering encryption keys on databases after Oracle Database 11g release 2 (11.2.0.4).

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose your compartment from the **Compartment** drop-down.

3. Navigate to the cloud VM cluster or DB system that contains the database for which you want to change encryption management or to rotate a key.

   **Cloud VM clusters**: Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, locate the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems**: Under **Bare Metal, VM, and Exadata**, click **DB Systems**. In the list of DB systems, locate the Exadata DB system you want to access and click its name to display its details page.

4. In the **Databases** section, click the name of the database for which you want to change encryption management or to rotate a key to display its details page.

5. Click the **More Actions** drop-down.
6. Click **Administer Encryption Key**.

   To rotate an encryption key on a database using customer-managed keys:
   a. Click **Rotate Encryption Key** to display a confirmation dialog.
   b. Click **Rotate Key**.

   To change key management type from Oracle-managed keys to customer-managed keys:
   a. Click **Change Key Management Type**.
   b. Select **Use customer-managed keys**.

   You must have a valid encryption key in Oracle Cloud Infrastructure Vault service and provide the information in the subsequent steps. See Key and Secret Management Concepts on page 3953.
   c. Choose a vault from the **Vault in compartment** drop-down. You can change the compartment by clicking the **CHANGE COMPARTMENT** link.
   d. Select an encryption key from the **Master encryption key in compartment** drop-down. You can change the compartment containing the encryption key you want to use by clicking the **CHANGE COMPARTMENT** link.
   e. If you want to use an encryption key that you import into your vault, then select **Choose the key version** and enter the OCID of the key you want to use in the **Key version OCID** field.

   **Note:**
   Changing key management causes the database to become briefly unavailable.

   **Caution:**
   After changing key management to customer-managed keys, do not delete the encryption key from the vault as this can cause the database to become unavailable.

7. Click **Apply**.

   On the database details page for this database, the **Encryption** section displays the encryption key name and the encryption key OCID.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage databases.

- ListDatabases
- GetDatabase
- CreateDatabase
- UpdateDatabase - Use this operation to move a database to another Database Home
- DeleteDatabase

For the complete list of APIs for the Database service, see Database Service API.

**Changing the Database Passwords**

The password that you specify in the Database Admin Password field when you create a new Exadata Cloud Service instance or database is set as the password for the SYS, SYSTEM, TDE wallet, and PDB Admin credentials. Use the following procedures if you need to change passwords for an existing database.

Note that if you are enabling Data Guard for a database, the SYS password and the TDE wallet password of the primary and standby databases must all be the same.

*To change the SYS password for an Exadata Cloud Service database*

1. Log onto the cloud VM cluster or DB system host as opc.
2. Run the following command:

```
sudo dbaascli database changepassword --dbname <database_name>
```

To change the TDE wallet password for an Exadata Cloud Service database

1. Log onto the cloud VM cluster or DB system host as opc.
2. Run the following command:

```
sudo dbaascli tde changepassword --dbname <database_name>
```

## Creating and Managing Exadata Databases Manually

Exadata Cloud Service instances include these command line tools for performing various tasks to manage individual databases:

- **dbaasapi** - For adding and removing databases from the Exadata Cloud Service instance. See Using dbaasapi on page 1313.
- **dbaascli** - For a variety of life-cycle and administration operations such as:
  - Starting and stopping a database
  - Starting and stopping the Oracle Net listener
  - Viewing information about Oracle Homes
  - Moving a database to another Oracle Home
  - Deleting an unused Oracle Home
  - Performing database configuration changes
  - Managing Oracle Database software images
  - Managing pluggable databases (PDBs)
  - Performing database recovery
  - Rotating the master encryption key

For details about how to use this CLI, see The dbaascli Utility.

### Using dbaasapi

You can use the dbaasapi command line utility to create and delete databases on an Exadata DB system. The utility operates like a REST API. It reads a JSON request body and produces a JSON response body in an output file.

The utility is located in the `/var/opt/oracle/dbaasapi/` directory on the compute nodes and must be run as the root user.

To learn how to add or remove Exadata databases by using the Oracle Cloud Infrastructure Console or API instead, see Creating and Managing Exadata Databases on page 1306.

### Note:

- You must update the cloud-specific tooling on all the compute nodes in your Exadata Cloud Service instance before performing the following procedures. For more information, see Updating an Exadata Cloud Service Instance on page 1274.
- Only one dbaasapi operation can execute at a given time. We recommend that you check the status of an operation to ensure it completed before you run another operation.
- Databases that you create by using dbaasapi are visible in the Console and through the API and CLI only if you create the database across all nodes in the cluster. However, it can take up to 5 hours before you see them.
Prerequisites

If you plan to create a database and store its backups in the Oracle Cloud Infrastructure Object Storage, refer to the prerequisites in Managing Exadata Database Backups on page 1320, and ensure that the system meets the networking requirements for backing up to Object Storage. Review Create Database Parameters on page 1316 and gather the information you'll need to supply in the input file you create for the dbaasapi operation.

Caution:

We recommend that you avoid specifying parameter values that include confidential information when you use the dbaasapi commands.

Creating a Database

The following procedure creates directory called dbinput, a sample input file called myinput.json, and a sample output file called createdb.out.

1. SSH to a compute node in the Exadata DB system.

   ```
   ssh -i <private_key_path> opc@<node_ip_address>
   ```

2. Log in as opc and then sudo to the root user.

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. Make a directory for the input file and change to the directory.

   ```
   [root@dbsys ~]# mkdir -p /home/oracle/dbinput
   # cd /home/oracle/dbinput
   ```

4. Create the input file in the directory. The following sample file will create a database configured to store backups in an existing bucket in Object Storage. For parameter descriptions, see Create Database Parameters on page 1316.

   ```json
   {
     "object": "db",
     "action": "start",
     "operation": "createdb",
     "params": {
       "nodelist": "",
       "dbname": "exadb",
       "edition": "EE_EP",
       "version": "12.1.0.2",
       "ohome_name": "oradbhome1",
       "adminPassword": "<password>",
       "sid": "exadb",
       "pdbName": "PDB1",
       "charset": "AL32UTF8",
       "ncharset": "AL16UTF16",
       "backupDestination": "OSS",
       "cloudStorageContainer": "https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/mycompany/DBBackups",
       "cloudStorageUser": "<name@example.com>",
       "cloudStoragePwd": "<auth_token>"
     },
     "outputfile": "/home/oracle/createdb.out",
     "FLAGS": ""
   }
   ```
5. Run the utility and specify the input file.

```
[root@dbsys ~]# /var/opt/oracle/dbaasapi/dbaasapi -i myinput.json
```

6. Check the output file and note the ID.

```
[root@dbsys ~]# cat /home/oracle/createdb.out
{
  "msg": "",
  "object": "db",
  "status": "Starting",
  "errmsg": "",
  "outputfile": "/home/oracle/createdb.out",
  "action": "start",
  "id": "170",
  "operation": "createdb",
  "logfile": "/var/opt/oracle/log/gsa1/dbaasapi/db/createdb/1.log"
}
```

7. Create a JSON file to check the database creation status. Note the action of "status". Replace the ID and the dbname with the values from the previous steps.

```
{
  "object": "db",
  "action": "status",
  "operation": "createdb",
  "id": 170,
  "params": {
    "dbname": "exadb"
  },
  "outputfile": "/home/oracle/createdb.out",
  "FLAGS": ""
}
```

8. Run the utility with the status file as input and then check the utility output.

Rerun the status action regularly until the response indicates that the operation succeeded or failed.

```
[root@dbsys ~]# /var/opt/oracle/dbaasapi/dbaasapi -i db_status.json
[root@dbsys ~]# cat /home/oracle/createdb.out
{
  "msg": "Sync sqnet file...[done]\n##Done executing tde\nWARN: Could not register elogger_parameters: elogger.pm::_init: /var/opt/oracle/dbaas_acfs/events does not exist\n##Invoking assistant bkup\nUsing cmd : /var/opt/oracle/ocde/assistants/bkup/bkup -out /var/opt/oracle/ocde/res/bkup.out -sid="exadb1" -reco_grp="RECOC1" -hostname="ed1db01.data.customer1.oraclevcn.com" -oracle_home="/u02/app/oracle/product/12.1.0/dbhome_5" -dbname="exadb" -dbtype="exarac" -exabm="\n
##Done executing bkup\nWARN: Could not register elogger_parameters: elogger.pm::_init: /var/opt/oracle/dbaas_acfs/events does not existRemoved all entries from creg file : /var/opt/oracle/creg/exadb.ini matching passwd or decrypt_key\n\\n\\n#### Completed OCDE Successfully ####\nWARN: Could not register elogger_parameters: elogger.pm::_init: /var/opt/oracle/dbaas_acfs/events does not exist",
```

Oracle Cloud Infrastructure User Guide 1315
### Create Database Parameters

Use the following parameters to create a database.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object</td>
<td>The value &quot;db&quot;.</td>
</tr>
<tr>
<td>action</td>
<td>The value &quot;start&quot;.</td>
</tr>
<tr>
<td>operation</td>
<td>The value &quot;createdb&quot;.</td>
</tr>
<tr>
<td>nodelist</td>
<td>The value &quot;&quot; (an empty string). The database will be created across all nodes in the cluster. <strong>Note:</strong> If you specify only a subset of nodes, then the database you create will not be visible in the Oracle Cloud Infrastructure interfaces (Console, API, and CLI).</td>
</tr>
<tr>
<td>dbname</td>
<td>The database name, in quotes.</td>
</tr>
<tr>
<td>edition</td>
<td>The value &quot;EE_EP&quot;. (Only Enterprise Edition - Extreme Performance is supported.)</td>
</tr>
<tr>
<td>version</td>
<td>The database version as 18.0.0.0, 12.2.0.1, 12.1.0.2, or 11.2.0.4, in quotes.</td>
</tr>
<tr>
<td>ohome_name</td>
<td>The name of the Oracle Database Home to use for the new database, in quotes.</td>
</tr>
<tr>
<td>adminPassword</td>
<td>The administrator (SYS and SYSTEM) password to use for the new database, in quotes. The password must be nine to thirty characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -.</td>
</tr>
<tr>
<td>sid</td>
<td>The SID of the database, in quotes.</td>
</tr>
<tr>
<td>pdbName</td>
<td>The name of the pluggable database, in quotes.</td>
</tr>
<tr>
<td>charset</td>
<td>The database character set, in quotes. For allowed values, see Allowed Create Database Charset Values on page 1318.</td>
</tr>
<tr>
<td>ncharset</td>
<td>The database national character set. The value AL16UTF16 or UTF8, in quotes.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>backupDestination</td>
<td>The database backup destination, in quotes. You can configure the following backup destinations.</td>
</tr>
<tr>
<td></td>
<td>NONE No backup destination is configured.</td>
</tr>
<tr>
<td></td>
<td>DISK Configure database backups to the local disk Fast Recovery Area.</td>
</tr>
<tr>
<td></td>
<td>OSS Configure database backups to an existing bucket in the Oracle Cloud Infrastructure Object Storage service. You must specify all the cloudStorage parameters.</td>
</tr>
<tr>
<td></td>
<td>BOTH Configure database backups to both local disk and an existing bucket in Object Storage. You must specify all the cloudStorage parameters.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>&quot;backupDestination&quot;:&quot;BOTH&quot;</td>
</tr>
<tr>
<td>cloudStorageContainer</td>
<td>Required if you specify a backup destination of OSS or BOTH. The Object Storage URL, your Oracle Cloud Infrastructure tenant, and an existing bucket in the object store to use as the backup destination, in the following format:</td>
</tr>
<tr>
<td></td>
<td><a href="https://swiftobjectstorage">https://swiftobjectstorage</a>.&lt;region_name&gt;.oraclecloud.com/v1/&lt;tenant&gt;/&lt;bucket&gt;</td>
</tr>
<tr>
<td></td>
<td>See Regions and Availability Domains on page 180 to look up the region name string.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>&quot;cloudStorageContainer&quot;:&quot;<a href="https://swiftobjectstorage">https://swiftobjectstorage</a>.&lt;region_name&gt;.oraclecloud.com/v1/&lt;company_name&gt;/DBBackups&quot;</td>
</tr>
<tr>
<td>cloudStorageUser</td>
<td>Required if you specify a backup destination of OSS or BOTH. The user name for the Oracle Cloud Infrastructure user account, for example:</td>
</tr>
<tr>
<td></td>
<td>&quot;cloudStorageUser&quot;:&quot;<a href="mailto:name@company.com">name@company.com</a>&quot;</td>
</tr>
<tr>
<td></td>
<td>This is the user name you use to sign in to the Console. The user name must be a member of the Administrators group, as described in Prerequisites on page 1314.</td>
</tr>
<tr>
<td>cloudStoragePwd</td>
<td>Required if you specify a backup destination of OSS or BOTH. The auth token generated by using the Console or IAM API, in quotes, for example:</td>
</tr>
<tr>
<td></td>
<td>&quot;cloudStoragePwd&quot;:&quot;&lt;auth_token&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>For more information, see Managing User Credentials on page 2456.</td>
</tr>
<tr>
<td></td>
<td>This is not the password for the Oracle Cloud Infrastructure user.</td>
</tr>
</tbody>
</table>
Database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outputfile</td>
<td>The absolute path for the output of the request, for example, &quot;outputfile&quot;: &quot;/home/oracle/createdb.out&quot;.</td>
</tr>
</tbody>
</table>

| FLAGS | The value "" (an empty string). |

**Allowed Create Database Charset Values**

AL32UTF8, AR8ADOS710, AR8ADOS720, AR8APTEC715, AR8ARABICMACS, AR8ASMO8X, AR8ISO8859P6, AR8MSWIN1256, AR8MUSSD768, AR8NAFITHA711, AR8NAFITHA721, AR8SAKHR706, AR8SAKHR707, AZ8ISO8859P9E, BG8MSWIN, BG8PC437S, BLT8CP924, BLT8ISO8859P13, BLT8MSWIN1257, BLT8PC775, BN8BSCII, CDN8PC863, CEL8ISO8859P14, CL8ISO8859P5, CL8ISO1R111, CL8KOI8R, CL8KOI8U, CL8MACCYRILLICS, CL8MSWIN1251, EB8ISO8859P2, EE8MACCES, EE8MACCROATIANS, EE8MSWIN1250, EE8PC852, EL8DEC, EL8ISO8859P7, EL8MACGREEKS, EL8MSWIN1253, EL8PC437S, EL8PC851, EL8PC869, ET8MSWIN923, HU8ABMOD, HU8CWI2, IN8ISCII, IS8PC861, IW8ISO8859P8, IW8MACHEBREWS, IW8MSWIN1255, IW8PC1507, JA16EUC, JA16EUCTILDE, JA16JSIS, JA16JSJISTILDE, JA16VMS, KO16KSCCS, KO16MSWIN949, LA8ISO6937, LA8PASSPORT, LT8MSWIN921, LT8PC772, LT8PC774, LV8PC1117, LV8PC8LR, LV8RS104090, N8PC865, NE8ISO8859P10, NEEBISO8859P4, RUBBESTA, RUBPC855, RUBPC866, SE8ISO8859P3, TH8MCTHAIS, TH8TISASCII, TR8DEC, TR8MACTURKISHS, TR8MSWIN1254, TR8PC857, US7ASCII, US8PC437, UTF8, VN8MSWIN1258, VN8VN3, WEB8DEC, WEB8DG, WE8ISO8859P15, WE8ISO8859P9, WE8MACROMAN8S, WE8MSWIN1252, WE8NCR4970, WEBNEXTSTEP, WE8PC850, WE8PC858, WEBPC860, WEBROMAN8, ZHS16CGB231280, ZHS16GBK, ZHT16BIG5, ZHT16CCDC, ZHT16DBT, ZHT16HKSCS, ZHT16MSWIN950, ZHT32EUC, ZHT32SOPS, ZHT32TRIS

**Deleting a Database**

We recommend that you create a final backup before you delete any production (non-test) database. See Managing Exadata Database Backups by Using bkup_api on page 1323 to learn how to back up an Exadata database.

1. SSH to a compute node (virtual machine) in the Exadata cloud VM cluster or DB system.

   ```
   ssh -i <private_key_path> opc@<node_ip_address>
   ```

2. Log in as opc and then sudo to the root user.

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. Make a directory for the input file and change to the directory.

   ```
   [root@dbsys ~]$ mkdir -p /home/oracle/dbinput
   
   # cd /home/oracle/dbinput
   ```

4. Create the input file in the directory and specify the database name to delete and an output file. For more information, see Delete Database Parameters on page 1320.

   ```
   {  
   "object": "db",  
   "action": "start",  
   "operation": "deletedb",  
   "params": {  
   "dbname": "exadb"
   },
   ```
5. Run the utility and specify the input file.

```bash
[root@dbsys ~]# /var/opt/oracle/dbaasapi/dbaasapi -i myinput.json
```

6. Check the output file and note the ID.

```bash
[root@ed1db01 ~]# cat /home/oracle/delete_exadb.out
```

7. Create a JSON file to check the database deletion status. Note the action of "status" in the sample file below. Replace the ID and the dbname with the values from the previous steps.

```json
{
  "object": "db",
  "action": "status",
  "operation": "deletedb",
  "id": 17,
  "params": {
    "dbname": "exadb"
  },
  "outputfile": "/home/oracle/deletedb.out",
  "FLAGS": ""
}
```

8. Run the utility with the status file as input and then check the utility output.

Rerun the status action regularly until the response indicates that the operation succeeded.

```bash
[root@dbsys ~]# /var/opt/oracle/dbaasapi/dbaasapi -i db_status.json
```

```bash
[root@dbsys ~]# cat /home/oracle/deletedb.out
```

```json
{
  "msg": "Using cmd : su - root -c "/var/opt/oracle/ocde/assistants/dg/dgcc -dbname exadb -action delete" \n\n##Done executing dg\n\nWARN: Could not register elogger_parameters: elogger.pm::_init: /var/opt/oracle/dbaas_acfs/events does not exist\n\n##Invoking assistant bkup\nUsing cmd : /var/opt/oracle/ocde/assistants/bkup/bkup -out /var/opt/oracle/ocde/res/bkup.out -bkup_oss_url="bkup_oss_url" -bkup_daily_time="0:13" -bkup_oss_user="bkup_oss_user" -dbname="exadb" -dctype="exarac" -exabm="yes" -firstrun="no" -action="delete" -bkup_cfg_files="no" -bkup_oss="no" -bkup_disk="no" -action=delete \n\n##Done executing bkup\n\nWARN: Could not register elogger_parameters: elogger.pm::_init: /var/opt/oracle/dbaas_acfs/events does not exist\n\n##Invoking assistant dbda\nUsing cmd : /var/opt/oracle/ocde/assistants/dbda\n```

```bash
```

```
```
Delete Database Parameters

Use the following parameters to delete a database.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object</td>
<td>The value &quot;db&quot;.</td>
</tr>
<tr>
<td>action</td>
<td>The value &quot;start&quot;.</td>
</tr>
<tr>
<td>operation</td>
<td>The value &quot;deletedb&quot;.</td>
</tr>
<tr>
<td>dbname</td>
<td>The database name, in quotes.</td>
</tr>
<tr>
<td>outputfile</td>
<td>The absolute path for the output of the request, for example, &quot;/home/oracle/deletedb.out&quot;.</td>
</tr>
<tr>
<td>FLAGS</td>
<td>The value &quot;&quot; (an empty string).</td>
</tr>
</tbody>
</table>

Managing Exadata Database Backups

This topic explains how to work with Exadata database backups managed by Oracle Cloud Infrastructure. You do this by using the Console or the API. (For unmanaged backups, see Managing Exadata Database Backups by Using bkup_api on page 1323.)

**Important:**

If you previously used bkup_api to configure backups and then you switch to using the Console or the API for backups:

- A new backup configuration is created and associated with your database. This means that you can no longer rely on your previously configured unmanaged backups to work.
- bkup_api uses cron jobs to schedule backups. These jobs are not automatically removed when you switch to using managed backups.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Prerequisites**

- Review the information and instructions in Configuring a Static Route for Accessing the Object Store on page 1254 and ensure that you configure the static route for the backup subnet on each compute node (for DB systems) or virtual machine (for cloud VM clusters) in the Exadata Cloud Service instance.
Your Exadata Cloud Service instance must have connectivity to the applicable Swift endpoint for Object Storage. See https://www.oracle.com/cloud/storage/object-storage-faq.html for information about the Swift endpoints to use.

**Important:**

To avoid backup failures, ensure that the database's archiving mode is set to `ARCHIVELOG` (the default).

**Using the Console**

You can use the Console to enable automatic incremental backups, create full backups on demand, and view the list of managed backups for a database. You can also use the Console to delete manual (on-demand) backups.

**Note:**

- The list of backups you see in the Console does not include any unmanaged backups (backups created directly by using `bkup_api`).
- All backups are encrypted with the same master key used for Transparent Data Encryption (TDE) wallet encryption.
- Backups for a particular database are listed on the details page for that database. The **Encryption Key** column displays either **Oracle-Managed Key** or a key name if you are using your own encryption keys to protect the database. See **Backing Up Vaults and Keys** on page 4003 for more information.

**Caution:**

Do not delete any necessary encryption keys from the vault because this causes databases and backups protected by the key to become unavailable.

The database and infrastructure (the VM cluster or DB system) must be in an “Available” state for a backup operation to run successfully. Oracle recommends that you avoid performing actions that could interfere with availability (such as patching operations) while a backup operation is in progress. If an automatic backup operation fails, the Database service retries the operation during the next day’s backup window. If an on-demand full backup fails, you can try the operation again when the Exadata Cloud Service instance and database availability are restored.

**Automatic Incremental Backups**

When you enable the Automatic Backup feature, the service creates daily incremental backups of the database to Object Storage. The first backup created is a level 0 backup. Then, level 1 backups are created every day until the next weekend. Every weekend, the cycle repeats, starting with a new level 0 backup.

**Backup Retention**

If you choose to enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The system automatically deletes your incremental backups at the end of your chosen retention period.

**Backup Scheduling**

The automatic backup process starts at any time during your daily backup window. You can optionally specify a 2-hour scheduling window for your database during which the automatic backup process will begin. There are 12 scheduling windows to choose from, each starting on an even-numbered hour (for example, one window runs from 4:00-6:00 AM, and the next from 6:00-8:00 AM). Backups jobs do not necessarily complete within the scheduling window.

The default backup window of 00:00 to 06:00 in the time zone of the Exadata Cloud Service instance's region is assigned to your database if you do not specify a window. Note that the default backup scheduling window is six hours long, while the windows you specify are two hours long.
**Note:**

- **Data Guard** - You can enable the Automatic Backup feature on a database with the standby role in a Data Guard association. However, automatic backups for that database will not be created until it assumes the primary role.
- **Retention Period Changes** - If you shorten your database’s automatic backup retention period in the future, existing backups falling outside the updated retention period are deleted by the system.
- **Object Storage Costs** - Automatic backups incur Object Storage usage costs.

**On-Demand Full Backups**

You can create a full backup of your database at any time.

**Standalone Backups**

When you terminate an Exadata Cloud Service instance, a database, all of its resources are deleted, along with any automatic backups. Full backups remain in Object Storage as standalone backups. You can use a standalone backup to create a new database.

**To configure automatic backups for a database**

When you create an Exadata Cloud Service instance, you can optionally enable automatic backups for the initial database. Use this procedure to enable or disable automatic backups after the database is created.

**Note:**

Databases in a security zone compartment must have automatic backups enabled. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system containing the database you want to configure:

   - **Cloud VM clusters (new resource model):** Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. In the list of databases, find the database for which you want to enable or disable automatic backups, and click its name to display database details. The details indicate whether automatic backups are enabled.
5. Click Configure Automatic Backups.
6. In the Configure Automatic Backups dialog, check or uncheck Enable Automatic Backup, as applicable. If you are enabling automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
7. Click Save Changes.

**To create an on-demand full backup of a database**

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system containing the database you want to back up:

   Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. In the list of databases, find the database for which you want to create an on-demand full backup and click its name to display database details.

5. Under Resources, click Backups.

   A list of backups is displayed.

6. Click Create Backup.

To delete full backups from Object Storage

Note:

You cannot explicitly delete automatic backups. Unless you terminate the database, automatic backups remain in Object Storage for 30 days, after which time they are automatically deleted.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.

2. Choose your Compartment.

3. Navigate to the cloud VM cluster or DB system containing the database backup you want to delete:

   Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. In the list of databases, find the database you are interested in and click its name to display database details.

5. Under Resources, click Backups.

   A list of backups is displayed.

6. Click the Actions icon (three dots) for the backup you are interested in, and then click Delete.

7. Confirm when prompted.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage database backups:

- ListBackups
- GetBackup
- CreateBackup
- DeleteBackup
- UpdateDatabase - To enable and disable automatic backups.

For the complete list of APIs for the Database service, see Database Service API.

What's Next?

See Recovering an Exadata Database from Object Storage on page 1328.

Managing Exadata Database Backups by Using bkup_api

You can use Exadata's backup utility, bkup_api, to back up databases on an Exadata Cloud Service instance to an existing bucket in the Oracle Cloud Infrastructure Object Storage service and to the local disk Fast Recovery Area.
For backups managed by Oracle Cloud Infrastructure, see Managing Exadata Database Backups on page 1320.

This topic explains how to:

• Create a backup configuration file that indicates the backup destination, when the backup should run, and how long backups are retained. If the backup destination is Object Storage, the file also contains the credentials to access the service.
• Associate the backup configuration file with a database. The database will be backed up as scheduled, or you can create an on-demand backup.

**Note:**
You must update the cloud-specific tooling on all the compute nodes in your Exadata Cloud Service instance before performing the following procedures. For more information, see Updating an Exadata Cloud Service Instance on page 1274.

**Prerequisites**

• The Exadata Cloud Service instance requires access to the Oracle Cloud Infrastructure Object Storage service. Oracle recommends using a service gateway with the VCN to enable this access. For more information, see Network Setup for Exadata Cloud Service Instances on page 1232. In that topic, pay particular attention to:
  • Service Gateway for the VCN on page 1237
  • Node Access to Object Storage: Static Route on page 1236
  • Backup egress rule: Allows access to Object Storage on page 1242
• An existing Object Storage bucket to use as the backup destination. You can use the Console or the Object Storage API to create the bucket. For more information, see Managing Buckets on page 3398.
• An auth token generated by Oracle Cloud Infrastructure. You can use the Console or the IAM API to generate the password. For more information, see Working with Auth Tokens.
• The user name specified in the backup configuration file must have tenancy-level access to Object Storage. An easy way to do this is to add the user name to the Administrators group. However, that allows access to all of the cloud services. Instead, an administrator should create a policy like the following that limits access to only the required resources in Object Storage for backing up and restoring the database:

```
Allow group <group_name> to manage objects in compartment <compartment_name> where target.bucket.name = '<bucket_name>'
Allow group <group_name> to read buckets in compartment <compartment_name>
```

For more information about adding a user to a group, see Managing Groups on page 2419. For more information about policies, see Getting Started with Policies on page 2135.

**Default Backup Configuration**

The backup configuration follows a set of Oracle best-practice guidelines:

• Full (level 0) backup of the database followed by rolling incremental (level 1) backups on a seven-day cycle (a 30-day cycle for the Object Storage destination).
• Full backup of selected system files.
• Automatic backups daily at a specific time set during the database deployment creation process.

Retention period:

• Both Object Storage and local storage: 30 days, with the 7 most recent days' backups available on local storage.
• Object Storage only: 30 days.
• Local storage only: Seven days.

Encryption:

• Both Object Storage and local storage: All backups to cloud storage are encrypted.
• Object Storage only: All backups to cloud storage are encrypted.
Managing Backups

To create a backup configuration file

**Important:**

The following procedure must be performed on the first compute node in the Exadata Cloud Service instance's VM cluster or DB system resource. To determine the first compute node, connect to any compute node as the grid user and execute the following command:

```
$ $ORACLE_HOME/bin/olsnodes -n
```

The first node has the number 1 listed beside the node name.

1. SSH to the first compute node in the VM cluster or DB system resource.

```bash
ssh -i <private_key_path> opc@<node_1_ip_address>
```

2. Log in as opc and then sudo to the root user.

```bash
login as: opc
[opc@dbsys ~]$ sudo su -
```

3. Create a new backup configuration file in `/var/opt/oracle/ocde/assistants/bkup/` as shown in the sample configuration file below. This example uses the file name `bkup.cfg`, but you can provide your own file name. The following file schedules a backup to both local storage and an existing bucket in Object Storage.

The parameters are described below this procedure.

```bash
[root@dbsys ~]$ cd /var/opt/oracle/ocde/assistants/bkup/
vi bkup.cfg
bkup_disk=yes
bkup_oss=yes
bkup_oss_url=https://swiftobjectstorage.<region>.oraclecloud.com/v1/ companyabc/DBBackups
bkup_oss_user=<oci_user_name>
bkup_oss_passwd=<password>
bkup_oss_recovery_window=7
bkup_daily_time=06:45
```

4. Change the permissions of the file.

```bash
[root@dbsys bkup]# chmod 600 bkup.cfg
```

5. Use the following command to install the backup configuration, configure the credentials, schedule the backup, and associate the configuration with a database name.

```bash
[root@dbsys bkup]# ./bkup -cfg bkup.cfg -dbname=<database_name>
```

The backup is scheduled via cron and can be viewed at `/etc/crontab`.

When the scheduled backup runs, you can check its progress with the following command.

```bash
[root@dbsys bkup]# /var/opt/oracle/bkup_api/bkup_api bkup_status
```

The backup configuration file parameters are described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bkup_disk=[yes</td>
<td>no]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bkup_oss=[yes</td>
<td>no]</td>
</tr>
<tr>
<td>bkup_oss_url=&lt;swift_url&gt;</td>
<td>Required if bkup_oss=yes. The Object Storage URL including the tenant and bucket you want to use. The URL is: <a href="https://swiftobjectstorage">https://swiftobjectstorage</a>.&lt;region_name&gt;.oraclecloud.com/v1/&lt;tenant&gt;/&lt;bucket&gt; where &lt;tenant&gt; is the lowercase tenant name (even if it contains uppercase characters) that you specify when signing in to the Console and &lt;bucket&gt; is the name of the existing bucket you want to use for backups.</td>
</tr>
<tr>
<td>bkup_oss_user=&lt;oci_user_name&gt;</td>
<td>Required if bkup_oss=yes. The user name for the Oracle Cloud Infrastructure user account. This is the user name you use to sign in to the Oracle Cloud Infrastructure Console. For example, <a href="mailto:jsmith@example.com">jsmith@example.com</a> for a local user or &lt;identity_provider&gt;/jsmith@example.com for a federated user. To determine which type of user you have, see the following topics: • Managing Users on page 2414 (for information on local users) • Federating with Identity Providers on page 2362 (for information on federated users) Note that the user must be a member of the Administrators group, as described in Prerequisites on page 1324.</td>
</tr>
<tr>
<td>bkup_oss_passwd=&lt;auth_token&gt;</td>
<td>Required if bkup_oss=yes. The auth token generated by using the Console or IAM API, as described in Prerequisites on page 1324. This is not the password for the Oracle Cloud Infrastructure user.</td>
</tr>
<tr>
<td>bkup_oss_recovery_window=n</td>
<td>Required if bkup_oss=yes. The number of days for which backups and archived redo logs are maintained in the Object Storage bucket. Specify 1 to 30 days.</td>
</tr>
<tr>
<td>bkup_daily_time=hh:mm</td>
<td>The time at which the daily backup is scheduled, specified in hours and minutes (hh:mm), in 24-hour format.</td>
</tr>
</tbody>
</table>

To create an on-demand backup

You can use the `bkup_api` utility to create an on-demand backup of a database.
1. SSH to the first compute node in the Exadata VM cluster or DB system resource.

   ```
   ssh -i <private_key_path> opc@<node_1_ip_address>
   ```

   To determine the first compute node, connect to any compute node as the `grid` user and execute the following command:

   ```
   $ $ORACLE_HOME/bin/olsnodes -n
   ```

   The first node has the number 1 listed beside the node name.

2. Log in as opc and then sudo to the root user.

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. You can let the backup follow the current retention policy, or you can create a long-term backup that persists until you delete it:

   - To create a backup that follows the current retention policy, enter the following command:

     ```
     # /var/opt/oracle/bkup_api/bkup_api bkup_start --dbname=<database_name>
     ```

   - To create a long-term backup, enter the following command:

     ```
     # /var/opt/oracle/bkup_api/bkup_api bkup_start --keep --dbname=<database_name>
     ```

4. Exit the root-user command shell and disconnect from the compute node:

   ```
   # exit
   $ exit
   ```

   By default, the backup is given a timestamp-based tag. To specify a custom backup tag, add the `--tag` option to the `bkup_api` command; for example, to create a long-term backup with the tag "monthly", enter the following command:

   ```
   # /var/opt/oracle/bkup_api/bkup_api bkup_start --keep --tag=monthly
   ```

   After you enter a `bkup_api bkup_start` command, the `bkup_api` utility starts the backup process, which runs in the background. To check the progress of the backup process, enter the following command:

   ```
   # /var/opt/oracle/bkup_api/bkup_api bkup_status --dbname=<database_name>
   ```

   To remove the backup configuration

   A backup configuration can contain the credentials to access the Object Storage bucket. For this reason, you might want to remove the file after successfully configuring the backup.

   ```
   [root@dbsys bkup]# rm bkup.cfg
   ```

   To delete a local backup

   To delete a backup of a database deployment on the Exadata Cloud Service instance, use the `bkup_api` utility.
1. Connect to the first compute node in your Exadata VM cluster or DB system resource as the opc user.
   To determine the first compute node, connect to any compute node as the grid user and execute the following command:

   ```bash
   $ $ORACLE_HOME/bin/olsnodes -n
   ```

   The first node has the number 1 listed beside the node name.

2. Start a root-user command shell:

   ```bash
   $ sudo -s#
   ```

3. List the available backups:

   ```bash
   # > /var/opt/oracle/bkup_api/bkup_api recover_list --dbname=<database_name>
   ```

   where dbname is the database name for the database that you want to act on.
   A list of available backups is displayed.

4. Delete the backup you want:

   ```bash
   # /var/opt/oracle/bkup_api/bkup_api bkup_delete --bkup=<backup-tag> --dbname=<database_name>
   ```

   where backup-tag is the tag of the backup you want to delete.

5. Exit the root-user command shell:

   ```bash
   # exit$
   ```

To delete a backup in Object Storage

Use the RMAN delete backup command to delete a backup from the Object Store.

What Next?

If you used Object Storage as a backup destination, you can display the backup files in your bucket in the Console on the Storage page, by selecting Object Storage.

You can manually restore a database backup by using the RMAN utility. For information about using RMAN, see the Oracle Database Backup and Recovery User's Guide for Release 18.1, 12.2, 12.1, or 11.2.

Recovering an Exadata Database from Object Storage

This topic explains how to recover an Exadata database from a backup stored in Object Storage by using the Console or the API. The Object Storage service is a secure, scalable, on-demand storage solution in Oracle Cloud Infrastructure. For information on backing up your databases to Object Storage, see Managing Exadata Database Backups on page 1320.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Using the Console

You can use the Console to restore the database from a backup in the Object Storage that was created by using the Console or the API. You can restore to the last known good state of the database, or you can specify a point in time or an existing System Change Number (SCN).
**Note:**

The list of backups you see in the Console does not include any unmanaged backups (backups created directly by using `bkup_api`).

## Restoring an Existing Database

**To restore a database**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the cloud VM cluster or DB system containing the database you want to restore:
   - **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. In the list of databases, find the database you want to restore, and click its name to display details about it.
5. Click **Restore**.
6. Select one of the following options, and click **Restore Database**:
   - **Restore to the latest:** Restores the database to the last known good state with the least possible data loss.
   - **Restore to the timestamp:** Restores the database to the timestamp specified.
   - **Restore to System Change Number (SCN):** Restores the database using the SCN specified. This SCN must be valid.

   **Tip:**
   
   You can determine the SCN number to use either by accessing and querying your database host, or by accessing any online or archived logs.

7. Confirm when prompted.

   If the restore operation fails, the database will be in a "Restore Failed" state. You can try restoring again using a different restore option. However, Oracle recommends that you review the RMAN logs on the host and fix any issues before reattempting to restore the database. These log files can be found in subdirectories of the `/var/opt/oracle/log` directory.

**To restore a database using a specific backup from Object Storage**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the cloud VM cluster or DB system containing the database you want to restore:
   - **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. In the list of databases, find the database you want to restore, and click its name to display details about it.
5. Under **Resources**, click **Backups**.

   A list of backups is displayed.
6. Click the Actions icon (three dots) for the backup you are interested in, and then click **Restore**.
7. Confirm when prompted.

## Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.
Use these API operations to recover a database:

- ListBackups
- GetBackup
- RestoreDatabase

For the complete list of APIs for the Database service, see Database Service API.

**Recovering an Exadata Database by Using RMAN**

If you backed up your Exadata database by using `bkup_api`, you can manually restore that database backup by using the Oracle Recovery Manager (RMAN) utility. For information about using RMAN, see the *Oracle Database Backup and Recovery User's Guide* for Release 18.1, 12.2, 12.1, or 11.2.

To restore an Exadata database from a managed backup, see Recovering an Exadata Database from Object Storage on page 1328.

**Creating Oracle Database Homes on an Exadata Cloud Service Instance**

You can add Oracle Database Homes (referred to as "Database Homes" in Oracle Cloud Infrastructure) to an existing Exadata Cloud Service instance by using the Oracle Cloud Infrastructure Console, the API, or the CLI.

A Database Home is a directory location on the Exadata database compute nodes that contains Oracle Database software binary files. Compute nodes are also referred to as virtual machines in the Oracle Cloud Infrastructure Console.

After you provision the Exadata Cloud Service instance, you can create one or more Database Homes in the instance, and add databases to any of the Database Homes.

You can also add and remove Database Homes, and perform other management tasks on a Database Home by using the dbaascli utility. For information and instructions, see Managing Oracle Database Homes Manually on page 1333.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

**Using the Console**

To create a new Database Home in an existing Exadata Cloud Service instance:

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to create the new Database Home on:

   - Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. Under Resources, click Database Homes.
   A list of Database Homes is displayed.
5. Click Create Database Home.
6. In the **Create Database Home** dialog, enter the following:

   - **Database Home display name**: The display name for the Database Home. Avoid entering confidential information.
   - **Database image**: Determines what Oracle Database version is used for the database. You can mix database versions on the DB system, but not editions. By default, the latest Oracle-published database software image is selected.

   Click **Change Database Image** to use an older Oracle-published image or a custom database software image that you have created in advance, then select an **Image Type**:

     - **Oracle Provided Database Software Images**: These images contain generally available versions of Oracle Database software.
     - **Custom Database Software Images**: These images are created by your organization and contain customized configurations of software updates and patches. Use the **Select a compartment** and **Select a Database version** selectors to limit the list of custom database software images to a specific compartment or Oracle Database software major release version.

   After choosing a software image, click **Select** to return to the Create Database dialog.

   - Click **Show Advanced Options** to specify advanced options for the Database Home.

     - **Tags**: If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

7. Click **Create**.

When the Database Home creation is complete, the status changes from Provisioning to Available.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the **CreateDbHome** API operation to create Database Homes.

For the complete list of APIs for the Database service, see **Database Service API**.

**Managing Oracle Database Homes on an Exadata Cloud Service Instance**

You can delete or view information about Oracle Database Homes (referred to as "Database Homes" in Oracle Cloud Infrastructure) by using the Oracle Cloud Infrastructure Console, the API, or the CLI.

For information on how to perform these tasks manually, see **Managing Oracle Database Homes Manually** on page 1333.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

For administrators: The policy in **Let database admins manage Oracle Cloud database systems** on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see **Getting Started with Policies** on page 2135 and **Common Policies** on page 2142. If you want to dig deeper into writing policies for databases, see **Details for the Database Service** on page 2240.

**Using the Console**

*To view information about a Database Home*

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Navigate to the cloud VM cluster or DB system containing the Database Home:

   **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. On the DB System Details page, under Resources, click **Database Homes**.

5. In the list of Database Homes, find the Database Home you are interested in, and then click its name to display details about it.

   **To delete a Database Home**

You cannot delete a Database Home that contains databases. You must first terminate the databases to empty the Database Home. See **To terminate a database** on page 1310 to learn how to terminate a database.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose your **Compartment**.

3. Navigate to the cloud VM cluster or DB system containing the Database Home you want to delete:

   **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. On the DB System Details page, under Resources, click **Database Homes**.

5. In the list of Database Homes, find the Database Home you want to delete, and then click its name to display details about it.

6. On the Database Home Details page, click **Delete**.

   If the Database Home contains databases, you will not be able to proceed. You must cancel the deletion, empty the Database Home as applicable, and then retry the deletion.

   **To manage tags for your Database Home**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose your **Compartment**.

3. Navigate to the cloud VM cluster or DB system containing the Database Home:

   **Cloud VM clusters (new resource model):** Under **Exadata at Oracle Cloud**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems:** Under Bare Metal, VM, and Exadata, click **DB Systems**. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. Under **Resources**, click **Database Homes**.

5. In the list of Database Homes, find the Database Home you want to administer.

6. Click the the Actions icon (three dots) on the row listing the Database Home, and then click **Add Tags**.

   For more information, see **Resource Tags** on page 211.

   **Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage Database Homes:

- **ListDbHomes**
- **GetDbHome**
- **DeleteDbHome**
Managing Oracle Database Homes Manually

This topic describes how to manage Oracle Database Homes (also called "Oracle Homes" or "Database Homes") by using the `dbaascli` utility.

An Oracle Database Home is a directory location on the compute nodes that contains Oracle Database binaries. Exadata Cloud Service instances enable multiple databases to share a set of Oracle Database binaries in a shared Oracle Home directory location.

For information on how to manage Database Homes by using the Oracle Cloud Infrastructure Console, the API, or the CLI, see Managing Oracle Database Homes on an Exadata Cloud Service Instance on page 1331.

Viewing Information About Oracle Homes

You can view information about Oracle Home directory locations by using the `dbhome info` subcommand of the `dbaascli` utility as follows.

1. Connect to a compute node as the `opc` user.
   For detailed instructions, see Connecting to an Exadata Cloud Service Instance on page 1269.
2. Start a root-user command shell:

   ```
   $ sudo -s
   #
   ```
3. Execute the `dbaascli` command with the `dbhome info` subcommand:

   ```
   # dbaascli dbhome info
   ```
4. When prompted, press Enter to view information about all Oracle Homes registered in your Exadata Cloud Service instance, or specify an Oracle Home name to view information only about that Oracle Home.
5. Exit the root-user command shell:

   ```
   # exit
   $```

Moving a Database to Another Oracle Home

Moving a database to another Oracle Home enables you to consolidate existing Oracle Homes and manage the storage that they consume. You can move a database to another Oracle Home by using the `database move` subcommand of the `dbaascli` utility as follows.

1. Connect to a compute node as the `opc` user.
   For detailed instructions, see Connecting to an Exadata Cloud Service Instance on page 1269.
2. Start a root-user command shell:

   ```
   $ sudo -s
   #
   ```
3. Ensure that all database instances associated with the database deployment are up and running.

   ```
   # dbaascli database status --dbname <dbname>
   ```

   In the preceding command, `<dbname>` specifies the name of the database that you want to check.
   Restart any database instances that are not running and open.
4. Execute the `dbaascli` command with the `database move` subcommand:

```
# dbaascli database move --dbname <dbname> --ohome <oracle_home>
```

In the preceding command:
- `<dbname>` — specifies the name of the database that you want to move.
- `<oracle_home>` — specifies the path to an existing Oracle Home directory location, which you want the specified database to use.

When performing a move operation to an Oracle Home with a different patch level, if the database is part of a Data Guard association, then ensure that you move the standby database to the new patchset before you move the primary database.

5. Exit the root-user command shell:

```
# exit
```

Creating an Oracle Home

You can create an Oracle Home directory location and software installation, without creating a database, by using the `dbhome create` subcommand of the `dbaascli` utility as follows.

1. Connect to a compute node as the opc user.
   
   For detailed instructions, see Connecting to an Exadata Cloud Service Instance on page 1269.

2. Start a root-user command shell:

```
$ sudo -s
#
```

3. Run the `dbaascli` command with the `dbhome create` subcommand:

```
# dbaascli dbhome create --version <software_version>
```

In the preceding command, `<software_version>` specifies an Oracle Database software version. For example, 19000, 18000, 12201, 12102, or 11204. The latest available bundle patch for the specified software version is automatically used.

To see information about Oracle Database software images that are available in your Exadata Cloud Service instance, including software version and bundle patch details, use the `dbaascli dbimage list` command.

When prompted, type `yes` to confirm that the installation is based on a local software image.

4. Exit the root-user command shell:

```
# exit
```

Deleting an Oracle Home

If an Oracle Home directory does not support any databases, you can delete it by using the `dbhome purge` subcommand of the `dbaascli` utility as follows.

1. Connect to a compute node as the opc user.

   For detailed instructions, see Connecting to an Exadata Cloud Service Instance on page 1269.

2. Start a root-user command shell:

```
$ sudo -s
#
```
3. Execute the dbaascli command with the dbhome purge subcommand:

```
# dbaascli dbhome purge
```

4. When prompted, enter:

- 1 — if you want to specify the Oracle Home name for the location being purged.
- 2 — if you want to specify the Oracle Home directory path for the location being purged.

5. When next prompted, enter the Oracle Home name or directory path for the location being purged.

If your entries are valid and the Oracle Home is not associated with a database, then the Oracle binaries are removed from the Oracle Home directory location and the associated metadata is removed from the system.

6. Exit the root-user command shell:

```
# exit
```

---

**Monitoring and Managing Exadata Storage Servers with ExaCLI**

The ExaCLI command line utility allows you to perform monitoring and management functions on Exadata storage servers in an Exadata Cloud Service instance. ExaCLI offers a subset of the commands found in the on-premises Exadata command line utility CellCLI. The utility runs on the database compute nodes in the Exadata Cloud Service instance.

See the [ExaCLI Command Reference](#) on page 1337 in this topic to learn what commands are available.

**Username and Password**

You need a username and password to connect to the Exadata Storage Server. On Exadata Cloud@Customer, the preconfigured user is `cloud_user_clustername`, where `clustername` is the name of the virtual machine (VM) cluster that is being used. You can determine the name of the VM cluster by running the following command as the `grid` user on any cluster node:

```
$ crsctl get cluster name
```

The password for `cloud_user_clustername` is initially set to the administration password that you specify when creating the starter database deployment on the VM cluster.

**Command Syntax**

For Exadata Storage Server targets, ExaCLI supports the same command syntax as CellCLI. Construct your commands using the syntax that follows. Note that the syntax example assumes you are the `opc` user on a compute node.

```
exacli -c [username@]remotehost[:port] [-l username] [--xml] [--cookie-jar filename] [-e {command | 'command; command' | @batchfile}]
```

**Example 1**

This example shows the user on an Exadata compute node issuing the command to log in to ExaCLI start an interactive ExaCLI session on a storage server:

```
[opc@exacs-node1 ~]$ exacli -l cloud_user_clustername -c 192.168.136.7
```

See [Connecting to a Storage Server with ExaCLI](#) for information on determining your storage server's IP address.

Once logged in, run additional commands as follows:

```
exacli cloud_user_clustername@192.168.136.7> LIST DATABASE
ASM
HRCDB
```
Example 2

This example shows a single command issued on a compute node that does the following:

- Connects to a storage server
- Performs a LIST action
- Exits the session (specified with the "-e" flag)

```
[opc@exacs-node1 ~]$ exacli -l cloud_user_clustername -c 192.168.136.7 --xml --cookie-jar -e list griddisk detail
```

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c [username@]remotehost</code> or <code>-connect [username@]remotehost[:port]</code></td>
<td>Specifies the remote node to which you want to connect. ExaCLI prompts for the user name if not specified.</td>
</tr>
<tr>
<td><code>-l username</code> or <code>-login-name username</code></td>
<td>Specifies the user name to log into the remote node. The preconfigured user is <code>cloud_user_clustername</code>.</td>
</tr>
<tr>
<td><code>--xml</code></td>
<td>Displays the output in XML format.</td>
</tr>
<tr>
<td><code>--cookie-jar [filename]</code></td>
<td>Specifies the filename of the cookie jar to use. If filename is not specified, the cookie is stored in a default cookie jar located at <code>HOME/.exacli/cookiejar</code>, where <code>HOME</code> is the home directory of the OS user running the ExaCLI command. The presence of a valid cookie allows the ExaCLI user to execute commands without requiring to login in subsequent ExaCLI sessions.</td>
</tr>
<tr>
<td><code>-e command</code> or <code>-e 'command[; command]'</code> or <code>-e @batchFile</code></td>
<td>Specifies either the ExaCLI commands to run or a batch file. ExaCLI exits after running the commands. If specifying multiple commands to run, enclose the commands in single quotes to prevent the shell from interpreting the semi-colon. Omit this option to start an interactive ExaCLI session.</td>
</tr>
<tr>
<td><code>--cert-proxy proxy[:port]</code></td>
<td>Specifies the proxy server to use when downloading certificates. If <code>port</code> is omitted, port 80 is used by default.</td>
</tr>
<tr>
<td><code>-n</code> or <code>--no-prompt</code></td>
<td>Suppresses prompting for user input.</td>
</tr>
</tbody>
</table>

Usage Notes

- Notes for the `--cookie-jar` option:
  - The user name and password are sent to the remote node for authentication. On successful authentication, the remote node issues a cookie (the login credentials) that is stored in the specified `filename` on the database.
node. If filename is not specified, the cookie is stored in a default cookie jar located at HOME/.exacli/cookiejar, where HOME is the home directory of the operating system user running the ExaCLI command. For the opc user, the home is /home/opc.

- The operating system user running the ExaCLI command is the owner of the cookie-jar file.
- A cookie jar can contain multiple cookies from multiple users on multiple nodes in parallel sessions.
- Cookies are invalidated after 24 hours.
- If the cookie is not found or is no longer valid, ExaCLI prompts for the password. The new cookie is stored in the cookie jar identified by filename, or the default cookie jar if filename is not specified.
- Even without the --cookie-jar option, ExaCLI still checks for cookies from the default cookie jar. However, if the cookie does not exist or is no longer valid, the new cookie will not be stored in the default cookie jar if the --cookie-jar option is not specified.

Notes for the -e option:

- ExaCLI exits after running the commands.
- If specifying multiple commands to run, be sure to enclose the commands in single quotes to prevent the shell from interpreting the semi-colon.
- The batch file is a text file that contains one or more ExaCLI commands to run.

Notes for the -n (--no-prompt) option:

- If ExaCLI needs additional information from the user, for example, if ExaCLI needs to prompt the user for a password (possibly because there were no valid cookies in the cookie-jar) or to prompt the user to confirm the remote node’s identity, then ExaCLI prints an error message and exits.

Connecting to a Storage Server with ExaCLI

To use ExaCLI on storage servers, you will need to know your target storage server's IP address. If you do not know the IP address of the node you want to connect to, you can find it by viewing the contents of the cellip.ora file.

The following example illustrates how to do so on the UNIX command line for a quarter rack system. (Note that a quarter rack has three storage cells, and each cell has two connections, so a total of six IP addresses are shown.)

```
[root@exacs-node1 ~]# cat /etc/oracle/cell/network-config/cellip.ora
cell="192.168.136.5;cell="192.168.136.6"
cell="192.168.136.7;cell="192.168.136.8"
cell="192.168.136.9;cell="192.168.136.10"
```

If you are connecting to a storage cell for the first time using ExaCLI, you may be prompted to accept an SSL certificate. The ExaCLI output in this case will look like the following:

```
[opc@exacs-node1 ~]$ exacli -l cloud_user_clustername -c 192.168.136.7 --cookie-jar
No cookies found for cloud_user_clustername@192.168.136.7
Password: *********
EXA-30016: This connection is not secure. You have asked ExaCLI to connect to cell 192.168.136.7 securely. The identity of 192.168.136.7 cannot be verified.
Got certificate from server:
C=US,ST=California,L=Redwood City,O=Oracle Corporation,OU=Oracle Exadata,CN=ed1cl03clu01-priv2.usdc2.oraclecloud.com
Do you want to accept and store this certificate? (Press y/n)
```

Accept the self-signed Oracle certificate by pressing "y" to continue using ExaCLI.

ExaCLI Command Reference

You can execute various ExaCLI commands to monitor and manage Exadata Storage Servers associated with your Oracle Cloud Infrastructure Exadata DB system. ExaCLI allows you to get up-to-date, real-time information about your Exadata Cloud Service.

Use the LIST command with the following services and objects:
• **ACTIVERQUEST** - Lists all active requests that are currently being served by the storage servers.

• **ALERTDEFINITION** - Lists all possible alerts and their sources for storage servers.

• **ALERTHISTORY** - Lists all alerts that have been issues for the storage servers.

• **CELL** - Used to list the details of a specific attribute of the storage servers or storage cells. The syntax is as follows: LIST CELL ATTRIBUTES A, B, C, with A, B, and C being attributes. To see all cell attributes, use the LIST CELL ATTRIBUTES ALL command.

• **CELLDISK** - Lists the attributes of the cell disks in the storage servers. Use the following syntax to list the cell disk details: LIST CELLDISK cell_disk_name DETAIL.

• **DATABASE** - Lists details of the databases. Uses the regular LIST command syntax: LIST DATABASE and LIST DATABASE DETAIL. You can also use this command to show an individual attribute with the following syntax: LIST DATABASE ATTRIBUTES NAME.

• **FLASHCACHE** - Lists the details of the Exadata system's flash cache. For this object, you can use the following syntax patterns: LIST FLASHCACHE DETAIL or LIST FLASHCACHE ATTRIBUTES attribute_name.

• **FLASHCACHECONTENT** - Lists the details of all objects in the flash cache, or the details of a specified object ID. To list all the details of all objects, use LIST FLASHCACHECONTENT DETAIL. To list details for a specific object, use a where clause as follows: LIST FLASHCACHECONTENT WHERE objectNumber=12345 DETAIL

  **Note:** To find the object ID of a specific object, you can query user_objects using the object's name to get the data_object_id of a partition or table.

• **FLASHLOG** - Lists the attributes for the Oracle Exadata Smart Flash Log.

• **GRIDDISK** - Lists the details of a particular grid disk. The syntax is similar to the CELLDISK command syntax. To view all attributes: LIST GRIDDISK grid_disk_name DETAIL. To view specified attributes of the grid disk: LIST GRIDDISK grid_disk_name ATTRIBUTES size, name.

• **IBPORT** - Lists details of the InfiniBand ports. Syntax is LIST IBPORT DETAIL.

• **IORMPROFILE** - Lists any IORM profiles that have been set on the storage servers. You can also refer back to the profile attribute on the DATABASE object if a database has an IORM profile on it. Syntax is LIST IORMPROFILE.

• **LUN** - The LUN (logical unit number) object returns the number and the detail of the physical disks in the storage servers. List the LUNs of the disks with LIST LUN. List the details of each LUN with LIST LUN lun_number DETAIL.

• **METRICCURRENT** - Lists the current metrics for a particular object type. Syntax is LIST METRICCURRENT WHERE objectType = 'CELLDISK'. This command also allows for sorting and results limits as seen in the following example:

  ```
  LIST METRICCURRENT attributes name, metricObjectName ORDER BY metricObjectName asc, name desc LIMIT 5
  ```

• **METRICDEFINITION** - Lists metric definitions for the object that you can then get details for. With the command LIST metricDefinition WHERE objectType=cell, you can get all the metrics for that object type. You can then use the metric definition object again to get details for one of those specific metrics just listed: LIST metricDefinition WHERE name= IORM_MODE DETAIL.

• **METRICHISTORY** - List metrics over a specified period of time. For example, with the command LIST METRICHISTORY WHERE ageInMinutes < 30, you can list all the metrics collected over the past 30 minutes. You can also use the predicate collectionTime to set a range from a specific time. Use collectionTime as shown in the follow example: LIST METRICHISTORY WHERE collectionTime > '2018-04-01T21:12:00-10:00'. The metric history object can also be used to see a specific metric using the object’s name (for example, LIST METRICHISTORY CT_FD_IO_RQ_SM) or with a "where" clause to get objects with similar attributes like name (for example, LIST METRICHISTORY WHERE name like 'CT_.*').

• **OFFLOADGROUP** - Lists the attributes for the offload group that are running on your storage servers. You can list all details for all groups with LIST OFFLOADGROUP DETAIL, or list the attributes for a specific group, as shown in the following example: LIST OFFLOADGROUP offloadgroup4. List specific attributes with LIST OFFLOADGROUP ATTRIBUTES name.

• **PHYSICALDISK** - Lists all physical disks. Use the results of LIST PHYSICALDISK to identify a specific disk for further investigation, then list the details of that disk using the command as follows: LIST PHYSICALDISK
To list the details of flash disks, use the command as follows:

```bash
LIST PHYSICALDISK FLASH_1_0 DETAIL
```

- **PLUGGABLEDATABASE** - Lists all PDBs. View the details of a specific PDB with

  ```bash
  LIST PLUGGABLEDATABASE pdb_name.
  ```

- **QUARANTINE** - Lists all SQL statements that you prevented from using Smart Scans. The syntax is

  ```bash
  LIST QUARANTINE DETAIL. You can also use a "where" clause on any of the available attributes.
  ```

Use the ExaCLI **CREATE, ALTER, DROP**, and **LIST** commands to act on the following Exadata Storage Server objects:

- **DIAGPACK** - Lists the diagnostic packages and their status in your Exadata system. The syntax is

  ```bash
  LIST DIAGPACK [DETAIL], with DETAIL being an optional attribute. Use CREATE DIAGPACK with the packStartTime attribute to gather logs and trace files into a single compressed file for downloading, as in the following example:
  ```

  ```bash
  CREATE DIAGPACK packStartTime=2019_12_15T00_00_00.
  ```

  You can also use the value "now" with packStartTime:

  ```bash
  CREATE DIAGPACK packStartTime=now
  ```

To download a diagnostic package, use

```bash
DOWNLOAD DIAGPACK package_name local_directory.
```

For example, the following command downloads a diagnostic package to the /tmp directory:

```bash
DOWNLOAD DIAGPACK cfclcx2647_diag_2018_06_03T00_44_24_1 /tmp
```

- **IORMPLAN** - You can List, create, alter, and drop IORM plans using ExaCLI. To see the details of all IORM plans, use

  ```bash
  LIST IORMPLAN DETAIL.
  ```

  You can also use the command to create and alter IORM plans, and to apply plans to storage servers.

**Example query: finding the object_id value of an object**

```bash
select object_name, data_object_id from user_objects where object_name = 'BIG_CENSUS';
```

<table>
<thead>
<tr>
<th>OBJECT_NAME</th>
<th>DATA_OBJECT_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIG_CENSUS</td>
<td>29152</td>
</tr>
</tbody>
</table>

**Using Oracle Data Guard with Exadata Cloud Service**

**Note:**

This procedure is only applicable to Exadata Cloud Service instances. To use Oracle Data Guard with bare metal and virtual machine DB systems, see Using Oracle Data Guard on page 1461.

This topic explains how to use the Oracle Cloud Infrastructure (OCI) Console or the API to manage Oracle Data Guard associations in your Exadata Cloud Service instances. This topic does not apply to Data Guard configurations created by accessing the host directly and setting up Oracle Data Guard manually.

When you use the Oracle Cloud Infrastructure Console or API to enable Oracle Data Guard for an Exadata Cloud Service database:

- The standby database is a physical standby.
- The peer databases (primary and standby) are:
  - in the same compartment
  - both Exadata system shapes
  - identical database versions
- You are limited to one standby database for each primary database.
- You must use Oracle-managed encryption keys.

To configure Oracle Data Guard between on-premises and OCI Exadata Cloud Service instances, or to configure your database with multiple standbys, you must access the database host directly and set up Oracle Data Guard manually.

For complete information on Oracle Data Guard, see the Data Guard Concepts and Administration documentation in the Oracle Help Center.
**Required IAM Service Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you are new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Prerequisites**

An Exadata Cloud Service Oracle Data Guard implementation requires two existing Exadata Cloud Service instances: one containing an existing database that is to be duplicated by Data Guard, and one that will house the new standby database by Data Guard. When enabling Data Guard, you can create a new Database Home on the standby Exadata instance to house the new standby database during the enable Data Guard operation. Alternately, you can choose to provision the standby database in an existing Database Home on the standby instance. For information on creating the required resources for the standby system, see the following topics:

- To create a cloud Exadata infrastructure resource on page 1245
- To create a cloud VM cluster resource on page 1246
- To create a new Database Home in an existing Exadata Cloud Service instance on page 1330

You can use a custom database software image that contains the necessary patches for your databases when creating a Database Home on either the primary or the standby Exadata instance. See Oracle Database Software Images on page 1567 for information on working with custom Oracle Database software images.

If you choose to provision a standby database in an existing Database Home, ensure that the target Database Home on the standby instance has all required patches that are in use for the primary database before you provision the standby database. See the following topics for more information on patching an existing Database Home:

- To patch the Oracle Database software in a Database Home (cloud VM cluster) on page 1286
- To patch the Oracle Database software in a Database Home (DB system) on page 1285

**Network Requirements**

Ensure that your environment meets the following network requirements:

- If you want to configure Oracle Data Guard across regions, then you must configure remote virtual cloud network (VCN) peering between the primary and standby databases. Networking is configured on the cloud VM cluster resource for systems using the new Exadata resource model, and on the DB system resource for system using the old resource model. See Remote VCN Peering (Across Regions) on page 3280.

  For Exadata Data Guard configurations, OCI supports the use of hub-and-spoke network topology for the VCNs within each region. This means that the primary and standby databases can each utilize a "spoke" VCN that passes network traffic to the "hub" VCN that has a remote peering connection. See Spoke-to-Spoke: Remote Peering with Transit Routing for information on setting up this network topology.

- To set up Oracle Data Guard within a single region, both Exadata Cloud Service instances must use the same VCN. When setting up Data Guard within the same region, Oracle recommends that the instance containing the standby database be in a different availability domain from the instance containing the primary database to improve availability and disaster recovery.

- Configure the ingress and egress security rules for the subnets of both Exadata Cloud Service instances in the Oracle Data Guard association to enable TCP traffic to move between the applicable ports. Ensure that the rules you create are stateful (the default).

  For example, if the subnet of the primary Exadata Cloud Service instance uses the source CIDR 10.0.0.0/24 and the subnet of the standby instance uses the source CIDR 10.0.1.0/24, then create rules as shown in the subsequent example.

  ```
  Note:
  The egress rules in the example show how to enable TCP traffic only for port 1521, which is a minimum requirement for Oracle Data Guard to
  ```
Database

If TCP traffic is already enabled for all destinations (0.0.0.0/0) on all of your outgoing ports, then you need not explicitly add these specific egress rules.

Security Rules for Subnet of Primary Exadata Cloud Service instance

**Ingress Rules:**

- Stateless: No
- Source: 10.0.1.0/24
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Allows: TCP traffic for ports: 1521

**Egress Rules:**

- Stateless: No
- Destination: 10.0.1.0/24
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Allows: TCP traffic for ports: 1521

Security Rules for Subnet of Standby Exadata Cloud Service instance

**Ingress Rules:**

- Stateless: No
- Source: 10.0.0.0/24
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Allows: TCP traffic for ports: 1521

**Egress Rules:**

- Stateless: No
- Destination: 10.0.0.0/24
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Allows: TCP traffic for ports: 1521

For information about creating and editing rules, see Security Lists on page 2850.

**Password Requirements**

For Oracle Data Guard operations to work, the SYS password and the TDE wallet password of the primary and standby databases must all be the same. If you change any one of these passwords, then you must update the rest of the passwords to match. See Changing the Database Passwords on page 1312 to learn how to change the SYS password or the TDE wallet password.

If you make any change to the TDE wallet (such as adding a master key for a new PDB or changing the wallet password), then you must copy the wallet from the primary database to the standby database so that Oracle Data Guard can continue to operate. For Oracle Database versions prior to Oracle Database 12c release 2 (12.2), if you change the SYS password on one of the peers, then you must manually sync the password file between the DB systems.
Working with Oracle Data Guard

Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data. The Oracle Cloud Infrastructure Database Data Guard implementation requires two databases: one in a primary role and one in a standby role. The two databases compose an Oracle Data Guard association. Most of your applications access the primary database. The standby database is a transactionally consistent copy of the primary database.

Oracle Data Guard maintains the standby database by transmitting and applying redo data from the primary database. If the primary database becomes unavailable, then you can use Oracle Data Guard to switch or failover the standby database to the primary role.

Switchover

A switchover reverses the primary and standby database roles. Each database continues to participate in the Oracle Data Guard association in its new role. A switchover ensures no data loss. Performing planned maintenance on an Exadata Cloud Service instance with an Oracle Data Guard association is typically done by switching the primary database to the standby role, performing maintenance on the standby database, and then switching the standby database back to the primary role.

Failover

A failover transitions the standby database into the primary role after the existing primary database fails or becomes unreachable. A failover might result in some data loss when you use Maximum Performance protection mode.

Reinstate

Reinstates a database into the standby role in an Oracle Data Guard association. You can use the reinstate command to return a failed database into service after correcting the cause of failure.

Note:

You cannot terminate a primary database that has an Oracle Data Guard association with a peer (standby) database. Delete the standby database first. Alternatively, you can switch over the primary database to the standby role, and then terminate it.

You cannot terminate an Exadata cloud VM cluster or DB system that includes Oracle Data Guard-enabled databases. You must first remove the Oracle Data Guard association by terminating the standby database.

Using the Console

Use the Console to enable an Oracle Data Guard association between databases, change the role of a database in an Oracle Data Guard association using either a switchover or a failover operation, and reinstate a failed database.

When you enable Oracle Data Guard, a separate Oracle Data Guard association is created for the primary and the standby database.

To enable Oracle Data Guard on an Exadata Cloud Service instance

Note:

If you use customer-managed encryption keys to protect this database, then enabling Oracle Data Guard for this database is not available.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the Compartment that contains the Exadata Cloud Service instance with the database for which you want to enable Oracle Data Guard.
3. Navigate to the cloud VM cluster or DB system that contains a database you want to assume the primary role:

*Cloud VM clusters (new resource model)*: Under *Exadata at Oracle Cloud*, click *Exadata VM Clusters*. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

*DB systems*: Under Bare Metal, VM, and Exadata, click *DB Systems*. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. On the VM cluster or DB system details page, in the *Databases* section, click the name of the database you want to make primary.

5. On the Database Details page, in the *Resources* section, click *Data Guard Associations*.

6. In the *Data Guard Associations* section, click *Enable Data Guard*.

7. On the *Enable Data Guard* page, configure the Oracle Data Guard association.

   - The settings in the *Data Guard association details* section are read only and cannot be changed.

   - **Protection mode**: The protection mode used for this Oracle Data Guard association is set to *Maximum Performance*.
   - **Transport type**: The redo transport type used for this Oracle Data Guard association is set to *Async* (asynchronous).

   - In the *Select peer DB system* section, provide the following information for the standby database to obtain a list of available DB systems in which to locate the standby database:

     - **Region**: Select a region where you want to locate the standby database. The region where the primary database is located is selected, by default. You can choose to locate the standby database in a different region. The hint text associated with this field tells you in which region the primary database is located.
     - **Availability domain**: Select an availability domain for the standby database. The hint text associated with this field tells you in which availability domain the primary database is located.
     - **Shape**: Select the shape of the standby DB system. The shape must be an Exadata DB system shape.
     - **Data Guard peer resource type**: Select *DB System* or *VM Cluster*.

   - Select a DB system or cloud VM cluster from the drop-down list.

   - In the *Choose Database Home* section, choose one of the following:

     - **Select an existing Database Home**: If you use this option, select a home from the *Database Home display name* drop-down list.
     - **Create a new Database Home**: Use this option to provision a new Database Home for your Data Guard peer database.

   Click *Change Database Image* to use an older Oracle-published image or a custom database software image that you have created in advance, then select an *Image Type*:

     - **Oracle Provided Database Software Images**: These images contain generally available versions of Oracle Database software.
     - **Custom Database Software Images**: These images are *created by your organization* and contain customized configurations of software updates and patches. Use the *Select a compartment* and *Select a Database version* selectors to limit the list of custom database software images to a specific compartment or Oracle Database software major release version.

   - In the *Configure standby database* section, enter the database administrator password of the primary database in the *Database password* field. Use this same database administrator password for the standby database.

   **Note:**

   The administrator password and the TDE wallet password must be identical. If the passwords are not identical, then follow the instructions in *Changing the Database Passwords* on page 1312 to ensure that they are.
8. Click Enable Data Guard.

When you create the association, the details for a database and its peer display their respective roles as Primary or Standby.

To perform a database switchover

You initiate a switchover operation by using the Data Guard association of the primary database.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the Compartment that contains the Exadata Cloud Service instance with the database for which you want to enable Oracle Data Guard.
3. Navigate to the cloud VM cluster or DB system that contains the Data Guard association:

   Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. Under Resources, click Data Guard Associations.
5. For the Data Guard association on which you want to perform a switchover, click the Actions icon (three dots), and then click Switchover.
6. In the Switchover Database dialog box, enter the database admin password, and then click OK.

   This database should now assume the role of the standby, and the standby should assume the role of the primary in the Data Guard association.

To perform a database failover

You initiate a failover operation by using the Data Guard association of the standby database.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the Compartment that contains the Exadata Cloud Service instance with the database for which you want to enable Oracle Data Guard.
3. Navigate to the cloud VM cluster or DB system that contains the Data Guard association:

   Cloud VM clusters (new resource model): Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB systems: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. Under Resources, click Data Guard Associations.
5. For the Data Guard association on which you want to perform a failover, click Failover.
6. In the Failover Database dialog box, enter the database admin password, and then click OK.

   This database should now assume the role of the primary, and the old primary's role should display as Disabled Standby.

To reinstate a database

After you fail over a primary database to its standby, the standby assumes the primary role and the old primary is identified as a disabled standby. After you correct the cause of failure, you can reinstate the failed database as a functioning standby for the current primary by using its Data Guard association.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the Compartment that contains the Exadata Cloud Service instance with the database for which you want to enable Oracle Data Guard.
3. Navigate to the cloud VM cluster or DB system that contains the Data Guard association:

   **Cloud VM clusters (new resource model):** Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. Under Resources, click Data Guard Associations.

5. For the Data Guard association on which you want to reinstate this database, click the Actions icon (three dots), and then click Reinstate.

6. In the Reinstate Database dialog box, enter the database admin password, and then click OK.

   This database should now be reinstated as the standby in the Data Guard association.

To terminate a Data Guard association on an Exadata Cloud Service instance

On an Exadata Cloud Service instance, you remove a Data Guard association by terminating the standby database.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.

2. Choose the Compartment that contains the Exadata Cloud Service instance with the database for which you want to enable Oracle Data Guard.

3. Navigate to the cloud VM cluster or DB system that contains the standby database:

   **Cloud VM clusters (new resource model):** Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   **DB systems:** Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

4. For the standby database you want to terminate, click the Actions icon (three dots), and then click Terminate.

5. In the Terminate Database dialog box, enter the name of the database, and then click OK.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage Data Guard associations on an Exadata Cloud Service instance:

- CreateDataGuardAssociation
- GetDataGuardAssociation
- ListDataGuardAssociations
- SwitchoverDataGuardAssociation
- FailoverDataGuardAssociation
- ReinstateDataGuardAssociation
- DeleteDatabase - To terminate an Exadata Cloud Service instance Data Guard association, you delete the standby database.

For the complete list of APIs for the Database service, see Database Service API.

Configuring Oracle Database Features for Exadata Cloud Service

This topic describes how to configure Oracle Multitenant, tablespace encryption, and Huge Pages for use with your Exadata Cloud Service instance.

Using Oracle Multitenant on an Exadata Cloud Service Instance

When you create an Exadata Cloud Service instance that uses Oracle Database 12c or later, an Oracle Multitenant environment is created.

The multitenant architecture enables an Oracle database to function as a multitenant container database (CDB) that includes zero, one, or many pluggable databases (PDBs). A PDB is a portable collection of schemas, schema objects,
Database

and non-schema objects that appears to an Oracle Net Services client as a non-CDB. All Oracle databases using versions earlier than Oracle Database 12c are non-CDBs.

To use Oracle Transparent Data Encryption (TDE) in a pluggable database (PDB), you must create and activate a master encryption key for the PDB.

In a multitenant environment, each PDB has its own master encryption key which is stored in a single keystore used by all containers.

You must export and import the master encryption key for any encrypted PDBs you plug into your Exadata Cloud Service instance CDB.

If your source PDB is encrypted, you must export the master encryption key and then import it.

You can export and import all of the TDE master encryption keys that belong to the PDB by exporting and importing the TDE master encryption keys from within a PDB. Export and import of TDE master encryption keys support the PDB unplug and plug operations. During a PDB unplug and plug, all of the TDE master encryption keys that belong to a PDB, as well as the metadata, are involved.


See "ADMINISTER KEY MANAGEMENT" in Oracle Database SQL Language Reference for Release 19, 18, 12.2 or 12.1.

To determine if you need to create and activate an encryption key for the PDB

1. Invoke SQL*Plus and log in to the database as the SYS user with SYSDBA privileges.
2. Set the container to the PDB:

   ```sql
   SQL> ALTER SESSION SET CONTAINER = pdb;
   ```

3. Query V$ENCRYPTION_WALLET as follows:

   ```sql
   SQL> SELECT wrl_parameter, status, wallet_type FROM v$encryption_wallet;
   ```

   If the STATUS column contains a value of OPEN_NO_MASTER_KEY, you need to create and activate the master encryption key.

To create and activate the master encryption key in a PDB

1. Set the container to the PDB:

   ```sql
   SQL> ALTER SESSION SET CONTAINER = pdb;
   ```
2. Create and activate a master encryption key in the PDB by executing the following command:

```
SQL> ADMINISTER KEY MANAGEMENT SET KEY USING TAG 'tag' FORCE KEYSTORE IDENTIFIED BY keystore-password WITH BACKUP USING 'backup_identifier';
```

In the previous command:

- `keystore-password` is the keystore password. By default, the keystore password is set to the value of the administration password that is specified when the database is created.
- The optional `USING TAG 'tag'` clause can be used to associate a tag with the new master encryption key.
- The `WITH BACKUP` clause, and the optional `USING 'backup_identifier'` clause, can be used to create a backup of the keystore before the new master encryption key is created.

See also `ADMINISTER KEY MANAGEMENT` in *Oracle Database SQL Language Reference for Release 19, 18 or 12.2*.

**Note:**

To enable key management operations while the keystore is in use, Oracle Database 12c Release 2, and later, includes the `FORCE KEYSTORE` option to the `ADMINISTER KEY MANAGEMENT` command. This option is also available for Oracle Database 12c Release 1 with the October 2017, or later, bundle patch.

If your Oracle Database 12c Release 1 database does not have the October 2017, or later, bundle patch installed, you can perform the following alternative steps:

a. Close the keystore.
b. Open the password-based keystore.
c. Create and activate a master encryption key in the PDB by using `ADMINISTER KEY MANAGEMENT` without the `FORCE KEYSTORE` option.
d. Update the auto-login keystore by using `ADMINISTER KEY MANAGEMENT` with the `CREATE AUTO_LOGIN KEYSTORE FROM KEYSTORE` option.

3. Query `V$ENCRYPTION_WALLET` again to verify that the `STATUS` column is set to `OPEN`:

```
SQL> SELECT wrl_parameter, status, wallet_type FROM v$encryption_wallet;
```

4. Query `V$INSTANCE` and take note of the value in the `HOST_NAME` column, which identifies the database server that contains the newly updated keystore files:

```
SQL> SELECT host_name FROM v$instance;
```
5. Copy the updated keystore files to all of the other database servers.

To distribute the updated keystore, you must perform the following actions on each database server that does not contain the updated keystore files:

a. Connect to the root container and query \texttt{V$ENCRYPTION\_WALLET}. Take note of the keystore location contained in the \texttt{WRL\_PARAMETER} column:

\begin{verbatim}
SQL> SELECT wrl_parameter, status FROM v$encryption_wallet;
\end{verbatim}

b. Copy the updated keystore files.

You must copy all of the updated keystore files from a database server that is already updated. Use the keystore location observed in the \texttt{WRL\_PARAMETER} column of \texttt{V$ENCRYPTION\_WALLET}.

Open the updated keystore:

\begin{verbatim}
SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE open FORCE KEYSTORE IDENTIFIED BY keystore-password CONTAINER=all;
\end{verbatim}

\textbf{Note:}

To enable key management operations while the keystore is in use, Oracle Database 12c Release 2, and later, includes the \texttt{FORCE KEYSTORE} option to the \texttt{ADMINISTER KEY MANAGEMENT} command. This option is also available for Oracle Database 12c Release 1 with the October 2017, or later, bundle patch.

If your Oracle Database 12c Release 1 database does not have the October 2017, or later, bundle patch installed, you can perform the following alternative steps:

a. Close the keystore before copying the updated keystore files.

b. Copy the updated keystore files.

c. Open the updated keystore by using \texttt{ADMINISTER KEY MANAGEMENT} without the \texttt{FORCE KEYSTORE} option.

6. Query \texttt{GV$ENCRYPTION\_WALLET} to verify that the \texttt{STATUS} column is set to \texttt{OPEN} across all of the database instances:

\begin{verbatim}
SQL> SELECT wrl_parameter, status, wallet_type FROM gv$encryption_wallet;
\end{verbatim}

\textbf{To export and import a master encryption key}

1. Export the master encryption key.

a. Invoke SQL*Plus and log in to the PDB.

b. Execute the following command:

\begin{verbatim}
SQL> ADMINISTER KEY MANAGEMENT EXPORT ENCRYPTION KEYS WITH SECRET "secret" TO 'filename' IDENTIFIED BY keystore-password;
\end{verbatim}

2. Import the master encryption key.

a. Invoke SQL*Plus and log in to the PDB.

b. Execute the following command:

\begin{verbatim}
SQL> ADMINISTER KEY MANAGEMENT IMPORT ENCRYPTION KEYS WITH SECRET "secret" FROM 'filename' IDENTIFIED BY keystore-password;
\end{verbatim}

\textbf{Managing Tablespace Encryption}

By default, all new tablespaces that you create in an Exadata database are encrypted.
However, the tablespaces that are initially created when the database is created may not be encrypted by default.

- For databases that use Oracle Database 12c Release 2 or later, only the USERS tablespaces initially created when the database was created are encrypted. No other tablespaces are encrypted including the non-USERS tablespaces in:
  - The root container (CDB$ROOT).
  - The seed pluggable database (PDB$SEED).
  - The first PDB, which is created when the database is created.
- For databases that use Oracle Database 12c Release 1 or Oracle Database 11g, none of the tablespaces initially created when the database was created are encrypted.

For further information about the implementation of tablespace encryption in Exadata, along with how it impacts various deployment scenarios, see Oracle Database Tablespace Encryption Behavior in Oracle Cloud.

Creating Encrypted Tablespaces

User-created tablespaces are encrypted by default.

By default, any new tablespaces created by using the SQL CREATE TABLESPACE command are encrypted with the AES128 encryption algorithm. You do not need to include the USING 'encrypt_algorithm' clause to use the default encryption.

You can specify another supported algorithm by including the USING 'encrypt_algorithm' clause in the CREATE TABLESPACE command. Supported algorithms are AES256, AES192, AES128, and 3DES168.

Managing Tablespace Encryption

You can manage the software keystore (known as an Oracle wallet in Oracle Database 11g), the master encryption key, and control whether encryption is enabled by default.

Managing the Master Encryption Key

Tablespace encryption uses a two-tiered, key-based architecture to transparently encrypt (and decrypt) tablespaces. The master encryption key is stored in an external security module (software keystore). This master encryption key is used to encrypt the tablespace encryption key, which in turn is used to encrypt and decrypt data in the tablespace.

When a database is created on an Exadata Cloud Service instance, a local software keystore is created. The keystore is local to the compute nodes and is protected by the administration password specified during the database creation process. The auto-login software keystore is automatically opened when the database is started.

You can change (rotate) the master encryption key by using the ADMINISTER KEY MANAGEMENT SQL statement. For example:

```
SQL> ADMINISTER KEY MANAGEMENT SET ENCRYPTION KEY USING TAG 'tag'
       IDENTIFIED BY password WITH BACKUP USING 'backup';
keystore altered.
```


Controlling Default Tablespace Encryption

The ENCRYPT_NEW_TABLESPACES initialization parameter controls the default encryption of new tablespaces. In Exadata databases, this parameter is set to CLOUD_ONLY by default.

Values of this parameter are as follows.
### Database

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALWAYS</td>
<td>During creation, tablespaces are transparently encrypted with the AES128 algorithm unless a different algorithm is specified in the ENCRYPTION clause.</td>
</tr>
<tr>
<td>CLOUDONLY</td>
<td>Tablespace created in an Exadata database are transparently encrypted with the AES128 algorithm unless a different algorithm is specified in the ENCRYPTION clause. For non-cloud databases, tablespaces are only encrypted if the ENCRYPTION clause is specified. ENCRYPTION is the default value.</td>
</tr>
<tr>
<td>DDL</td>
<td>During creation, tablespaces are not transparently encrypted by default, and are only encrypted if the ENCRYPTION clause is specified.</td>
</tr>
</tbody>
</table>

**Note:**

With Oracle Database 12c Release 2 (12.2), or later, you can no longer create an unencrypted tablespace in an Exadata database. An error message is returned if you set ENCRYPT_NEW_TABLESPACES to DDL and issue a CREATE TABLESPACE command without specifying an ENCRYPTION clause.

### Managing Huge Pages

Huge Pages provide considerable performance benefits for Oracle Database on systems with large amounts of memory. Oracle Database on an Exadata Cloud Service instance hosted in Oracle Cloud Infrastructure provides configuration settings that make use of Huge Pages by default; however, you can make manual adjustments to optimize the configuration of Huge Pages.

Huge Pages is a feature integrated into the Linux kernel 2.6. Enabling Huge Pages makes it possible for the operating system to support large memory pages. Using Huge Pages can improve system performance by reducing the amount of system CPU and memory resources required to manage Linux page tables, which store the mapping between virtual and physical memory addresses. For Oracle Databases, using Huge Pages can drastically reduce the number of page table entries associated with the System Global Area (SGA).

On Exadata Cloud Service instances hosted in Oracle Cloud Infrastructure, a standard page is 4 KB, while a Huge Page is 2 MB by default. Therefore, an Oracle Database on an Exadata DB system with a 50 GB SGA requires 13,107,200 standard pages to house the SGA, compared with only 25,600 Huge Pages. The result is much smaller page tables, which require less memory to store and fewer CPU resources to access and manage.

### Adjusting the Configuration of Huge Pages

The configuration of Huge Pages for Oracle Database is a two-step process:

- At the operating system level, the overall amount of memory allocated to Huge Pages is controlled by the `vm.nr_hugepages` entry in the `/etc/sysctl.conf` file. This setting is made on each compute node in the environment and it is strongly recommended that the setting is consistent across all of the compute nodes. To alter the Huge Page allocation, you can execute the following command on each compute node as the root user:

  ```
  # sysctl -w vm.nr_hugepages=value
  
  where value is the number of Huge Pages that you want to allocate.
  ```

On Exadata Cloud Service instances hosted in Oracle Cloud Infrastructure, each Huge Page is 2 MB by default. Therefore, to allocate 50 GB of memory to Huge Pages you can execute the following command:

```
# sysctl -w vm.nr_hugepages=25600
```
At the Oracle Database level, the use of Huge Pages is controlled by the `USE_LARGE_PAGES` instance parameter setting. This setting applies to each database instance in a clustered database. Oracle strongly recommends a consistent setting across all of the database instances associated with a database. The following options are available:

- **TRUE** — specifies that the database instance can use Huge Pages if they are available. For all versions of Oracle Database after 11.2.0.3, Oracle allocates as much of the SGA as it can, using Huge Pages. When the Huge Page allocation is exhausted, standard memory pages are used.
- **FALSE** — specifies that the database instance does not use Huge Pages. This setting is generally not recommended if Huge Pages are available.
- **ONLY** — specifies that the database instance must use Huge Pages. With this setting, the database instance fails to start if the entire SGA cannot be accommodated in Huge Pages.

If you make any adjustments at either the operating system or Oracle Database level, ensure that the overall configuration works.

For more information, see the *Oracle Database Administrator's Reference for Linux and UNIX-Based Operating Systems* for Release 19, 18, 12.1, or 11.2 for a general overview of Huge Pages and more information about configuring Huge Pages. Also, see `USE_LARGE_PAGES` in the *Oracle Database Reference* for Release 12.2, 12.1, or 11.2.

### Exadata Fixed Hardware Shapes: X6, X7, X8 and Exadata Base

This topic describes the available fixed-size Exadata Cloud Service hardware shapes in Oracle Cloud Infrastructure.

**Note:**

For information on the flexible X8M shape, see [Overview of X8M Scalable Exadata Infrastructure](#) on page 1227.

Exadata X8 shapes:

- **Exadata.Quarter3.100**: Provides a 2-node Exadata DB system with up to 100 CPU cores, and 149 TB of usable storage.
- **Exadata.Half3.200**: Provides a 4-node Exadata DB system with up to 200 CPU cores, and 299 TB of usable storage.
- **Exadata.Full3.400**: Provides an 8-node Exadata DB system with up to 400 CPU cores, and 598 TB of usable storage.

Exadata X7 shapes:

- **Exadata.Quarter2.92**: Provides a 2-node Exadata DB system with up to 92 CPU cores, and 106 TB of usable storage.
- **Exadata.Half2.184**: Provides a 4-node Exadata DB system with up to 184 CPU cores, and 212 TB of usable storage.
- **Exadata.Full2.368**: Provides an 8-node Exadata DB system with up to 368 CPU cores, and 424 TB of usable storage.

Exadata X6 shapes:

- **Exadata.Quarter1.84**: Provides a 2-node Exadata DB system with 22 enabled CPU cores, with up to 62 additional CPU cores, and 84 TB of usable storage.
- **Exadata.Half1.168**: Provides a 4-node Exadata DB system with 44 enabled CPU cores, with up to 124 additional CPU cores, and 168 TB of usable storage.
- **Exadata.Full1.336**: Provides an 8-node Exadata DB system with 88 enabled CPU cores, with up to 248 additional CPU cores, and 336 TB of usable storage.

Exadata base system:

- **Exadata.Base.48**: Provides a 2-node Exadata DB system with up to 48 CPU cores, and 74 TB of usable storage.
All Exadata shapes provide unlimited I/O, and support only Enterprise Edition - Extreme Performance. All Exadata shapes provide 720 GB RAM per node except for Exadata base systems, which provide 360 GB RAM per node. For more details about Exadata shapes, see Exadata Shape Configurations on page 1223.

For information on provisioning an Exadata Cloud Service instance, see Creating an Exadata Cloud Service Instance on page 1243.

**The X8M Virtual Machine File System Structure**

Exadata Cloud Service X8M systems use the following file system organization on the virtual machine nodes.

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Mounted On</th>
</tr>
</thead>
<tbody>
<tr>
<td>devtmpfs</td>
<td>/dev</td>
</tr>
<tr>
<td>tmpfs</td>
<td>/dev/shm</td>
</tr>
<tr>
<td>tmpfs</td>
<td>/run</td>
</tr>
<tr>
<td>tmpfs</td>
<td>/sys/fs/cgroup</td>
</tr>
<tr>
<td>tmpfs</td>
<td>/run/user/0</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDb-LVDbSys1</td>
<td>/</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDb-LVDbOra1</td>
<td>/u01</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDb-LVDbTmp</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDb-LVDbVar1</td>
<td>/var</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDb-LVDbVarLog</td>
<td>/var/log</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDb-LVDbHome</td>
<td>/home</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDbDisk.u02_extra.img-LVDBDisk</td>
<td>/u02</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDbDisk.varLogAudit</td>
<td>/var/log/audit</td>
</tr>
<tr>
<td>/dev/sda1</td>
<td>/boot</td>
</tr>
<tr>
<td>/dev/mapper/VGExaDbDisk.grid19.0.0.0.200414.img-LVDBDisk</td>
<td>/u01/app/19.0.0.0/grid</td>
</tr>
<tr>
<td>/dev/asm/acfsvol01-142</td>
<td>/acfs01</td>
</tr>
</tbody>
</table>

**Bare Metal and Virtual Machine DB Systems**

Oracle Cloud Infrastructure offers single-node DB systems on either bare metal or virtual machines, and 2-node RAC DB systems on virtual machines. If you need to provision a DB system for development or testing purposes, a special fast-provisioning single-node virtual machine system is available.

You can manage these systems by using the Console, the API, the Oracle Cloud Infrastructure CLI, the Database CLI (DBCLI), Enterprise Manager, Enterprise Manager Express, or SQL Developer.

**Note:**

This documentation is intended for Oracle database administrators and assumes familiarity with Oracle databases and tools. If you need additional information, see the product documentation available at [http://docs.oracle.com/en/database/](http://docs.oracle.com/en/database/).
Supported Database Editions and Versions

All single-node Oracle RAC DB systems support the following Oracle Database editions:

- Standard Edition
- Enterprise Edition
- Enterprise Edition - High Performance
- Enterprise Edition - Extreme Performance

Two-node Oracle RAC DB systems require Oracle Enterprise Edition - Extreme Performance.

For standard provisioning of DB systems (using Oracle Automatic Storage Management (ASM) as your storage management software), the supported database versions are:

- Oracle Database 21c
- Oracle Database 19c
- Oracle Database 18c (18.0)
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1)
- Oracle Database 11g Release 2 (11.2)

For fast provisioning of single-node virtual machine database systems (using Logical Volume Manager as your storage management software), the supported database versions are:

- Oracle Database 21c
- Oracle Database 19c
- Oracle Database 18c

**Tip:**

Your DB system's operating system will periodically need to be updated, just as your Oracle Database software will need to be updated. Before attempting an OS update, be sure to read the information in Updating a DB System on page 1397 and back up your DB system's databases.

Upgrading the Oracle Database Software in Your DB System

You can upgrade database instances that use Oracle Database 18c and earlier to Oracle Database 19c (Long Term Release). For information on prerequisites and upgrade instructions see Upgrading a Database on page 1424.

Oracle Database Preview Version Availability

Oracle Cloud Infrastructure periodically offers preview software versions of Oracle Database for testing purposes. You can provision a virtual machine DB system using preview version software to test applications before the general availability of the software in the Database service. When you provision a DB system with preview version software, the system remains available to you until you decide to terminate it.

Preview version DB systems are provisioned in the same manner as non-preview systems. If available, preview version software is displayed as one of the choices in the Database version selector in the Create DB System dialog. See To create a DB system on page 1372 for instructions on provisioning a virtual machine DB system using preview version software.

**Current Preview Version Software**

There is no Oracle Database preview software version available at this time for bare metal and virtual machine DB systems in Oracle Cloud Infrastructure.

**Oracle Database Preview Version Restrictions**

Preview version software cannot be used for production databases. The following restrictions apply to preview version software:
• Only available for non-RAC virtual machine DB systems. Preview software is not available for bare metal systems, Exadata systems, or virtual machine systems using RAC.
• Uses Logical Volume Manager (LVM) storage management software only. Automatic Storage Management (ASM) is not available.
• Patching and database version upgrades (including upgrades to the generally available release of the preview software) are not available.
• You cannot create a new DB system from a backup of a database that uses preview version software.
• Standalone backups cannot be created.
• Data Guard is not available.
• Preview version software DB systems cannot be created from backups. In-place restores are supported.

Availability of Older Database Versions for Virtual Machine DB Systems

For virtual machine DB systems, Oracle Cloud Infrastructure also supports the creation of DB systems using older database versions. For each shape, the latest version and the two prior versions of the release are available at provisioning.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
</table>

If you need to launch your DB system with an older database version, see Critical Patch Updates for information on known security issues with your chosen database version. You will also need to analyze and patch known security issues for the operating system included with the older database version. See Securing Database on page 3685 for information on security best practices for databases in Oracle Cloud Infrastructure.

Per-Second Billing for Bare Metal and Virtual Machine Database Resources

For databases using bare metal and virtual machine infrastructure, Oracle Cloud Infrastructure uses per-second billing. This means that OCPU and storage usage is billed by the second, with a minimum usage period of 1 minute for virtual machine DB systems and 1 hour for bare metal DB systems.

Bare Metal DB Systems

Bare metal DB systems consist of a single bare metal server running Oracle Linux 6.8, with locally attached NVMe storage. If the node fails, you can simply launch another system and restore the databases from current backups.

When you launch a bare metal DB system, you select a single Oracle Database edition that applies to all the databases on that DB system. The selected edition cannot be changed. Each DB system can have multiple database homes, which can be different versions. Each database home can have only one database, which is the same version as the database home.

Shapes for Bare Metal DB Systems

When you launch a DB system, you choose a shape, which determines the resources allocated to the DB system. The available shapes for a bare metal DB system are:

• **BM.DenseIO2.52:** Provides a 1-node DB system (one bare metal server), with up to 52 CPU cores, 768 GB memory, and eight 6.4 TB locally attached NVMe drives (51.2 TB total) to the DB system.

• **BM.DenseIO1.36:** Limited availability. Provides a 1-node DB system (one bare metal server), with up to 36 CPU cores, 512 GB memory, and nine 3.2 TB locally attached NVMe drives (28.8 TB total) to the DB system.

*Note:* BM.DenseIO1.36 is available only to monthly universal credit customers existing on or before November 9th, 2018. This shape is available only in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.
Bare Metal DB System Storage Considerations

The shape you choose for a bare metal DB system determines its total raw storage, but other options, like 2- or 3-way mirroring and the space allocated for data files, affect the amount of usable storage on the system. The following table shows how various configurations affect the usable storage for bare metal DB systems.

<table>
<thead>
<tr>
<th>Shape</th>
<th>Raw Storage</th>
<th>Usable Storage with Normal Redundancy (2-way Mirroring)</th>
<th>Usable Storage with High Redundancy (3-way Mirroring)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BM.DenseIO2.52</td>
<td>51.2 TB NVMe</td>
<td>DATA 16 TB, RECO 4 TB</td>
<td>DATA 9 TB, RECO 2.3 TB</td>
</tr>
<tr>
<td>BM.DenseIO1.36</td>
<td>28.8 TB NVMe</td>
<td>DATA 9.4 TB, RECO 1.7 TB</td>
<td>DATA 5.4 TB, RECO 1 TB</td>
</tr>
</tbody>
</table>

Note: BM.DenseIO1.36 availability is limited to monthly universal credit customers existing on or before November 9th, 2018, in the us-phoenix-1, us-ashburn-1, and eu-frankfurt-1 regions.

Virtual Machine DB Systems

There are two types of DB systems on virtual machines:

- A 1-node virtual machine DB system consists of one virtual machine.
- A 2-node virtual machine DB system consists of two virtual machines.

When you launch a virtual machine DB system, you select the Oracle Database edition and version that applies to the database on that DB system. The selected edition cannot be changed. Depending on your selected Oracle Database edition and version, your DB system can support multiple pluggable databases (PDBs). See the following Oracle Database licensing topics for information about the maximum number of pluggable and container databases available for your selected Oracle Database version:

- Oracle Database 18c: Permitted Features, Options, and Management Packs by Oracle Database Offering
- Oracle Database 19c: Permitted Features, Options, and Management Packs by Oracle Database Offering

Unlike a bare metal DB system, a virtual machine DB system can have only a single Database Home, which in turn can have only a single database. The databases will be the same version as the Database Home.

Virtual machine DB systems also differ from bare metal DB systems in the following ways:

- A virtual machine DB system database uses Oracle Cloud Infrastructure block storage instead of local storage. You specify a storage size when you launch the DB system, and you can scale up the storage as needed at any time.
- To change the number of CPU cores on an existing virtual machine DB system, you must change the shape of that DB system. See To change the shape of a virtual machine DB system on page 1384 for more information.

Note:
The shape-changer operation takes place in a rolling fashion for multi-node DB systems, allowing you to change the shape with no database downtime.

Fast Provisioning Option for Single-Node Virtual Machine DB Systems

For 1-node virtual machine DB systems, Oracle Cloud Infrastructure provides have a "fast provisioning" option that allows you to create your DB system using Logical Volume Manager as your storage management software. The alternative ("standard provisioning") is to provision with Oracle Automatic Storage Management (ASM).

Note:
- When using the fast provisioning option, the number and size of the block volumes specified during provisioning determines the maximum total

- Multi-node Virtual Machine DB systems require Oracle Automatic Storage Management and cannot be created using the fast-provisioning option.
- You can clone virtual machine DB systems that have been created using the fast provision option. See Cloning a Virtual Machine DB System on page 1388 for instructions.
- You cannot use a custom database software image when provisioning a system with logical volume manager storage software.

Cloning a Fast-Provisioned Virtual Machine DB System

You can create a clone of a virtual machine DB system that was created using the "fast provisioning" option (these are single-node systems that use Logical Volume Manager storage management software). For more information and instructions, see Cloning a Virtual Machine DB System on page 1388.

Fault Domain Considerations for Two-Node Virtual Machine DB Systems

When you provision a 2-node RAC DB systems, the system assigns each node to a different fault domain by default. Using the Advanced Options link in the provisioning dialog, you can select the fault domain(s) to be used for your 2-node RAC DB systems and the system will assign the nodes to your selected fault domains. Oracle recommends that you place each node of a 2-node RAC DB system in a different fault domain. For more information on fault domains, see Fault Domains on page 182.

Rebooting a Virtual Machine DB System Node for Planned Maintenance

Virtual machine DB system nodes use underlying physical hosts that periodically need to undergo maintenance. When such maintenance is needed, Oracle Cloud Infrastructure schedules a reboot of your virtual machine DB system node and notifies you of the upcoming reboot. The reboot allows your virtual machine DB system node to be migrated to a new physical host which is not in need of maintenance. (Stopping and starting the node will also result in the migration to a new physical host.) The only impact to your virtual machine DB system node is the reboot itself. The planned maintenance of the original physical hardware takes place after your node has been migrated to its new host, and has no impact on your DB system.

If your virtual machine DB system node is scheduled for a maintenance reboot, you can proactively reboot your node (by stopping and starting it) using the Console or the API. This lets you control how and when your node experiences downtime. If you choose not to reboot before the scheduled time, then Oracle Cloud Infrastructure will reboot and migrate your node at the scheduled time.

To identify the virtual machine DB system nodes that you can proactively reboot, navigate to your system's DB System Details page in the Console and check the Node Maintenance Reboot field. If the instance has a maintenance reboot scheduled and can be proactively rebooted, this field displays the date and start time for the reboot. When the Maintenance Reboot field does not display a date, your virtual machine DB system has no scheduled node maintenance events.

To check for scheduled maintenance events using the API, use the GetDbNode operation to check the timeMaintenanceWindowEnd field of the DbNode resource. This field specifies when the system will initiate the next scheduled node reboot.

To make it easier to locate nodes that have scheduled maintenance reboots, you can use the Search service with a predefined query to find all DB systems that have a maintenance reboot scheduled.

For instructions on using the Console to reboot a node, see To start, stop, or reboot a database system on page 1383.

Shapes for Virtual Machine DB Systems

When you launch a virtual machine DB system, you choose a shape, which determines the resources allocated to the DB system. After you provision the system, you can change the shape to adapt to new processing capacity requirements.

The following table shows the available shapes in the X7 series for a virtual machine DB system.
## Database

<table>
<thead>
<tr>
<th>Shape</th>
<th>CPU Cores</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard2.1</td>
<td>1</td>
<td>15 GB</td>
</tr>
<tr>
<td>VM.Standard2.2</td>
<td>2</td>
<td>30 GB</td>
</tr>
<tr>
<td>VM.Standard2.4</td>
<td>4</td>
<td>60 GB</td>
</tr>
<tr>
<td>VM.Standard2.8</td>
<td>8</td>
<td>120 GB</td>
</tr>
<tr>
<td>VM.Standard2.16</td>
<td>16</td>
<td>240 GB</td>
</tr>
<tr>
<td>VM.Standard2.24</td>
<td>24</td>
<td>320 GB</td>
</tr>
</tbody>
</table>

The following table shows the available shapes in the X5 series for a virtual machine DB system.

### Note:

Availability of X5 shapes is limited to monthly universal credit customers existing on or before November 9th, 2018, in the us-phoenix-1, us-ashburn-1, and eu-frankfurt-1 regions.

<table>
<thead>
<tr>
<th>Shape</th>
<th>CPU Cores</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.Standard1.1</td>
<td>1</td>
<td>7 GB</td>
</tr>
<tr>
<td>VM.Standard1.2</td>
<td>2</td>
<td>14 GB</td>
</tr>
<tr>
<td>VM.Standard1.4</td>
<td>4</td>
<td>28 GB</td>
</tr>
<tr>
<td>VM.Standard1.8</td>
<td>8</td>
<td>56 GB</td>
</tr>
<tr>
<td>VM.Standard1.16</td>
<td>16</td>
<td>112 GB</td>
</tr>
</tbody>
</table>

## Storage Options for Virtual Machine DB Systems

Virtual machine DB systems use Oracle Cloud Infrastructure block storage. The following table shows details of the storage options for a virtual machine DB system. Total storage includes available storage plus recovery logs.

<table>
<thead>
<tr>
<th>Available Storage (GB)</th>
<th>Total Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>712</td>
</tr>
<tr>
<td>512</td>
<td>968</td>
</tr>
<tr>
<td>1024</td>
<td>1480</td>
</tr>
<tr>
<td>2048</td>
<td>2656</td>
</tr>
<tr>
<td>4096</td>
<td>5116</td>
</tr>
<tr>
<td>6144</td>
<td>7572</td>
</tr>
<tr>
<td>8192</td>
<td>10032</td>
</tr>
<tr>
<td>10240</td>
<td>12488</td>
</tr>
<tr>
<td>12288</td>
<td>14944</td>
</tr>
<tr>
<td>14336</td>
<td>17404</td>
</tr>
<tr>
<td>16384</td>
<td>19860</td>
</tr>
<tr>
<td>18432</td>
<td>22320</td>
</tr>
<tr>
<td>20480</td>
<td>24776</td>
</tr>
<tr>
<td>Available Storage (GB)</td>
<td>Total Storage (GB)</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>22528</td>
<td>27232</td>
</tr>
<tr>
<td>24576</td>
<td>29692</td>
</tr>
<tr>
<td>26624</td>
<td>32148</td>
</tr>
<tr>
<td>28672</td>
<td>34608</td>
</tr>
<tr>
<td>30720</td>
<td>37064</td>
</tr>
<tr>
<td>32768</td>
<td>39520</td>
</tr>
<tr>
<td>34816</td>
<td>41980</td>
</tr>
<tr>
<td>36864</td>
<td>44436</td>
</tr>
<tr>
<td>38912</td>
<td>46896</td>
</tr>
<tr>
<td>40960</td>
<td>49352</td>
</tr>
</tbody>
</table>

For 2-node RAC virtual machine DB systems, storage capacity is shared between the nodes.

**Security Hardening Tool for Virtual Machine DB systems**

Oracle Cloud Infrastructure virtual machine DB systems provisioned using Oracle Linux 7 include a python script, referred to as the Security Technical Implementation Guide (STIG) tool, that you can use to perform security hardening for your virtual machine DB system. See Security Technical Implementation Guide (STIG) Tool for Virtual Machine DB systems on page 1555 and Enabling FIPS, SE Linux, and STIG on Bare Metal or Virtual Machine DB System Components on page 1556 for more information.

**Boot Volume Backups**

Oracle maintains a weekly boot volume backup of your virtual machine DB system so that the system can be easily restored in the event of a serious error or system failure. Boot volume backups are currently not accessible to users (there is no Console, API, or CLI access to a DB system boot volume backup), and Oracle bears the cost of keeping and maintaining the backup. In the event of a system failure, contact My Oracle Support to request that Oracle perform a restore of your system from the boot volume backup.

**Database Backups, Restoring from a Backup, and Creating a Database or DB System from a backup**

**Backup Options**

Oracle Cloud Infrastructure offers you the ability to create and store automatic daily backups and on-demand full backups. You can store backups in your DB system's local storage, or in Oracle Cloud Infrastructure Object Storage. See Backing Up a Database on page 1435 for information about the backup storage options you have for your cloud databases. See Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435 for information about managed automatic backups in Oracle Cloud Infrastructure.

**Restoring from a Backup**

See Recovering a Database from Object Storage on page 1446 for information on restoring a database from a backup in Object Storage.

**Creating a Database or DB System Using a Backup**

See To create a DB system from a backup and To create a database from a backup in an existing DB system for information about creating a database or DB system from the following sources:

- Daily automatic backups or on-demand full backups.
• The last archived redo log backup. Requires that you have automatic backups enabled. This backup combines data from the most recent daily automatic backup and data from archived redo logs, and represents the most current backup available.
• Daily automatic backup data used to create a point-in-time copy of the source database based on a specified timestamp.
• Standalone Backups on page 1438

Moving Databases to Oracle Cloud DB Systems Using Zero Downtime Migration

Oracle now offers the Zero Downtime Migration service, a quick and easy way to move on-premises Oracle Databases and Oracle Cloud Infrastructure Classic databases to Oracle Cloud Infrastructure. You can migrate databases to the following types of Oracle Cloud Infrastructure systems: Exadata, Exadata Cloud@Customer, bare metal, and virtual machine.

Zero Downtime Migration leverages Oracle Active Data Guard to create a standby instance of your database in an Oracle Cloud Infrastructure system. You switch over only when you are ready, and your source database remains available as a standby. Use the Zero Downtime Migration service to migrate databases individually or at the fleet level. See Move to Oracle Cloud Using Zero Downtime Migration for more information.

Network Setup for DB Systems

Note:
This topic is not applicable to Exadata DB systems. For information on the network setup for an Exadata DB system, see Network Setup for Exadata Cloud Service Instances on page 1232.

Before you set up a bare metal or virtual machine DB system, you must set up a virtual cloud network (VCN) and other Networking service components. This topic describes the recommended configuration for the VCN.

VCN and Subnets

To launch a DB system, you must have:

• A VCN in the region where you want the DB system
• At least one subnet in the VCN (either a public subnet or a private subnet)

In general, Oracle recommends using regional subnets, which span all availability domains in the region. For a bare metal or virtual machine DB system, either a regional subnet or AD-specific subnet works. For more information, see Overview of VCNs and Subnets on page 2822.

You will create a custom route table. You will also create security rules to control traffic to and from the DB system's compute notes. More information follows about that.

Certain details of the VCN and subnet configuration depend on your choice for DNS resolution within the VCN. For more information, see DNS for the DB System on page 1362.

Option 1: Public Subnet with Internet Gateway

This option can be useful when doing a proof-of-concept or development work. You can use this setup in production if you want to use an internet gateway with the VCN, or if you have services that run only on a public network and need access to the database. See the following diagram and description.
You set up:

- **Public subnet.**
- **Internet gateway.**
- **Service gateway** to reach Object Storage for database backups and patching. Also see Option 1: Service Gateway Access Only to Object Storage on page 1366.
- **Route table**: A custom route table for the subnet, with two rules:
  - A rule for 0.0.0.0/0, and target = internet gateway.
  - A rule for the service CIDR label called **OCI <region> Object Storage**, and target = the service gateway. Also see Option 1: Service Gateway Access Only to Object Storage on page 1366.
- **Security rules** to enable the desired traffic to and from the DB system nodes. See Security Rules for the DB System on page 1367.

**Important:**

See this known issue for information about configuring route rules with service gateway as the target on route tables associated with public subnets.
**Option 2: Private Subnet**

Oracle recommends this option for a production system. The subnet is private and cannot be reached from the internet. See the following diagram and description.

![Diagram of Private Subnet]

You set up:

- Private subnet.
- Gateways for the VCN:
  - Dynamic routing gateway (DRG), with a FastConnect or IPSec VPN to your on-premises network.
  - Service gateway to reach Object Storage for database backups and patching, and to reach Oracle YUM repos for OS updates. Also see Option 2: Service Gateway Access to Both Object Storage and YUM Repos on page 1366.
  - NAT gateway (to reach public endpoints not supported by the service gateway).
- Route table: A custom route table for the subnet, with these rules:
  - A route for the on-premises network's CIDR, and target = DRG.
  - A rule for the service CIDR label called All `<region>` Services in Oracle Services Network, and target = the service gateway. Also see Option 2: Service Gateway Access to Both Object Storage and YUM Repos on page 1366.
  - If you want to access the Oracle YUM repos through the NAT gateway, add a route rule for the regional YUM repo's public IP address, and target = the NAT gateway. If you just use the next rule only, the traffic to the
YUM repo would still be routed to the service gateway, because the service gateway route is more specific than 0.0.0.0/0.

- A rule for 0.0.0.0/0, and target = NAT gateway.
- Security rules to enable the desired traffic to and from the DB system nodes. See Security Rules for the DB System on page 1367.

Requirements for IP Address Space

If you are setting up DB systems (and thus VCNs) in more than one region, make sure the IP address space of the VCNs does not overlap.

The subnet you create for a bare metal or virtual machine DB system cannot overlap with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance.

The following table lists the minimum required subnet size.

<table>
<thead>
<tr>
<th>DB System Type</th>
<th># Required IP Addresses</th>
<th>Minimum Subnet Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-node bare metal or virtual machine</td>
<td>1 + 3 reserved in subnet = 4</td>
<td>/30 (4 IP addresses)</td>
</tr>
<tr>
<td>2-node RAC virtual machine</td>
<td>(2 addresses * 2 nodes) + 3 for SCANs + 3 reserved in subnet = 10</td>
<td>/28 (16 IP addresses)</td>
</tr>
</tbody>
</table>

VCN Creation Wizard: Not for Production

The Networking section of the Console includes a handy wizard that creates a VCN along with related resources. It can be useful if you just want to try launching an instance. However, the wizard automatically creates a public subnet and an internet gateway. You may not want this for your production network, so Oracle recommends you create the VCN and other resources individually yourself instead of using the wizard.

DNS for the DB System

There are two choices for DNS and hostname resolution for the DB system:

- Recommended: Use the default DNS functionality in the VCN (called the Internet and VCN Resolver)
- Use a custom DNS resolver of your choice

The following table shows which choices are supported with each type of DB system, and the endpoints that need to be resolved for the DB system to function.

<table>
<thead>
<tr>
<th>DB System Type</th>
<th>Supported DNS Choices</th>
<th>Endpoints to BeResolved</th>
</tr>
</thead>
</table>
| 1-node bare metal or virtual machine | - Recommended: Default (Internet and VCN Resolver)  
|                                   | - Custom DNS resolver of your choice |  
| | | - Object Storage endpoints (includes both the Object Storage endpoints and Swift endpoints)  
| | | - Oracle YUM repo endpoints |
| 2-node RAC virtual machine      | - Default (Internet and VCN Resolver) |  
| | | - Object Storage endpoints (includes both the Object Storage endpoints and Swift endpoints)  
| | | - Oracle YUM repo endpoints  
| | | - Single Client Access Names (SCANs) |
The following sections give more details about the DNS choices.

**Default (Internet and VCN Resolver)**

See the preceding table for the types of DB systems that support the Internet and VCN Resolver.

Oracle recommends using the Internet and VCN Resolver for DNS. It's the default, built-in DNS functionality that comes with each VCN. It enables hosts in a VCN to resolve these items:

- Hostnames of other hosts in the same VCN
- Hostnames that are publicly published on the Internet

For general information about the Internet and VCN Resolver, see *DNS in Your Virtual Cloud Network* on page 2910.

For a DB system, the Internet and VCN Resolver handles resolution of all necessary endpoints: Object Storage endpoints (includes both the Object Storage endpoints and Swift endpoints), YUM repos, and SCANs (SCANs are used only with 2-node RAC systems).

By default, each VCN is configured to use the Internet and VCN Resolver. If you plan to use a custom DNS resolver, you must configure the VCN in a different way. For more information, see *To use a custom DNS resolver with your DB system* on page 1364.

**To use the Internet and VCN Resolver with your DB System**

As part of the overall network setup, perform these tasks:

1. Create the VCN with the required DNS settings:
   - When creating the VCN, select the check box for **Use DNS Hostnames in this VCN**.
   - Specify a DNS label for the VCN. See the restrictions in *Hostname restrictions for using the Internet and VCN Resolver* on page 1363.
   - Notice that you cannot change these VCN DNS settings after you create the VCN.

2. Create each subnet with the required DNS settings:
   - When creating a subnet in the VCN, select the check box for **Use DNS Hostnames in this Subnet**.
   - Specify a DNS label for the subnet. See the restrictions in *Hostname restrictions for using the Internet and VCN Resolver* on page 1363.
   - Notice that you cannot change these subnet DNS settings after you create the subnet.

3. Use the default set of DHCP options that come with the VCN:
   - When creating each subnet, configure it to use the VCN's default set of DHCP options.
   - By default, the default set of DHCP options is configured to use the Internet and VCN Resolver.

4. Create the DB system with a hostname prefix:
   - Later, when creating the DB system, specify a value in the **Hostname Prefix** field. See the restrictions in *Hostname restrictions for using the Internet and VCN Resolver* on page 1363.
   - Notice that the DB system's **Host Domain Name** value is automatically assigned based on the VCN and subnet DNS labels.

The resulting DB system has a fully qualified domain name (FQDN) based on the hostname prefix, VCN label, and subnet label you specify.

**Hostname restrictions for using the Internet and VCN Resolver**

When you create the VCN, subnet, and DB system, you must carefully set the following identifiers, which are related to DNS in the VCN:

- VCN DNS label
- Subnet DNS label
- Hostname prefix for the DB system

These values make up the node's fully qualified domain name (FQDN):
For RAC systems only, the Database service automatically appends a node number after the hostname prefix.

For example:
- Node 1: `dbsys1.ad1.acmevcniad.oraclevcn.com`
- Node 2: `dbsys2.ad1.acmevcniad.oraclevcn.com`

Requirement for the DB system's hostname prefix:
- Recommended maximum: 16 characters. For more information, see the example under the following section, "Requirements for the VCN and subnet DNS labels", for more details.
- Must start with an alphabetical character.
- Cannot be the string `localhost`.

Requirements for the VCN and subnet DNS labels:
- Recommended maximum: 15 characters.
- No hyphens or underscores.
- Recommended: Include the region name in the VCN's name, and include the availability domain name in the subnet's name.
- The FQDN has a maximum total limit of 63 characters, so set the VCN and subnet DNS labels short enough to meet that requirement. Here is a safe general rule:

  `<16_chars_max>\.<15_chars_max>\.<15_chars_max>.oraclevcn.com`

- The recommended maximums are not enforced when you create the VCN and subnets. However, the DB system deployment fails if the FQDN has more than 63 characters.

**Custom DNS Resolver**

See the preceding table for the types of DB systems that support the use of a custom DNS resolver.

A custom DNS resolver is a DNS server that you set up in your on-premises network and maintain yourself. It must resolve the endpoints required by the DB system.

By default, the VCN is configured to use the Internet and VCN Resolver. Therefore, if you instead want to use a custom DNS resolver, you must configure the VCN and DHCP options in a different way. See the following process.

**To use a custom DNS resolver with your DB system**

As part of the overall network setup, perform these tasks:

1. Create the VCN with the recommended DNS settings:
   - When creating the VCN, Oracle recommends that you select the check box for **Use DNS Hostnames in this VCN** and then specify a DNS label for the VCN. See the restrictions listed in Hostname restrictions when using a custom DNS resolver on page 1365.
   - Notice that you cannot change the preceding VCN DNS settings after you create the VCN. They are optional for a custom DNS server, but required if you use the Internet and VCN Resolver. Therefore, Oracle recommends that you configure them now in case you later want to use the Internet and VCN Resolver.

2. Create each subnet with the recommended DNS settings:
   - When creating a subnet in the VCN, Oracle recommends that you select select the check box for **Use DNS Hostnames in this Subnet** and then specify a DNS label for the subnet. See the restrictions listed in Hostname restrictions when using a custom DNS resolver on page 1365.
   - Notice that you cannot change the preceding subnet DNS settings after you create the subnet. They are optional for a custom DNS server, but required if you use the Internet and VCN Resolver. Therefore, Oracle recommends that you configure them now in case you later want to use the Internet and VCN Resolver.
3. Edit the default set of DHCP options to use a custom resolver:
   • When creating each subnet, configure it to use the VCN’s default set of DHCP options.
   • Edit the default set of DHCP options so that **DNS Type** is set to **Custom Resolver**. Provide the IP address for at least one DNS server (maximum three). Optionally provide a single search domain (which will automatically be added to the host's `/etc/resolv.conf` file).

4. Create the DB system with required DNS entries:
   • Later, when creating the DB system, specify a **Hostname Prefix**.
   • For the **Host Domain Name**: If you selected the check box for **Use DNS Hostnames** in the preceding steps, the **Host Domain Name** is automatically generated from the VCN and subnet DNS labels. Otherwise, you must provide a value for the **Host Domain Name**. See the restrictions listed in **Hostname restrictions when using a custom DNS resolver** on page 1365.
   • Notice that when launching the DB system, the Database service automatically assigns an IP address from the VCN’s CIDR block and resolves the address locally based on the host's `/etc/hosts` file. Your custom DNS resolver does not need to resolve the hostname in advance for the DB system launch to succeed.

**Hostname restrictions when using a custom DNS resolver**

Requirement for the DB system's hostname prefix:
   • Recommended maximum: 16 characters. For more information, see the example under the next section, **Requirements for the VCN and subnet DNS labels**.
   • Must start with an alphabetical character.
   • Cannot be the string `localhost`.

Requirements for the VCN and subnet DNS labels:
   • You can provide a value for the DNS labels only if you select the check box for **Use DNS Hostnames** when creating the VCN and subnets. The resulting FQDN for the DB system follows this format:
     <hostname_prefix>.<subnet_DNS_label>.<VCN_DNS_label>.oraclevcn.com
   • Recommended maximum for each DNS label: 15 characters.
   • No hyphens or underscores.
   • Recommended: Include the region name in the VCN's name, and include the availability domain name in the subnet's name.
   • The FQDN has a maximum total limit of 63 characters, so set the VCN and subnet DNS labels short enough to meet that requirement. Here is a safe general rule:
     <16_chars_max>.<15_chars_max>.<15_chars_max>.oraclevcn.com
   • The recommended maximums are not enforced when you create the VCN and subnets. However, the DB system deployment fails if the FQDN has more than 63 characters.

Requirements for the DB system's host domain name:
   • You can provide a value in the **Host Domain Name** field only if you did not select the check box for **Use DNS Hostnames** when creating the VCN and subnets.
   • No hyphens or underscores.
   • Ensure that the value results in an FQDN that is no longer than 63 characters. Otherwise the DB system deployment will fail.

**DNS: Between On-Premises Network and VCN**

If you are using the Internet and VCN Resolver and want to enable the use of hostnames when on-premises hosts and VCN resources communicate with each other, you can set up an instance in the VCN to be a custom DNS server. For an example of an implementation of this scenario with the Oracle Terraform provider, see **Hybrid DNS Configuration**.

**Service Gateway for the VCN**

Your VCN needs access to both Object Storage (for backing up databases, patching, and updating the cloud tooling on a DB system) and Oracle YUM repos for OS updates.
Depending on whether you use option 1 or option 2 described previously, you use the service gateway in different ways. See the next two sections.

**Option 1: Service Gateway Access Only to Object Storage**

You configure the subnet to use the service gateway for access only to Object Storage. As a reminder, here's the diagram for option 1:

In general, you must:

- Perform the tasks for setting up a service gateway on a VCN, and specifically enable the service CIDR label called `OCI <region> Object Storage`.
- In the task for updating routing, add a route rule to the subnet's custom route table. For the destination service, use `OCI <region> Object Storage` and target = the service gateway.
- In the task for updating security rules for the subnet, perform the task on the DB system's custom network security group (NSG) or security list. Here you set up a security rule with the destination service set to `OCI <region> Object Storage`. See Custom Security Rules on page 1368.

**Option 2: Service Gateway Access to Both Object Storage and YUM Repos**

You configure the subnet to use the service gateway for access to the Oracle Services Network, which includes both Object Storage and the Oracle YUM repos.
Important:

See this known issue for information about accessing Oracle YUM services through the service gateway.

As a reminder, here's the diagram for option 2:

In general, you must:

- Perform the tasks for setting up a service gateway on a VCN, and specifically enable the service CIDR label called All <region> Services in Oracle Services Network.
- In the task for updating routing in the subnet, add a rule to the subnet's custom route table. For the destination service, use All <region> Services in Oracle Services Network and target = the service gateway.
- In the task for updating security rules for the subnet, perform the task on the subnet's custom network security group (NSG) or security list. Here you set up a security rule with the destination service set to All <region> Services in Oracle Services Network. See Custom Security Rules on page 1368.

Security Rules for the DB System

This section lists the security rules to use with your DB system. Security rules control the types of traffic allowed in and out of the DB system's compute nodes. The rules are divided into two sections.

There are different ways to implement these rules. For more information, see Ways to Implement the Security Rules on page 1370.
Important:
Your instances running Oracle-provided DB system images also have firewall rules that control access to the instance. Make sure that both the instance's security rules and firewall rules are set correctly. Also see Opening Ports on the DB System on page 1433.

General Rules Required for Basic Connectivity

This section has several general rules that enable essential connectivity for hosts in the VCN.

If you use security lists to implement your security rules, be aware that the rules that follow are included by default in the default security list. Update or replace the list to meet your particular security needs. The two ICMP rules (general ingress rules 2 and 3) are required for proper functioning of network traffic within the Oracle Cloud Infrastructure environment. Adjust the general ingress rule 1 (the SSH rule) and the general egress rule 1 to allow traffic only to and from hosts that require communication with resources in your VCN.

General ingress rule 1: Allows SSH traffic from anywhere
- **Stateless**: No (all rules must be stateful)
- **Source Type**: CIDR
- **Source CIDR**: 0.0.0.0/0
- **IP Protocol**: TCP
- **Source Port Range**: All
- **Destination Port Range**: 22

General ingress rule 2: Allows Path MTU Discovery fragmentation messages
This rule enables hosts in the VCN to receive Path MTU Discovery fragmentation messages. Without access to these messages, hosts in the VCN can have problems communicating with hosts outside the VCN.
- **Stateless**: No (all rules must be stateful)
- **Source Type**: CIDR
- **Source CIDR**: 0.0.0.0/0
- **IP Protocol**: ICMP
- **Type**: 3
- **Code**: 4

General ingress rule 3: Allows connectivity error messages within the VCN
This rule enables the hosts in the VCN to receive connectivity error messages from each other.
- **Stateless**: No (all rules must be stateful)
- **Source Type**: CIDR
- **Source CIDR**: Your VCN's CIDR
- **IP Protocol**: ICMP
- **Type**: 3
- **Code**: All

General egress rule 1: Allows all egress traffic
- **Stateless**: No (all rules must be stateful)
- **Destination Type**: CIDR
- **Destination CIDR**: 0.0.0.0/0
- **IP Protocol**: All

Custom Security Rules
The following rules are necessary for the DB system's functionality.
Important:

Custom ingress rules 1 and 2 only cover connections initiated from within the VCN. If you have a client that resides outside the VCN, Oracle recommends setting up two additional similar rules that instead have the Source CIDR set to the public IP address of the client.

Custom ingress rule 1: Allows ONS and FAN traffic from within the VCN

This rule is recommended and enables the Oracle Notification Services (ONS) to communicate about Fast Application Notification (FAN) events.

- Stateless: No (all rules must be stateful)
- Source Type: CIDR
- Source CIDR: VCN's CIDR
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 6200
- Description: An optional description of the rule.

Custom ingress rule 2: Allows SQL*NET traffic from within the VCN

This rule is for SQL*NET traffic and is required only if you need to enable client connections to the database.

- Stateless: No (all rules must be stateful)
- Source Type: CIDR
- Source CIDR: VCN's CIDR
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Description: An optional description of the rule.

Custom egress rule 1: Allows outbound SSH access

This rule enables SSH access between nodes in a 2-node DB system. It is redundant with the general egress rule in General Rules Required for Basic Connectivity (and in the default security list). It is optional but recommended in case the general rule (or default security list) is inadvertently changed.

- Stateless: No (all rules must be stateful)
- Destination Type: CIDR
- Destination CIDR: 0.0.0.0/0
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 22
- Description: An optional description of the rule.

Custom egress rule 2: Allows access to Object Storage and YUM repos

This rule enables the DB system to communicate with Object Storage alone (for option 1), or with the Oracle Services Network, which includes both Object Storage and the Oracle YUM repos (for option 2). It is redundant with the general egress rule in General Rules Required for Basic Connectivity on page 1368 (and in the default security list). It is optional but recommended in case the general rule (or default security list) is inadvertently changed.

- Stateless: No (all rules must be stateful)
- Destination Type: Service
- Destination Service:
  - For option 1, use the service CIDR label called OCI <region> Object Storage
  - For option 2, use the service CIDR label called All <region> Services in Oracle Services Network
- IP Protocol: TCP
• **Source Port Range:** All
• **Destination Port Range:** 443 (HTTPS)
• **Description:** An optional description of the rule.

**Ways to Implement the Security Rules**

The Networking service offers two ways to implement security rules within your VCN:

• **Network security groups**
• **Security lists**

For a comparison of the two methods, see [Comparison of Security Lists and Network Security Groups](#) on page 2833.

*If you use network security groups*

If you choose to use network security groups (NSGs), here is the recommended process:

1. Create a network security group for DB systems. Add the following security rules to that NSG:
   - The rules listed in [General Rules Required for Basic Connectivity](#) on page 1368
   - The rules listed in [Custom Security Rules](#) on page 1368
2. When the database administrator creates the DB system, they must choose several networking components (for example, which VCN and subnet to use). They can also choose which NSG or NSGs to use. Make sure they choose the NSG you created.

You could instead create one NSG for the general rules and a separate NSG for the custom rules. Then when the database administrator chooses which NSGs to use for the DB system, make sure they choose both NSGs.

*If you use security lists*

If you choose to use security lists, here is the recommended process:

1. Configure the subnet to use the required security rules:
   a. Create a custom security list for the subnet and add the rules listed in [Custom Security Rules](#) on page 1368.
   b. Associate the following two security lists with the subnet:
      - VCN's default security list with all its default rules. This automatically comes with the VCN.
      - The new custom security list you created for the subnet
2. Later when the database administrator creates the DB system, they must choose several networking components. When they select the subnet that you have already created and configured, the security rules are automatically enforced for the compute nodes created in the subnet.

**Caution:**

Do not remove the default egress rule from the default security list. If you do, instead make sure to include the following replacement egress rule in the subnet's custom security list:

- **Stateless:** No (all rules must be stateful)
- **Destination Type:** CIDR
- **Destination CIDR:** 0.0.0.0/0
- **IP Protocol:** All

**Creating Bare Metal and Virtual Machine DB Systems**

This topic explains how to create a bare metal or virtual machine DB system, and set up DNS for a single-node or two-node Oracle RAC DB system.

When you create a DB system using the Console, the API, or the CLI, the system is provisioned to support Oracle databases, and an initial database is created based on the options you provide and some default options described later in this topic.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more information about writing policies for databases, see Details for the Database Service on page 2240.

Prerequisites

You'll need the following items to create any DB system:

- The public key, in OpenSSH format, from the key pair that you plan to use for connecting to the DB System via SSH. A sample public key, abbreviated for readability, is shown below.

  ssh-rsa AAAAB3NzaC1yc2EAAAABJQAA...lo/gKMLVM2xzc1xJr/
  Hc26biw3TXWGEakrK1OQ== rsa-key-20160304

  For more information, see Managing Key Pairs on Linux Instances on page 693.

- A correctly configured virtual cloud network (VCN) to launch the DB system in. Its related networking resources (gateways, route tables, security lists, DNS, and so on) must also be configured as necessary for the DB system. For more information, see Network Setup for DB Systems on page 1359.

- If you plan to back up your DB system to Object Storage or to use the managed patching feature, then Oracle recommends using a service gateway to enable access to Object Storage. For more information, see Service Gateway for the VCN on page 1365.

- For a two-node Oracle RAC DB system, ensure that port 22 is open for both ingress and egress on the subnet, and that the security rules you create are stateful (the default), otherwise, the DB system might fail to provision successfully.

Default Options for the Initial Database

To simplify creating a DB system in the Console, and when using the API, the following default options are used for the initial database and for any additional databases that you create. (Several advanced options, such as time zone, can be set when you can use the dbcli command line interface to create databases.)

- **Console Enabled**: False
- **Create Container Database**: False for Oracle Database 11g (11.2.0.4) databases. Otherwise, true.
- **Create Instance Only (for standby and migration)**: False
- **Database Home ID**: Creates a new database home
- **Database Language**: AMERICAN
- **Database Sizing Template**: odb2
- **Database Storage**: Oracle Automatic Storage Management Cluster File System (ACFS) for Oracle Database 11g (11.2.0.4) databases. Otherwise, Automatic Storage Management (ASM) for all bare metal and multi-node virtual machine DB systems. Single-node VM systems can optionally be provisioned using Logical Volume Manager for faster provisioning.
- **Database Territory**: AMERICA
- **Database Unique Name**: The user-specified database name and a system-generated suffix, for example, dbtst_phx1cs.
- **PDB Admin Name**: pdbuser (Not applicable for Oracle Database 11g (11.2.0.4) databases.)

For a list of the database options that you can set, see To create a DB system on page 1372.
Using a Backup to Create the Initial Database

When creating a new DB system using a backup stored in Object Storage as the source of the initial database, you have the following options:

- **Daily automatic backup**. Requires that you have automatic backups enabled and an available backup to use. If you are creating a database from an automatic backup, you can choose any level 0 weekly backup, or a level 1 incremental backup created after the most recent level 0 backup. For more information on automatic backups, see Oracle Cloud Infrastructure Managed Backup Features on page 1436.
- **On-demand full backup**. See To create an on-demand full backup of a database on page 1439 for information on creating an on-demand backup.
- **Standalone backup**. For more information, see Standalone Backups on page 1438.
- **Last archived redo log backup**. Requires that you have automatic backups enabled. This backup combines data from the most recent daily automatic backup and data from archived redo logs, and represents the most current backup available. The time of the last archived redo log backup is visible on the database details page in the Last Backup Time field.
- **Point-in-time out of place restore**. Specify a timestamp to create a new copy of the database that included data up to a specified point in time. The timestamp must be earlier or equal to the Last Backup Time time displayed on the database details page. Note the following limitations when performing a point-in-time out of place restore:
  - The timestamp must be within the recovery window of the database
  - The timestamp must be available within the database incarnation of the available automatic backups
  - The timestamp cannot fall within two overlapping database incarnations
  - The create database operation will fail if the database has undergone structural changes since the specified timestamp. Structural changes include operations such as creating or dropping a tablespace.
  - The create database operation cannot be started if another point-in-time database copy operation is in progress.

Custom IP Addresses for Non-RAC DB Systems

When creating a new non-RAC DB system or cloning an existing VM DB system, you can optionally define the IP address of the DB system being provisioned. This is useful in development contexts where you create and delete the same DB system over and over, and you need each new iteration of the DB system to use the same IP address.

**Using the Console**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To create a DB system

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Click Create DB System.
3. On the **Create DB System** page, provide the basic information for the DB system:

- **Select a compartment**: By default, the DB system is created in your current compartment and you can use the network resources in that compartment.
- **Name your DB system**: A non-unique, display name for the DB system. An Oracle Cloud Identifier (OCID) uniquely identifies the DB system. Avoid entering confidential information.
- **Select an availability domain**: The availability domain in which the DB system resides.
- **Select a shape type**: The shape type you select sets the default shape and filters the shape options in the next field.
- **Select a shape**: The shape determines the type of DB system created and the resources allocated to the system. To specify a shape other than the default, click **Change Shape**, and select an available shape from the list.

**Bare metal shapes**

- **BM.DenseIO2.52**: Provides a 1-node DB system (one bare metal server), with up to 52 CPU cores, 768 GB memory, and eight 6.4 TB locally attached NVMe drives (51.2 TB total) to the DB system.
- **BM.DenseIO1.36**: Limited availability. Provides a 1-node DB system (one bare metal server), with up to 36 CPU cores, 512 GB memory, and nine 3.2 TB locally attached NVMe drives (28.8 TB total) to the DB system.

*Note*: BM.DenseIO1.36 is available only to monthly universal credit customers existing on or before November 9th, 2018. This shape is available only in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.

**Virtual machine shapes**

Virtual machine X7 shapes:

- **VM.Standard2.1**: Provides a 1-node DB system with 1 core.
- **VM.Standard2.2**: Provides a 1- or 2-node DB system with 2 cores.
- **VM.Standard2.4**: Provides a 1- or 2-node DB system with 4 cores.
- **VM.Standard2.8**: Provides a 1- or 2-node DB system with 8 cores.
- **VM.Standard2.16**: Provides a 1- or 2-node DB system with 16 cores.
- **VM.Standard2.24**: Provides a 1- or 2-node DB system with 24 cores.

Virtual machine X5 shapes:

- **VM.Standard1.1**: Provides a 1-node DB system with 1 core.
- **VM.Standard1.2**: Provides a 1- or 2-node DB system with 2 cores.
- **VM.Standard1.4**: Provides a 1- or 2-node DB system with 4 cores.
- **VM.Standard1.8**: Provides a 1- or 2-node DB system with 8 cores.
- **VM.Standard1.16**: Provides a 1- or 2-node DB system with 16 cores.

*Note*: X5-based shapes availability is limited to monthly universal credit customers existing on or before November 9th, 2018, in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.

- **VM.Standard1.1** and **VM.Standard2.1** shapes cannot be used for 2-node RAC clusters.

**Configure the DB system**: Specify the following:

- **Total node count**: The number of nodes in the DB system, which depends on the shape you select. For virtual machine DB systems, you can specify either one or two nodes, except for **VM.Standard2.1** and **VM.Standard1.1**, which are single-node DB systems.
- **Oracle Database software edition**: The database edition supported by the DB system. For bare metal systems, you can mix supported database releases on the DB system to include older database versions, but
not editions. The database edition cannot be changed and applies to all the databases in this DB system. Virtual machine systems support only one database.

- **CPU core count:** Displays only for bare metal DB systems to allow you to specify the number of CPU cores for the system. (Virtual machine DB system shapes have a fixed number of CPU cores.) The text below the field indicates the acceptable values for that shape. For a multi-node DB system, the core count is evenly divided across the nodes.

  
  **Note:**
  After you provision the DB system, you can increase the CPU cores to accommodate increased demand. On a bare metal DB system, you scale the CPU cores directly. For virtual machine DB systems, you change the number of CPU cores by changing the shape.

- **Choose Storage Management Software:** Select Oracle Grid Infrastructure to use Oracle Automatic Storage Management (recommended for production workloads). Select Logical Volume Manager to quickly provision your DB system using Logical Volume Manager storage management software. Note that the Available storage (GB) value you specify during provisioning determines the maximum total storage available through scaling. The total storage available for each choice is detailed in the Storage Scaling Considerations for Virtual Machine Databases Using Fast Provisioning on page 1555 topic.

  See Fast Provisioning Option for 1-node Virtual Machine DB Systems for more information about this feature.

- **Configure storage:** Specify the following:

  - **Available storage (GB):** Virtual machine only. The amount of Block Storage in GB to allocate to the virtual machine DB system. Available storage can be scaled up or down as needed after provisioning your DB system.
  
  - **Total storage (GB):** Virtual machine only. The total Block Storage in GB used by the virtual machine DB system. The amount of available storage you select determines this value. Oracle charges for the total storage used.
  
  - **Cluster name:** (Optional) A unique cluster name for a multi-node DB system. The name must begin with a letter and contain only letters (a-z and A-Z), numbers (0-9) and hyphens (-). The cluster name can be no longer than 11 characters and is not case sensitive.
  
  - **Data storage percentage:** Bare metal only. The percentage (40% or 80%) assigned to DATA storage (user data and database files). The remaining percentage is assigned to RECO storage (database redo logs, archive logs, and recovery manager backups).

- **Add public SSH keys:** The public key portion of each key pair you want to use for SSH access to the DB system. You can browse or drag and drop .pub files, or paste in individual public keys. To paste multiple keys, click + Another SSH Key, and supply a single key for each entry.

- **Choose a license type:** The type of license you want to use for the DB system. Your choice affects metering for billing.

  - **License Included** means the cost of this Oracle Cloud Infrastructure Database service resource will include both the Oracle Database software licenses and the service.
  
  - **Bring Your Own License (BYOL)** means you will use your organization’s Oracle Database software licenses for this Oracle Cloud Infrastructure Database service resource. See Bring Your Own License for more information.

4. **Specify the network information:**

  - **Virtual cloud network:** The VCN in which to create the DB system. Click Change Compartment to select a VCN in a different compartment.
  
  - **Client Subnet:** The subnet to which the DB system should attach. For 1- and 2-node RAC DB systems: Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private
interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.

Click **Change Compartment** to select a subnet in a different compartment.

- **Network Security Groups:** Optionally, you can specify one or more network security groups (NSGs) for your DB system. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to your DB system. A maximum of five NSGs can be specified. For more information, see Network Security Groups on page 2841 and Network Setup for DB Systems on page 1359.

Note that if you choose a subnet with a security list, the security rules for the DB system will be a union of the rules in the security list and the NSGs.

**To use network security groups**

a. Check the **Configure Network Security Groups** check box. Note that you must have a virtual cloud network selected to be able to assign NSGs to your DB system.

b. Specify the NSG to use with the DB system. You might need to use more than one NSG. If you're not sure, contact your network administrator.

c. To use additional NSGs, click **+ Another Network Security Group**.

- **Hostname prefix:** Your choice of host name for the bare metal or virtual machine DB system. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for bare metal and virtual machine DB systems is 16.

  **Important:**

  The host name must be unique within the subnet. If it is not unique, the DB system will fail to provision.

- **Host domain name:** The domain name for the DB system. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, then this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. Hyphens (-) are not permitted.

- **Host and domain URL:** Combines the host and domain names to display the fully qualified domain name (FQDN) for the database. The maximum length is 64 characters.

- **Private IP address:** Optionally, for non-RAC DB systems, you can define the IP address of the new DB system. This is useful in development contexts where you create and delete a DB system over and over, and you need each new iteration of the DB system to use the same IP address. If you specify an IP address that is currently in use within the subnet, the provisioning operation will fail with an error message regarding the invalid IP address.

5. Click **Show Advanced Options** to specify advanced options for the DB system:

- **Disk redundancy:** *For bare metal systems only.* The type of redundancy configured for the DB system.
  - **Normal** is 2-way mirroring, recommended for test and development systems.
  - **High** is 3-way mirroring, recommended for production systems.

- **Fault domain:** The fault domain(s) in which the DB system resides. You can choose which fault domain to use for your DB system. For two-node Oracle RAC DB systems, you can specify which two fault domains to use. Oracle recommends that you place each node of a two-node Oracle RAC DB system in a different fault domain. For more information on fault domains, see About Regions and Availability Domains on page 180.

- **Time zone:** The default time zone for the DB system is UTC, but you can specify a different time zone. The time zone options are those supported in both the Java.util.TimeZone class and the Oracle Linux operating system. For more information, see DB System Time Zone on page 1575.

  **Tip:**

  If you want to set a time zone other than UTC or the browser-detected time zone, and if you do not see the time zone you want, try selecting "Miscellaneous" in the **Region or country** list.

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more
6. After you complete the network configuration and specify any advanced options, click **Next**.

7. Provide information for the initial database:

   - **Database name**: The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
   - **Database image**: This controls the version of the initial database created on the DB system. By default, the latest available Oracle Database version is selected. You can also choose an older Oracle Database version, or choose a customized database software image that you have previously created in your current region with your choice of updates and one-off (interim) patches. See Oracle Database Software Images on page 1567 for information on creating and working with database software images.

   To use an older Oracle-published software image:

   a. Click **Change Database Image**.
   b. In the Select a Database Software Image dialog, select **Oracle-published Database Software Images**.
   c. In the Oracle Database Version list, check the version you wish to use to provision the initial database in your DB system. If you are launching a DB system with a virtual machine shape, you have option of selecting an older database version.

   Display all available versions: Use this switch to include older database updates in the list of database version choices. When the switch is activated, you will see all available PSUs and RUs. The most recent release for each major version is indicated with "(latest)". See Availability of Older Database Versions for Virtual Machine DB Systems on page 1354 for more information.

   d. Click **Select**.

To use a user-created database software image:

   a. Click **Change Database Image**.
   b. In the Select a Database Software Image dialog, select **Custom Database Software Images**.
   c. Select the compartment that contains your database software image.
   d. Select the Oracle Database version that your database software image uses.
   e. A list of database software images is displayed for your chosen Oracle Database version. Check the box beside the display name of the image you want to use.

   After the DB system is active, you can create additional databases for bare metal systems. You can mix database versions on the DB system, but not editions. Virtual machine DB systems are limited to a single database.

   - **PDB name**: Not applicable to Oracle Database 11g (11.2.0.4). The name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of eight alphanumeric characters. The only special character permitted is the underscore (_).
   - **Create administrator credentials**: A database administrator SYS user will be created with the password you supply.

     - **Username**: SYS
     - **Password**: Supply the password for this user. The password must meet the following criteria:

       A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The
special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.

- **Confirm password:** Re-enter the SYS password you specified.
- **Use the administrator password for the TDE wallet:** When this option checked, the password entered for the SYS user is also used for the TDE wallet. To set the TDE wallet password manually, uncheck this option and enter the TDE wallet password.
- **Select workload type:** Choose the workload type that best suits your application:
  - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
  - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
- **Configure database backups:** Specify the settings for backing up the database to Object Storage:
  - **Enable automatic backup:** Check the check box to enable automatic incremental backups for this database. If you are creating a database in a security zone compartment, you must enable automatic backups.
  - **Backup retention period:** If you enable automatic backups, then you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
  - **Backup Scheduling:** If you enable automatic backups, then you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, then the six-hour default window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See Backup Scheduling for more information.
- **Click Show Advanced Options** to specify advanced options for the initial database:
  - **Character set:** The character set for the database. The default is AL32UTF8.
  - **National character set:** The national character set for the database. The default is AL16UTF16.

8. Click **Create DB System**. The DB system appears in the list with a status of Provisioning. The DB system's icon changes from yellow to green (or red to indicate errors).

After the DB system's icon turns green, with a status of Available, you can click the highlighted DB system name to display details about the DB system. Note the IP addresses. You'll need the private or public IP address, depending on network configuration, to connect to the DB system.

**To create a DB system from a backup**

You can create a new DB system from a backup. See Using a Backup to Create the Initial Database on page 1372 in this topic for details on backup source options.

Before you begin, note the following:

- When you create a DB system from a backup, the availability domain is the same as where the backup is hosted.
- The shape you specify must be the same type as the database from which the backup was taken. For example, if you are using a backup of a single-node database, then the DB system you select as your target must also be a single-node DB system.
- The Oracle database software version you specify must be an equal or greater version than that of the backed up database.
- If you specify a virtual machine DB system shape, then the Available Storage Size will default to the data size of the backup, rounded up to the closest storage size option. However, you can specify a larger storage size.
- If you are creating a new DB system from an automatic backup, you may choose any level 0 weekly backup, or a level 1 incremental backup created after the most recent level 0 backup. For more information on automatic backups, see Oracle Cloud Infrastructure Managed Backup Features on page 1436.
- If the backup being used to create a DB system is in a security zone compartment, the DB system cannot be created in a compartment that is not in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.

   A list of DB systems is displayed.

3. Navigate to the backup or standalone backup you want to use to create the new DB system:

   **Tip:**
   
   If you are creating a database from an automatic backup, you may choose any level 0 weekly backup, or a level 1 incremental backup created after the most recent level 0 backup. For more information on automatic backups, see Oracle Cloud Infrastructure Managed Backup Features on page 1436.

   **To select a daily automatic backup or on-demand full backup as the source**
   
   a. Click the DB system name that contains the specific database to display the DB System Details page.
   b. From the Databases list, click the database name associated with the backup you want to use.
   c. Find your desired backup in the Backups list. If you don't see the backups list on the database details page, click Backups in the Resources menu.
   d. Click the Actions icon (three dots) for the backup, and then click Create Database.

   **To select the last archived redo log automatic backup as the source**
   
   a. Find the DB system where the database is located, and click the system name to display details about it.
   b. Find the database associated with the backup you wish to use, and click its name to display details about it.
   c. On the database details page, click Create Database from Last Backup.
   d. In the Create Database from Backup dialog, select Create database from last backup.

   **To specify a timestamp for a point-in-time copy of the source**
   
   a. Click the DB system name that contains the specific database to display the DB System Details page.
   b. From the Databases list, click the database name associated with the backup data you want to use as the source for the initial database in your new DB system.
   c. On the database details page, click Create Database from Last Backup.
   d. In the Create Database from Backup dialog, select Create database from specified timestamp.

   **To select a standalone backup as the source**
   
   a. Click Standalone Backups under Bare Metal, VM, and Exadata.
   b. In the list of standalone backups, find the backup you want to use to create the database.
   c. Click the Actions icon (three dots) for the backup you are interested in, and then click Create Database.
4. In the **Create Database from Backup** dialog, enter the following:

**DB System Information**

- **DB System Information**: Select **Launch New DB System**.
- **Display Name**: A friendly, display name for the DB system. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system. Avoid entering confidential information.
- **Shape**: The shape to use to launch the DB system. The shape determines the type of DB system and the resources allocated to the system.

The selected shape must support the same number of nodes as the DB system from which the backup was created.

**Bare metal shapes**

- **BM.DenseIO2.52**: Provides a 1-node DB system (one bare metal server), with up to 52 CPU cores, 768 GB memory, and eight 6.4 TB locally attached NVMe drives (51.2 TB total) to the DB system.
- **BM.DenseIO1.36**: Limited availability. Provides a 1-node DB system (one bare metal server), with up to 36 CPU cores, 512 GB memory, and nine 3.2 TB locally attached NVMe drives (28.8 TB total) to the DB system.

**Note:** BM.DenseIO1.36 is available only to monthly universal credit customers existing on or before November 9th, 2018. This shape is available only in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.

**Virtual machine shapes**

Virtual machine X7 shapes:

- **VM.Standard2.1**: Provides a 1-node DB system with 1 core.
- **VM.Standard2.2**: Provides a 1- or 2-node DB system with 2 cores.
- **VM.Standard2.4**: Provides a 1- or 2-node DB system with 4 cores.
- **VM.Standard2.8**: Provides a 1- or 2-node DB system with 8 cores.
- **VM.Standard2.16**: Provides a 1- or 2-node DB system with 16 cores.
- **VM.Standard2.24**: Provides a 1- or 2-node DB system with 24 cores.

Virtual machine X5 shapes:

- **VM.Standard1.1**: Provides a 1-node DB system with 1 core.
- **VM.Standard1.2**: Provides a 1- or 2-node DB system with 2 cores.
- **VM.Standard1.4**: Provides a 1- or 2-node DB system with 4 cores.
- **VM.Standard1.8**: Provides a 1- or 2-node DB system with 8 cores.
- **VM.Standard1.16**: Provides a 1- or 2-node DB system with 16 cores.

**Note:**

- X5-based shapes availability is limited to monthly universal credit customers existing on or before November 9th, 2018, in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.
- **VM.Standard1.1** and **VM.Standard2.1** shapes cannot be used for 2-node RAC clusters.

**Total Node Count**: *Virtual machine DB systems only*. The number of nodes in the DB system. The number depends on the shape you select. You can specify 1 or 2 nodes for virtual machine DB systems, except for **VM.Standard2.1** and **VM.Standard1.1**, which are single-node DB systems.

**Oracle Database Software Edition**: The database edition supported by the DB system. For bare metal systems, you can mix supported database releases on the DB system to include older database versions, but not
editions. The database edition cannot be changed and applies to all the databases in this DB system. Virtual machine systems support only one database.

- **Available Storage Size:** *Virtual machine DB systems only.* The amount of Block Storage you wish to allocate to the virtual machine DB system.
- **Cluster Name:** A unique cluster name for a multi-node DB system. The name must begin with a letter and contain only letters (a-z and A-Z), numbers (0-9) and hyphens (-). The cluster name can be no longer than 11 characters and is not case sensitive.
- **License Type:** The type of license you want to use for the DB system. Your choice affects metering for billing.
  - **License included** means the cost of this Oracle Cloud Infrastructure Database service resource will include both the Oracle Database software licenses and the service.
  - **Bring Your Own License (BYOL)** means you will use your organization’s Oracle Database software licenses for this Oracle Cloud Infrastructure Database service resource. See Bring Your Own License for more information.
- **SSH Public Key:** The public key portion of the key pair you want to use for SSH access to the DB system. To provide multiple keys, paste each key on a new line. Make sure each key is on a single, continuous line. The length of the combined keys cannot exceed 10,000 characters.
- **Data Storage Percentage:** *For bare metal DB systems only.* The percentage (40% or 80%) assigned to DATA storage (user data and database files). The remaining percentage is assigned to RECO storage (database redo logs, archive logs, and recovery manager backups).
- **Available Storage Size:** *For virtual machine DB systems only.* The amount of block storage to allocate to the virtual machine DB system. Available storage can be scaled up or down as needed after provisioning your DB system.

If you are creating a DB system from a backup, the minimum value for available storage is determined by the size of the backup.

- **Advanced Options:**
  - **Disk redundancy:** *For bare metal systems only.* The type of redundancy configured for the DB system.
    - **Normal** is 2-way mirroring, recommended for test and development systems.
    - **High** is 3-way mirroring, recommended for production systems.
  - **Fault Domain:** The fault domain(s) in which the DB system resides. You can choose which fault domain to use for your DB system. For 2-node RAC DB systems, you can specify which two fault domains are to be used. Oracle recommends that you place each node of a 2-node RAC DB system in a different fault domain. For more information on fault domains, see Fault Domains on page 182.

**Network Information**

- **Virtual Cloud Network:** The VCN in which to launch the DB system.
- **Client Subnet:** The subnet to which the bare metal or virtual machine DB system should attach. *For 1- and 2-node RAC DB systems:* Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.
- **Network Security Groups:** Optionally, you can specify one or more network security groups (NSGs) for your DB system. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules
to your DB system. A maximum of five NSGs can be specified. For more information, see Network Security Groups on page 2841 and Network Setup for DB Systems on page 1359.

To use network security groups

a. Check the Configure Network Security Groups check box. Note that you must have a virtual cloud network selected to be able to assign NSGs to your DB system.

b. Specify the NSG to use with the DB system. You might need to use more than one NSG. If you're not sure, contact your network administrator.

c. To use additional NSGs, click + Another Network Security Group.

- **Hostname Prefix:** Your choice of host name for the bare metal or virtual machine DB system. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for bare metal and virtual machine DB systems is 16.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The host name must be unique within the subnet. If it is not unique, the DB system will fail to provision.</td>
</tr>
</tbody>
</table>

- **Private IP address:** Optionally, for non-RAC DB systems, you can define the IP address of the new DB system. This is useful in development contexts where you create and delete a DB system over and over, and you need each new iteration of the DB system to use the same IP address. If you specify an IP address that is currently in use within the subnet, the provisioning operation will fail with an error message regarding the invalid IP address.

**Database Information**

- **Database Name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.

- **Database Admin Password:**
  
  A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be , #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.

- **Confirm Database Admin Password:** Re-enter the Database admin password you specified.

- **Password for Transparent Data Encryption (TDE) Wallet or RMAN Encryption:**
  
  Enter either the TDE wallet password or the RMAN encryption password for the backup, whichever is applicable. The TDE wallet password is the SYS password provided when the database was created by using the Oracle Cloud Infrastructure Console, API, or CLI. The RMAN encryption password is typically required instead if the password was subsequently changed manually.

5. Click **Create Database**.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to create DB system components.

**DB systems:**

- ListDbSystems
- GetDbSystem
- LaunchDbSystem

**Database homes:**

- ListDbHomes
- GetDbHome
- CreateDbHome
- DeleteDbHome
Databases:

- ListDatabases
- GetDatabase

Shapes and database versions:

- ListDbSystemShapes
- ListDbVersions

For the complete list of APIs for the Database service, see Database Service API.

Setting up DNS for a DB System

DNS lets you use host names instead of IP addresses to communicate with a DB system. You can use the Internet and VCN Resolver (the DNS capability built into the VCN) as described in DNS in Your Virtual Cloud Network on page 2910.

Alternatively, you can use your choice of DNS server. You associate the host name and domain name to the public or private IP address of the DB system. You can find the host and domain names and IP addresses for the DB system in the Oracle Cloud Infrastructure Console on the Database page.

To associate the host name to the DB system's public or private IP address, contact your DNS administrator and request a custom DNS record for the DB system’s IP address. For example, if your domain is example.com and you want to use clouddb1 as the host name, you would request a DNS record that associates clouddb1.example.com to your DB system's IP address.

If you provide the public IP address to your DNS administrator as described above, you should also associate a custom domain name to the DB system's public IP address:

1. Register your domain name through a third-party domain registration vendor, such as register.com.
2. Resolve your domain name to the DB system's public IP address, using the third-party domain registration vendor console. For more information, refer to the third-party domain registration documentation.

Managing Bare Metal and Virtual Machine DB Systems

This topic explains how to perform a variety of management tasks for a bare metal or virtual machine database system. Tasks include:

- Starting, stopping, rebooting, and terminating a DB system
- Scaling the CPU count and storage
- Changing the shape of a virtual machine DB system
- Managing network security groups (NSGs) for your system
- Managing licenses for your DB system
- Checking the system status
- Moving a system to another compartment
- Creating a serial console connection to your DB system nodes
- Managing tags for your system
- Viewing work requests related to your system

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.
Using the Console

To check the status of a DB system

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.

   A list of database systems is displayed.
3. In the list of DB systems, find the system you're interested in and check its icon. The color of the icon and the text next to it indicates the status of the system.
   - **Provisioning**: Yellow icon. Resources are being reserved for the DB system, the system is booting, and the initial database is being created. Provisioning can take several minutes. The system is not ready to use yet.
   - **Available**: Green icon. The DB system was successfully provisioned. A few minutes after the system enters this state, you can SSH to it and begin using it.
   - **Terminating**: Gray icon. The DB system is being deleted by the terminate action in the Console or API.
   - **Terminated**: Gray icon. The DB system has been deleted and is no longer available.
   - **Failed**: Red icon. An error condition prevented the provisioning or continued operation of the DB system.

To view the status of a database node, under Resources, click Nodes to see the list of nodes. In addition to the states listed for a DB system, a node's status can be one of the following:
   - **Starting**: Yellow icon. The database node is being powered on by the start or reboot action in the Console or API.
   - **Stopping**: Yellow icon. The database node is being powered off by the stop or reboot action in the Console or API.
   - **Stopped**: Yellow icon. The database node was powered off by the stop action in the Console or API.

You can also check the status of database systems and database nodes by using the ListDbSystems or ListDbNodes API operations, which return the lifecycleState attribute.

To start, stop, or reboot a database system

DB system nodes are stopped, started, or rebooted individually. For multi-node DB systems, you may need to act on only one node (as in the case of proactively rebooting a virtual machine node with scheduled maintenance).

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.

   A list of database systems is displayed.
3. In the list of database systems, find the DB system you want to stop or start, and then click its name to display details about it.
4. In the list of nodes, click the Actions icon (three dots) for a node and then click one of the following actions:
   - **Start**: Restarts a stopped node. After the node is restarted, the **Stop** action is enabled.
   - **Stop**: Shuts down the node. After the node is powered off, the **Start** action is enabled.
   - **Reboot**: Shuts down the node, and then restarts it.

**Note:**

- Resource billing differs between bare metal and virtual machine DB systems as follows:
  - **Bare metal DB systems** - The **Stop** state has no effect on the resources you consume. Billing continues for nodes that you stop, and related resources continue to apply against any relevant quotas. You must **Terminate** a DB system to remove its resources from billing and quotas.
  - **Virtual machine DB systems** - Stopping a node stops billing for all OCPUs associated with that node. Billing resumes if you restart the node.
After you restart or reboot a node, the floating IP address might take several minutes to be updated and display in the Console.

To scale the CPU cores for a bare metal DB system

If a bare metal DB system requires more compute node processing power, you can scale up (increase) the number of enabled CPU cores in the system without impacting the availability of that system.

Note:
You cannot change the number of CPU cores for a virtual machine DB system in the same way. Instead, you must change the shape to one with a different number of OCPUs. See To change the shape of a virtual machine DB system on page 1384 to learn how.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of database systems is displayed.
3. In the list of DB systems, find the system you want to scale and click its highlighted name.
   The system details are displayed.
4. Click Scale CPU Cores, and then change the number in the CPU Core Count field. The text below the field indicates the acceptable values, based on the shape used when the DB system was launched.
5. Click Update.

To change the shape of a virtual machine DB system

After you provision a virtual machine DB system, you can change the shape at any time to adapt to changes in performance needs. For example, you might require a system with a higher number of OCPUs, or you might want to reduce costs by reducing the number of OCPUs. See Virtual Machine DB Systems on page 1355 for resource details for each shape in a series.

Note:
The shape-changer operation takes place in a rolling fashion for multi-node DB systems, allowing you to change the shape with no database downtime.

Changing the shape does not impact the amount of storage available to the DB system. However, the new shape can have different memory and network bandwidth characteristics, and you might need to reapply any customizations to these aspects after the change.

Prerequisites:
• DB system and database are in the Available state
• DB system is registered with the Cluster Ready Services (CRS) Grid Infrastructure stack. By default, virtual machine DB systems use CRS.
• Database can be successfully restarted
• Database is configured to use SPFILE (server parameter file), not PFILE. By default, databases in virtual machine DB systems use the SPFILE configuration.
• The SGA_TARGET parameter for Automatic Shared Memory Management (ASMM) has a non-zero value. By default, virtual machine DB systems use this ASMM configuration.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of database systems is displayed.
3. In the list of DB systems, find the system you want to scale and click its highlighted name.
   The system details are displayed.
4. Click Change Shape.
5. Select the new shape from the list of compatible and available shapes, and click **Change Shape**. Compatible shapes are those shapes within the same series. For example, if the current shape is VM.Standard 2.2, you can select another X7 shape that has not reached its usage limit in the selected availability domain.

   **Note:**

   If the current shape supports Oracle RAC, then you can only change that shape to another shape that also supports Oracle RAC. For example, you cannot change the shape from VM.Standard2.2 to VM.Standard2.1.

6. Review the information on the confirmation dialog, and proceed as applicable.

   **Tip:**

   If your shape change operation is not successful, see the troubleshooting tips in [Shape Change Failures for Virtual Machine DB Systems](#) on page 1663.

**To scale up the storage for a virtual machine DB system**

If a virtual machine DB system requires more block storage, you can increase the storage at any time without impacting the system.

   **Note:**

   This procedure does not apply to bare metal DB systems.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose your **Compartment**.

   A list of database systems is displayed.

3. In the list of DB systems, find the system you want to scale up and click its highlighted name.

   The system details are displayed.

4. Click **Scale Storage Up**, and then select the new available storage size from the drop-down list.

   The new total storage size displays in the total storage field. Oracle charges for the total storage used.

5. Click **Update**.

**To move a DB system to another compartment**

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose your **Compartment**.

   A list of database systems is displayed.

3. In the list of DB systems, find the system you want to move and click its highlighted name.

   The system details are displayed.

4. Click **Move Resource**.

5. Select the new compartment.

6. Click **Move Resource**.

   For information about dependent resources for Database resources, see [Moving Database Resources to a Different Compartment](#) on page 1141.
To terminate a DB system

Terminating a DB system permanently deletes it and any databases running on it.

**Note:**

The database data is local to the DB system and will be lost when the system is terminated. Oracle recommends that you back up any data in the DB system prior to terminating it.

Terminating a DB system removes all automatic incremental backups of all databases in the DB system from Oracle Cloud Infrastructure Object Storage. Full backups remain in Object Storage as standalone backups which you can use to create a new database. See Creating Databases on page 1414 for information on creating a new database from a backup.

**Important:** If your DB system has Data Guard enabled, you must terminate the standby DB system before terminating the primary DB system. If you try to terminate a primary DB system that has a standby, the terminate operation will not complete.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   
   A list of database systems is displayed.
3. For the DB system you want to terminate, click the Actions icon (three dots) and then click Terminate.
4. Confirm when prompted.
   
   The database system's icon indicates Terminating.

At this point, you cannot connect to the system and any open connections will be terminated.

To edit the network security groups (NSGs) for your DB system

Your DB system can use up to five network security groups (NSGs). Note that if you choose a subnet with a security list, the security rules for the DB system will be a union of the rules in the security list and the NSGs. For more information, see Network Security Groups on page 2841 and Network Setup for DB Systems on page 1359.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   
   A list of database systems is displayed.
3. In the list of DB systems, find the system you want to manage and click its highlighted name.
   
   The system details are displayed.
4. In the Network details, click the Edit link to the right of the Network Security Groups field.
5. In the Edit Network Security Groups dialog, click + Another Network Security Group to add an NSG to the DB system.
   
   To change an assigned NSG, click the drop-down menu displaying the NSG name, then select a different NSG.
   
   To remove an NSG from your DB system, click the X icon to the right of the displayed NSG name.
6. Click Save.

To manage your BYOL database licenses on your bare metal DB system

If you want to control the number of database licenses that you run at any given time on a bare metal system, you can scale up or down the number of OCPUs on the instance. These additional licenses are metered separately.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   
   A list of database systems is displayed.
3. In the list of DB systems, find the system you want to scale and click its highlighted name.
   The system details are displayed.
4. Click **Scale CPU Cores**, and then change the number.

*To change the license type of a bare metal or virtual machine DB system*

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. In the list of DB systems, find the DB system you want to administer and click its highlighted name.
4. On the DB system details page, click **Update License Type**.
   The dialog displays the options with your current license type selected.
5. Select the new license type.
6. Click **Save**.

See **Known Issue**.

*To manage tags for your DB systems and database resources*

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. Find the DB system or database resource you're interested in, and click the name.
4. Click the **Tags** tab to view or edit the existing tags. Or click **More Actions** and then **Apply Tags** to add new ones.

For more information, see **Resource Tags** on page 211.

*To view a work request for your DB systems and database resources*

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
   A list of database systems is displayed.
3. Find the DB system or database resource you're interested in, and click the name.
4. In the **Resources** section, click **Work Requests**. The status of all work requests appears on the page.
5. To see the log messages, error messages, and resources that are associated with a specific work request, click the operation name. Then, select an option in the **More information** section.
   For associated resources, you can click the Actions icon (three dots) next to a resource to copy the resource’s OCID.

For more information, see **Work Requests** on page 258.

*To create a serial console connection to your database system*

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
   A list of database systems is displayed.
3. Find the DB system or database resource you're interested in, and click the name.
4. In the **Resources** section, click **Console Connections**.
5. Click **Create Console Connection**. Note that if all nodes currently have existing console connections, this button will be disabled.
6. In the **Create Console Connection** dialog, specify the following:
   - The DB system node. For multi-node DB systems, select which node or nodes you wish to create a connection for. No node selector will display if the DB system has only one node, or if there is only one node in a multi-node system that currently lacks a connection.
   - The SSH key. You can browse or drag and drop .pub files, or paste in individual public keys.
7. Click **Create Console Connection**.
To delete a serial console connection to your database system

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of database systems is displayed.
3. Find the DB system or database resource you're interested in, and click the name.
4. In the Resources section, click Console Connections. Your current console connections are displayed.
5. To delete a connection, click the Actions icon (three dots) in the row listing the connection, then click Delete.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage DB system components.

- **database systems:**
  - ListDbSystems
  - GetDbSystem
  - UpdateDbSystem
  - ChangeDbSystemCompartment
  - TerminateDbSystem

- **Database homes:**
  - ListDbHomes
  - GetDbHome
  - DeleteDbHome

- **Databases:**
  - ListDatabases
  - GetDatabase

- **Nodes:**
  - DbNodeAction: Use this operation to power cycle a node in the database system.
  - ListDbNodes
  - GetDbNode

For the complete list of APIs for the Database service, see Database Service API.

Cloning a Virtual Machine DB System

This topic explains how to clone a virtual machine DB system that uses Logical Volume Manager storage management software. See Fast Provisioning Option for Single-Node Virtual Machine DB Systems on page 1355 for more information on these virtual machine DB systems.

Cloning creates a copy of a source DB system as it exists at the time of the cloning operation, including the storage configuration software and database volumes. When creating a clone, you can specify a new SSH key and ADMIN password.

Note:

- Cloning is not supported for bare metal DB systems or virtual machine systems using Oracle Automatic Storage Management.
- You can't clone a virtual machine DB system in a security zone to create a virtual machine DB system that isn't in a security zone. See the Security Zone Policies topic for a full list of policies that affect Database service resources.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more information about writing policies for databases, see Details for the Database Service on page 2240.

Using the Console to Clone a Virtual Machine DB System

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the compartment where the source DB system is located.
3. In the list of DB systems, find the virtual machine DB system you want to clone and click its highlighted name.
   Note that only system using Logical Volume Manager storage management software can be cloned.
4. On the DB System Details page of your source DB system, click Clone. This opens the Clone DB System dialog.
5. Select a compartment: By default, the DB system is created in your current compartment and you can use the network resources in that compartment.
6. Display name: A non-unique, display name for the DB system. An Oracle Cloud Identifier (OCID) uniquely identifies the DB system. Avoid entering confidential information.
7. Add public SSH keys: The public key portion of each key pair you want to use for SSH access to the DB system.
   You can browse or drag and drop .pub files, or paste in individual public keys. To paste multiple keys, click + Another SSH Key, and supply a single key for each entry.
   The clone will use the SSH keys specified during the cloning operation, and the source DB system will continue to use the SSH keys that were in place prior to the cloning operation.
8. Choose a license type: The type of license you want to use for the DB system. Your choice affects metering for billing.
   - License Included means the cost of this Oracle Cloud Infrastructure Database service resource will include both the Oracle Database software licenses and the service.
   - Bring Your Own License (BYOL) means you will use your organization's Oracle Database software licenses for this Oracle Cloud Infrastructure Database service resource. See Bring Your Own License for more information.
   Note that this license selection only applies to the clone, and does not affect the source DB system.
9. Specify the network information:
   - Virtual cloud network: The VCN in which to create the DB system. Click Change Compartment to select a VCN in a different compartment. Note that the clone can use a different VCN and subnet from the source DB system.
   - Client Subnet: The subnet to which the DB system should attach. For 1- and 2-node RAC DB systems:
     Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.
     Click Change Compartment to select a subnet in a different compartment.
   - Network Security Groups: Optionally, you can specify one or more network security groups (NSGs) for your DB system. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules
to your DB system. A maximum of five NSGs can be specified. For more information, see Network Security Groups on page 2841 and Network Setup for DB Systems on page 1359.

Note that if you choose a subnet with a security list, the security rules for the DB system will be a union of the rules in the security list and the NSGs.

- **Hostname prefix:** Your choice of host name for the bare metal or virtual machine DB system. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for bare metal and virtual machine DB systems is 16.

  \[\text{Important:}\]
  
  The host name must be unique within the subnet. If it is not unique, the DB system will fail to provision. If the clone is created in a different subnet from the source, the same host name can be used for both the clone and the source DB system.

- **Host domain name:** The domain name for the DB system. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, then this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. Hyphens (-) are not permitted.

- **Host and domain URL:** Combines the host and domain names to display the fully qualified domain name (FQDN) for the database. The maximum length is 64 characters.

- **Private IP address:** Optionally, you can define the IP address of the clone. This is useful in development contexts where you create and delete clones of the same source DB system over and over, and you need each new iteration of the clone to use the same IP address. If you specify an IP address that is currently in use within the subnet, the cloning operation will fail with an error message regarding the invalid IP address.

10. **Fault domain:** The fault domain in which the DB system resides. You can choose which fault domain to use for your DB system. For more information on fault domains, see About Regions and Availability Domains on page 180.

11. Provide information for the initial database of the clone:

- **Database name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted. You can use the same database name that is used in the source DB system.

- **Password:** A strong password for the SYS user. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS or SYSTEM) or the word "oracle" either in forward or reversed order and regardless of casing. The password will be used for the SYS and SYSTEM administrator accounts.

  \[\text{Important:}\] The TDE wallet password is inherited from the source DB system.

- **Confirm password:** Re-enter the password you specified.

12. Clicking **Show Advanced Options** allows you to configure the following:

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

13. Click **Clone DB System**.

**Connecting to a DB System**

This topic explains how to connect to an active DB system. How you connect depends on the client tool or protocol you use, the purpose of the connection, and how your cloud network is set up. You can find information on various networking scenarios in Networking Overview on page 2748, but for specific recommendations on how you should connect to a database in the cloud, contact your network security administrator.
Prerequisites
This section describes prerequisites you'll need to perform various tasks in this topic.

- To use the Console or the API to get the default administration service connection strings, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. See Authentication and Authorization for more information on user authorizations for the Oracle Cloud Infrastructure Database service.

- To connect to the database, you'll need the public or private IP address of the DB system.

Use the private IP address to connect to the system from your on-premises network, or from within the virtual cloud network (VCN). This includes connecting from a host located on-premises connecting through a VPN or FastConnect to your VCN, or from another host in the same VCN. Use the Exadata system’s public IP address to connect to the system from outside the cloud (with no VPN). You can find the IP addresses in the Oracle Cloud Infrastructure Console as follows:

- Cloud VM clusters (new resource model): On the Exadata VM Cluster Details page, click Virtual Machines in the Resources list.
- DB systems: On the DB System Details page, click Nodes in the Resources list.

The values are displayed in the Public IP Address and Private IP Address & DNS Name columns of the table displaying the Virtual Machines or Nodes of the Exadata Cloud Service instance.

- For Secure Shell (SSH) access to the DB system, you'll need the full path to the file that contains the private key associated with the public key used when the DB system was launched.

If you have problems connecting, see Troubleshooting Connection Issues on page 1396.

Database Services and Connection Strings
Database services allow you to control client access to a database instance depending on the functionality needed. For example, you might need to access the database for administration purposes only or you might need to connect an application to the database. Connection strings are specific to a database service.

When you provision a DB system, a default database administration service is automatically created. For 12c and later Oracle Databases, this service is for administrating the database at the CDB level. Because this service provides limited functionality, it is not suitable for connecting an application. Oracle recommends that you create a default application service for the initial database after you create your DB system. For 12c and later Oracle Databases, application services connect at the PDB level. Here are some important functions an application service can provide:

- Workload identification
- Load balancing
- Application continuity and Transaction Guard
- Fast Application Notification
- Resource assignment based on the service name

For details about these and other High Availability capabilities, see Client Failover Best Practices for Highly Available Oracle Databases.

Creating an Application Service
You use the srvctl utility to create an application service. Before you can connect to the service, you must start it.

To create an application service for a PDB or an 11g Oracle database

1. Log in to the DB system host as opc.
2. Switch to the oracle user, and set your environment to the Oracle Database you want to administer.

```bash
$ sudo su - oracle
$ . oraenv
ORACLE_SID = [oracle] ? <database_name>
```
The Oracle base has been set to /u01/app/oracle

3. Create the application service for the database. Include the pdb option only if you are creating an application service for a PDB.

```bash
$ srvctl add service
   -db <DB_unique_name>
   -pdb <PDB_name>
   -service <app_service_name>
   -role PRIMARY
   -notification TRUE
   -session_state dynamic
   -failovertype transaction
   -failovermethod basic
   -commit_outcome TRUE
   -failoverretry 30
   -failoverdelay 10
   -replay_init_time 900
   -clbgoal SHORT
   -rlbgoal SERVICE_TIME
   -preferred <rac_node1>,<rac_node2>
   -retention 3600
```

Note that the preferred option is required only for multi-node databases to specify the hostname of the node in the RAC.

4. Start the application service.

```bash
$ srvctl start service -db <DB_unique_name> -s <app_service_name>
```

For more information about services for a PDB, see Managing Services for PDBs.

**Database Connection Strings**

You must use the appropriate connection string to access a database administration or application service. You can use the Console or the API to get the string for connecting to the default administration service from within a VCN. For 12c and later Oracle Databases, this service is for administrating the database at the CDB level. The string is provided in both the Easy Connect and in the full connect descriptor (long) format. Use the long format for the connection if hostname resolution is not available. You can also use the long format to create an alias in the tnsnames.ora file.

For accessing a database service within the VCN, the connection string for a Real Application Cluster (RAC) DB system uses the Single Client Access Name (SCAN) while the connection string for single instance DB system uses the hostname instead.

The private SCAN name is a Round Robin DNS entry created when you launch a 2-node RAC DB system. The private SCAN name is resolvable only within the VCN. If the client and the database are in the same VCN, the connection mechanism is the same as an on-premises RAC database; all the features provided by VIPs and SCAN VIPs, such as server side load balancing and VIP failover, are available.

**Note:**

If you manually change the DB_UNIQUE_NAME, DB_DOMAIN, or listener port on the DB system, the connection strings you see in the Console or API will not reflect your changes. Ensure that you use the actual values of these parameters when you make a connection.

To get the connection strings for the default administration service

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Find the DB system you're interested in, and click the name.
4. Click **DB Connection**.
5. Click the applicable link to view or copy the connection string.

You can derive the connection strings for other database services by replacing part of the default application service connection string with the applicable values.

**To derive the connection string for a PDB administration service or an application service**

1. Follow the procedure to get the Easy Connect string for the default administration service. That string should have the following format:

   ```
   <hostname|SCAN>:1521/<DB_unique_name>.<DB_domain>
   ```

2. Make the appropriate substitution:
   - For the PDB administration service, replace **DB_unique_name** with the PDB name.
     ```
     <hostname|SCAN>:1521/<PDB_name>.<DB_domain>
     ```
   - For an application service, replace **DB_UNIQUE_NAME** with the name of the application service.
     ```
     <hostname|SCAN>:1521/<app_service_name>.<DB_domain>
     ```

### Connecting to a Database Service by Using SQL*Net

This section describes how to connect to a database service from a computer that has a SQL*Net client installed. Port 1521 must be open to support the SQL*Net protocol.

#### Connecting from Within the VCN

For security reasons, Oracle recommends that you connect to your database services from within the VCN. You can use this method whether you are connecting to an administration service or to an application service.

To connect using SQL*Plus, you run the following command using the applicable connection string:

```
sqlplus system/<password>@<connection_string>
```

Consider the following:

- If your system is not using the VCN Resolver, ensure that the DB system's hostname (for single-node systems) or SCAN name (for multi-node systems) can be resolved. See [DNS in Your Virtual Cloud Network](#) on page 2910 for information about DNS name resolution.
- For connecting to the administration service of a PDB, ensure that the PDB is open or the service will not be available.
- For connecting to an application service, ensure that the service is started. For Fast Application Notification to work, ensure that port 6200 can be reached. See [Client Failover Best Practices for Highly Available Oracle Databases](#) for information about Fast Application Notification.

#### Connecting from the Internet

Although Oracle does not recommend connecting to your database from the Internet, you can connect to a database service by using a public IP address if port 1521 is open to the public for ingress.

To use this method, you run the following command using the public IP address instead of the hostname or SCAN in the connection string:

```
sqlplus system/<password>@<public_IP>:1521/<service_name>.<DB_domain>
```

Consider the following:

- SCANs and hostnames are not resolvable on the Internet, therefore load balancing and failover for multi-node DB systems, which rely on these names, cannot work.
• For multi-node DB systems, which normally use SCANs, you must specify the IP address of one of the RAC hosts to access the database.

**Important:**

Do not use this method to connect to the database from within the VCN. Doing so negatively impacts performance because traffic to the database is routed out of the VCN and back in through the public IP address.

**Example: Connecting in SQL Developer Using SQL*Net**

**Prerequisites:**

• Ensure that port 1521 is open for the Oracle default listener. (You can do this by checking the DB system's security list.)
• If port 1521 is open only to hosts in the VCN, then you must run your SQL Developer client from a machine that has direct access to the VCN. If you are connecting to the database from the Internet instead, then the public IP address of your computer must be granted access to port 1521 in the security list. (Alternatively, the security list can grant full access to port 1521, however, this is not recommended for security reasons.) You must use the public IP address of the host because connecting from the Internet does not support SCAN name resolution.

**To connect from within the VCN using a private IP address**

After the prerequisites are met, start SQL Developer and create a connection by supplying the following connection details:

• **Username:** sys as sysdba
• **Password:** The Database Admin Password that was specified in the Launch DB System dialog in the Console.
• **Hostname:** The hostname as it appears in the Easy Connect format of the connection string. (See Database Connection Strings on page 1392 for help with getting the connection string and identifying the hostname.)
• **Port:** 1521
• **Service name:** The concatenated name of the service and host domain name, for example, `db1_phx1tv.example.com`. You can identify this value as the last part of the Easy Connect string, `<service_name>.<DB_domain>`.

**Connecting to a Database with a Public IP by Using SSH Tunneling**

You can access the services of DB system databases with public IP addresses by using SSH tunneling. The main advantage of this method is that port 1521 does not need to be opened to the public internet. However, just like accessing the database with a public IP using a SQL*Net client, load balancing and failover for multi-node DB systems cannot work because they rely on SCANs and hostnames.

Oracle SQL Developer and Oracle SQLcL and are two tools that facilitate the use of tunneling for Oracle Database access.

To open a tunnel, and then connect to a database service by using SQLcL, you run commands like the following:

```
SQL> sshtunnel opc@<public_IP> -i <private_key> -L <local_port>:<private_IP>:1521
Using port:22
SSH Tunnel connected
SQL> connect
system/<password>@localhost:<local_port>/<service_name>.<DB_domain>
```

See Oracle SQL Developer and Oracle SQLcL for information about these tools.

**Connecting to a Database by Using SSH and the Bequeath Protocol**

This method allows you to connect to the database without using the network listener. It should be used to connect only for administration purposes.

When connecting to a multi-node DB system, you'll SSH to each individual node in the cluster.
To connect from a UNIX-style system

Use the following SSH command to access the DB system: $ ssh -i <private_key> 
opc@<DB_system_IP_address>

<private_key> is the full path and name of the file that contains the private key associated with the DB system you want to access.

Use the DB system’s private or public IP address depending on your network configuration. For more information, see Prerequisites on page 1391.

To connect from a Windows system

1. Open putty.exe.

2. In the Category pane, select Session and enter the following fields:
   - Host Name (or IP address): opc@<DB_system_IP_address>
     Use the DB system’s private or public IP address depending on your network configuration. For more information, see Prerequisites on page 1391.
   - Connection type: SSH
   - Port: 22

3. In the Category pane, expand Connection, expand SSH, and then click Auth, and browse to select your private key.

4. Optionally, return to the Session category screen and save this session information for reuse later.

5. Click Open to start the session.

To access a database after you connect

1. Log in as opc and then sudo to the grid user.

   login as: opc
   [opc@ed1db01 ~]$ sudo su - grid

2. List all the databases on the system.

   root@ed1db01 ]# srvctl config database -v
cdbm01 /u02/app/oracle/product/12.1.0/dbhome_2 12.1.0.2.0
exadb /u02/app/oracle/product/11.2.0/dbhome_2 11.2.0.4.0
mmdb /u02/app/oracle/product/12.1.0/dbhome_3 12.1.0.2.0

3. Connect as the oracle user and get the details about one of the databases by using the srvctl command.

   [root@ed1db01 ~]$ su - oracle
   [oracle@ed1db01 ~]$ . oraenv
   ORACLE_SID = [oracle] ? cdbm01
   The Oracle base has been set to /u02/app/oracle
   [oracle@ed1db01 ~]$ srvctl config database -d cdbm01
   Database unique name: cdbm01 <<== DB unique name
   Database name: Oracle home: /u02/app/oracle/product/12.1.0/dbhome_2
   Oracle user: oracle
   Spfile: +DATAC1/cdbm01/spfilecdbm01.ora
   Password file: +DATAC1/cdbm01/PASSWORD/passwd
   Domain: data.customer1.oraclevcn.com
   Start options: open
   Stop options: immediate
   Database role: PRIMARY
   Management policy: AUTOMATIC
   Server pools:
   Disk Groups: DATAC1,RECO1
Mount point paths:
Services:
Type: RAC
Start concurrency:
Stop concurrency:
OSDBA group: dba
OSOPER group: racoper
Database instances: cdbm011,cdbm012 <== SID
Configured nodes: ed1db01,ed1db02
Database is administrator managed

4. Set the ORACLE_SID and ORACLE_UNIQUE_NAME using the values from the previous step.

[oracle@ed1db01 ~]$ export ORACLE_UNIQUE_NAME=cdbm01
[oracle@ed1db01 ~]$ export ORACLE_SID=cdbm011
[oracle@ed1db01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 12.1.0.2.0 Production on Wed Apr 19 04:10:12 2017
Copyright (c) 1982, 2014, Oracle. All rights reserved.

Connected to:
Oracle Database 12c EE Extreme Perf Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Real Application Clusters, Automatic Storage
Management, Oracle Label Security, OLAP, Advanced Analytics and Real Application Testing options

Serial Console Access for Troubleshooting and Managing a Bare Metal or VM System
You can create and delete serial console connections to your bare metal or virtual machine DB system in the Oracle
Cloud Infrastructure Console. This allows you to manage and troubleshoot your system in single-user mode using an
SSH connection. See the following topics for more information:

- To create a serial console connection to your database system on page 1387
- To delete a serial console connection to your database system on page 1388

Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on
page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the GetDatabase API operation to get the default administration service connection strings.

Troubleshooting Connection Issues
The following issues might occur when connecting to a DB system or database.

ORA-28365: Wallet is Not Open Error
For a 1-node DB system or 2-node RAC DB system, regardless of how you connect to the DB system, before
you use OS authentication to connect to a database (for example, sqlplus / as sysdba) be sure to set
the ORACLE_UNQNAME variable. Otherwise, commands that require the TDE wallet will result in the error
ORA-28365: wallet is not open.

Note that this is not an issue when using a TNS connection because ORACLE_UNQNAME is automatically set in the
database CRS resource.

SSH Access Stops Working
If the DB system’s root volume becomes full, you might lose the ability to SSH to the system (the SSH command
will fail with permission denied errors). Before you copy a large amount of data to the root volume, for example, to
migrate a database, use the dbcli create-dbstorage command to set up storage on the system’s NVMe drives.
and then copy the database files to that storage. For more information, see Setting Up Storage on the DB System on page 1637.

**What Next?**

Before you begin updating your DB system, review the information in Updating a DB System on page 1397.

For information about setting up an Enterprise Manager console to monitor your databases, see Monitoring a Database on page 1427.

**Updating a DB System**

---

**Note:**

This topic is not applicable to Exadata DB systems. For information on how to update an Exadata DB system, see Updating an Exadata Cloud Service Instance on page 1274.

This topic includes information and instructions on how to update the OS of a bare metal or virtual machine DB system.

---

**Caution:**

- Review all of the information before you begin updating the system. Updating the operating system through methods not described on this page can cause permanent loss of access.
- Always back up your databases prior to updating your DB system's operating system.

**Bash Profile Updates**

Do not add interactive commands such as `oraenv`, or commands that might return an error or warning message, to the `.bash_profile` file for the grid or oracle users. Adding such commands can prevent Database service operations from functioning properly.

**Essential Firewall Rules**

For a 1-node DB system or 2-node RAC DB system, do not remove or modify the following firewall rules in `/etc/sysconfig/iptables`:

- The firewall rules for ports 1521, 7070, and 7060 allow the Database service to manage the DB system. Removing or modifying them can result in the Database Service no longer operating properly.
- The firewall rules for 169.254.0.2:3260 and 169.254.0.3:80 prevent non-root users from escalating privileges and tampering with the system’s boot volume and boot process. Removing or modifying these rules can allow non-root users to modify the system's boot volume.

**OS Updates**

Before you update the OS, review the following important guidelines and information:

- Back up your DB system's databases prior to attempting an OS update.
- Do not remove packages from a DB system. However, you might have to remove custom RPMs (packages that were installed after the system was provisioned) for the update to complete successfully.

---

**Caution:**

Do not install NetworkManager on the DB system. Installing this package and reboots the system results in severe loss of access to the system.

- Oracle recommends that you test any updates thoroughly before updating a production system.
- The image used to launch a DB system is updated regularly with the necessary patches. After you launch a DB system, you are responsible for applying the required OS security updates published through the Oracle public YUM server.
To apply OS updates, the DB system's VCN must be configured to allow access to the YUM repository. For more information, see Network Setup for DB Systems on page 1359.

**To update an OL7 OS on a DB system host**

You can update the OS on 2-node RAC virtual machine DB systems in a rolling fashion.

*Note:* Ensure the Oracle Clusterware (CRS) is completely shut down before performing the OS kernel updates.

1. Log on to the DB system host as opc, and then sudo to the root user.

   ```bash
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ``

2. If your DB system uses an image with the kernel version 4.1.12-124.27.1.el7uek (used with older images), then change the bootefi label before updating the OS.

3. Identify the host region by running the following command:

   ```bash
   # curl -s http://169.254.169.254/opc/v1/instance/ | grep region
   ``

4. With the region noted from the previous step, determine the region name, and perform the following two steps.

   See Regions and Availability Domains on page 180 to look up the region name.

   **a.** Download the repo.

   ```bash
   # wget https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/dbaaspatchstore/DBaaSOSPatches/oci_dbaas_ol7repo -O /tmp/oci_dbaas_ol7repo
   ``

   This example output assumes the region is us-phoenix-1 (PHX).

   ```bash
   # wget https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/dbaaspatchstore/DBaaSOSPatches/oci_dbaas_ol7repo -O /tmp/oci_dbaas_ol7repo
   Resolving swiftobjectstorage.us-phoenix-1.oraclecloud.com...
   129.146.13.177, 129.146.13.180, 129.146.12.235, ...
   Connecting to swiftobjectstorage.us-phoenix-1.oraclecloud.com|129.146.13.177|:443... connected.
   HTTP request sent, awaiting response... 200 OK
   Length: 1394 (1.4K) [binary/octet-stream]
   Saving to: `/tmp/oci_dbaas_ol7repo'
   100%[==============================================] 1,394 --.-K/s in 0s
   ```
b. Download the version lock files.

```bash
# wget https://swiftobjectstorage.<region_name>.oraclecloud.com/
v1/dbaaspatchstore/DBaaSOSPatches/versionlock_ol7.list -O /tmp/
versionlock.list
```

This example output assumes the region is us-phoenix-1 (PHX).

```bash
# wget https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/
v1/dbaaspatchstore/DBaaSOSPatches/versionlock_ol7.list -O /tmp/
versionlock.list
```

5. Copy the repo file to the `/etc/yum.repos.d` directory.

```bash
cp /tmp/oci_dbaas_ol7repo /etc/yum.repos.d/ol7.repo
```

6. Copy and overwrite the existing version lock file.

```bash
cp /etc/yum/pluginconf.d/versionlock.list /etc/yum/pluginconf.d/
versionlock.list-`date +%Y%m%d`
cp /tmp/versionlock.list /etc/yum/pluginconf.d/versionlock.list
```

The initial version lock file should be empty. However, it is a good practice to back it up in case it is not and you need to refer to it later.

7. Run the update command.

```bash
|  18 MB 00:00 |
# yum update
Loaded plugins: kernel-update-handler, ulninfo, versionlock
Excluding 250 updates due to versionlock (use "yum versionlock status" to show them)
Resolving Dependencies
---> Running transaction check
----> Package kernel-uek.x86_64 0:4.1.12-124.28.5.el7uek will be installed
----> Package kernel-uek-firmware.noarch 0:4.1.12-124.28.5.el7uek will be
    installed
----> Package libtalloc.x86_64 0:2.1.10-1.el7 will be updated
----> Package libtalloc.x86_64 0:2.1.13-1.el7 will be an update
----> Package pytalloc.x86_64 0:2.1.10-1.el7 will be updated
----> Package pytalloc.x86_64 0:2.1.13-1.el7 will be an update
---> Finished Dependency Resolution
```
## Dependencies Resolved

<table>
<thead>
<tr>
<th>Package</th>
<th>Arch</th>
<th>Version</th>
<th>Repository</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>kernel-uek</td>
<td>x86_64</td>
<td>4.1.12-124.28.5.el7uek</td>
<td>ol7_UEKR4</td>
<td>44 M</td>
</tr>
<tr>
<td>kernel-uek-firmware</td>
<td>noarch</td>
<td>4.1.12-124.28.5.el7uek</td>
<td>ol7_UEKR4</td>
<td>1.0 M</td>
</tr>
<tr>
<td>libtalloc</td>
<td>x86_64</td>
<td>2.1.13-1.el7</td>
<td>ol7_latest</td>
<td>31 k</td>
</tr>
<tr>
<td>pytalloc</td>
<td>x86_64</td>
<td>2.1.13-1.el7</td>
<td>ol7_latest</td>
<td>16 k</td>
</tr>
</tbody>
</table>

### Transaction Summary

- **Install**: 2 Packages
- **Upgrade**: 2 Packages
- Total download size: 46 M
- Is this ok [y/d/N]: y

Downloading packages:
- No Presto metadata available for ol7_UEKR4
- No Presto metadata available for ol7_latest

(1/4): kernel-uek-firmware-4.1.12-124.28.5.el7uek.noarch.rpm  | 1.0 MB 00:00:00
(2/4): libtalloc-2.1.13-1.el7.x86_64.rpm                 | 31 kB 00:00:00
(3/4): pytalloc-2.1.13-1.el7.x86_64.rpm                 | 16 kB 00:00:00
(4/4): kernel-uek-4.1.12-124.28.5.el7uek.x86_64.rpm    | 44 MB 00:00:01

Total 41 MB/s | 46 MB 00:00:01

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

**Warning: RPMDB altered outside of yum.**

**Found 7 pre-existing rpmdbs, 'yum check' output follows:**
oda-hw-mgmt-19.3.0.0.0_LINUX.X64_190530-1.x86_64 has missing requires of libnfsodm19.so() (64bit)
oda-hw-mgmt-19.3.0.0.0_LINUX.X64_190530-1.x86_64 has missing requires of perl(GridDefParams)
oda-hw-mgmt-19.3.0.0.0_LINUX.X64_190530-1.x86_64 has missing requires of perl(Sys::Syslog)
oda-hw-mgmt-19.3.0.0.0_LINUX.X64_190530-1.x86_64 has missing requires of perl(a_GridSteps)
perl-RPC-XML-0.78-3.el7.noarch has missing requires of perl(DateTime) >= ('0', '0.70', None)
perl-RPC-XML-0.78-3.el7.noarch has missing requires of perl(DateTime::Format::ISO8601) >= ('0', '0.07', None)
perl-RPC-XML-0.78-3.el7.noarch has missing requires of perl(Module::Load) >= ('0', '0.24', None)
Installing : kernel-uek-firmware-4.1.12-124.28.5.el7uek.noarch 1/6
Updating   : libtalloc-2.1.13-1.el7.x86_64 2/6
Updating : pytalloc-2.1.13-1.el7.x86_64 3/6
Installing : kernel-uek-4.1.12-124.28.5.el7uek.x86_64 4/6
Cleanup    : pytalloc-2.1.10-1.el7.x86_64 5/6
Cleanup    : libtalloc-2.1.10-1.el7.x86_64 6/6

Note:
• Ignore the error activating message that results from running the update.
• An update will occur only if a versionlock file has a valid update available to apply to the DB system.

8. Restart the system.

$ sudo su -
# reboot

9. Run the following command to validate the update:

# uname -r
4.1.12-124.28.5

In this example, then new kernel version is 4.1.12-124.28.5.

To check the kernel version
Run the following command.

$ uname -r

Example response indicating kernel version 4.1.12-124.27.1.el7uek:

4.1.12-124.27.1.el7uek.x86_64

If you have kernel version 4.1.12-124.27.1.el7uek, then proceed to change the bootefi label.

To change the bootefi label (each node)

1. Edit /etc/fstab: Change the label bootefi to BOOTEFI (uppercase).

Example:

LABEL=BOOTEFI             /boot/efi             vfat    defaults        1

2. Restart the DB node.

3. Run the following command to ensure that the required link is created.

$ sudo ls -lrt /etc/grub2-efi.cfg

Example response indicating that the required link exists:

lrwxrwxrwx 1 root root 31 Sep  4 11:49 /etc/grub2-efi.cfg -> ../boot/efi/EFI/redhat/grub.cfg

To update an OL6 OS on a DB system host
You can update the OS on 2-node RAC virtual machine DB systems in a rolling fashion.
Note:
Ensure the Oracle Clusterware (CRS) is completely shut down before performing the OS kernel updates.

1. Log on to the DB system host as opc, and then sudo to the root user.
   
   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

2. Identify the host region by running the following command:
   
   ```
   # curl -s http://169.254.169.254/opc/v1/instance/ | grep region
   ```

3. With the region you noted from the previous step, determine the region name, and perform the following two steps.
   
   See Regions and Availability Domains on page 180 to look up the region name.

   a. Download the repo.
      
      ```
      # wget https://swiftobjectstorage.<region_name>.oraclecloud.com/
      v1/dbaaspatchstore/DBaaSOSPatches/oci_dbaas_ol6repo -O /tmp/
      oci_dbaas_ol6repo
      ```
      
      This example output assumes the region is us-phoenix-1 (PHX).

      ```
      # wget https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/
      v1/dbaaspatchstore/DBaaSOSPatches/oci_dbaas_ol6repo -O /tmp/
      oci_dbaas_ol6repo
      Resolving swiftobjectstorage.us-phoenix-1.oraclecloud.com... 129.146.13.177, 129.146.13.180, 129.146.12.235, ...
      Connecting to swiftobjectstorage.us-phoenix-1.oraclecloud.com 129.146.13.177:443... connected.
      HTTP request sent, awaiting response... 200 OK
      Length: 1394 (1.4K) [binary/octet-stream]
      Saving to: `/tmp/oci_dbaas_ol6repo'
      100%[======================================================================================================================================================================================================================================>
      1,394 --.-K/s in 0s
      2018-03-16 10:40:42 (34.5 MB/s) - `/tmp/oci_dbaas_ol6repo' saved [1394/1394]
      ```

   b. Download the version lock files.
      
      ```
      # wget https://swiftobjectstorage.<region_name>.oraclecloud.com/
      v1/dbaaspatchstore/DBaaSOSPatches/versionlock_ol6.list -O /tmp/
      versionlock.list
      ```
      
      This example output assumes the region is us-phoenix-1 (PHX).

      ```
      # wget https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/
      v1/dbaaspatchstore/DBaaSOSPatches/versionlock_ol6.list -O /tmp/
      versionlock.list
      Resolving swiftobjectstorage.us-phoenix-1.oraclecloud.com... 129.146.12.224, 129.146.12.164, 129.146.14.172, ...
      ```
Connecting to swiftobjectstorage.us-phoenix-1.oraclecloud.com|129.146.12.224|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15769 (15K) [binary/octet-stream]
Saving to: `~/tmp/versionlock.list'

100%[======================================================================================================================================================================================================================================>
15,769 --.-K/s in 0.1s

2018-03-16 10:41:39 (123 KB/s) - `~/tmp/versionlock.list' saved [15769/15769]

4. Enable the repo for your region.
   a. Copy the repo file to the /etc/yum.repos.d directory.

```bash
cp /tmp/oci_dbaas_ol6repo /etc/yum.repos.d/ol6.repo
```

b. Modify the ol6.repo file to enable the repo for your region.

```bash
vi /etc/yum.repos.d/ol6.repo
```

```bash
[ol6_latest_PHX]
name=Oracle Linux $releasever Latest ($basearch)
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1 <= Enabled.

[ol6_UEKR4_PHX]
name=Latest Unbreakable Enterprise Kernel Release 4 for Oracle Linux $releasever ($basearch)
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1 <= Enabled.
```

5. Install yum-plugin-versionlock.

```bash
$ sudo su -
# yum repolist
Loaded plugins: kernel-update-handler, security, ulninfo
ol6_UEKR4
ol6_UEKR4/primary
ol6_UEKR4
588/588
ol6_latest
ol6_latest/primary
ol6_latest
39825/39825
repo id repo name
status
ol6_UEKR4 Latest Unbreakable Enterprise Kernel Release 4 for Oracle Linux 6Server (x86_64) 588
```
[root@jigsosupg ~]# yum install yum-plugin-versionlock
Loaded plugins: kernel-update-handler, security, ulninfo
Setting up Install Process
Resolving Dependencies
---> Running transaction check
---> Package yum-plugin-versionlock.noarch 0:1.1.30-40.0.1.el6 will be installed
---> Finished Dependency Resolution

Dependencies Resolved

Package | Arch
---------|------
Version | Repository
Size

Installing:
yum-plugin-versionlock noarch
1.1.30-40.0.1.el6 ol6_latest
32 k

Transaction Summary

Install 1 Package(s)
Total download size: 32 k
Installed size: 43 k
Is this ok [y/N]: y

Downloading Packages:
yum-plugin-versionlock-1.1.30-40.0.1.el6.noarch.rpm | 32 kB 00:00

Warning: rpmmts_HdrFromFdno: Header V3 RSA/SHA256 Signature, key ID ec551f03: NOKEY
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
Importing GPG key 0xEC551F03:
Userid : Oracle OSS group (Open Source Software group)
<build@oss.oracle.com>
Package: 6:oraclelinux-release-6Server-8.0.3.x86_64 (@odadom1)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Warning: RPMDB altered outside of yum.
** Found 4 pre-existing rpmdb problem(s), 'yum check' output follows:
oda-hw-mgmt-12.2.0.1.0_LINUX.X64_170614.TR1221-1.x86_64 has missing requires of /usr/local/bin/perl
oda-hw-mgmt-12.2.0.1.0_LINUX.X64_170614.TR1221-1.x86_64 has missing requires of libnfsodm12.so()(64bit)
oda-hw-mgmt-12.2.0.1.0_LINUX.X64_170614.TR1221-1.x86_64 has missing requires of perl(GridDefParams)
oda-hw-mgmt-12.2.0.1.0_LINUX.X64_170614.TR1221-1.x86_64 has missing requires of perl(s_GridSteps)
Installing : yum-plugin-versionlock-1.1.30-40.0.1.el6.noarch
1/1
Verifying : yum-plugin-versionlock-1.1.30-40.0.1.el6.noarch
1/1
Installed:
  yum-plugin-versionlock.noarch 0:1.1.30-40.0.1.el6

Complete!

**Note:**

Ignore the RPMDB warning messages that refer to oda-hw-mgmt.

6. Copy and overwrite the existing version lock file.

```bash
cp /etc/yum/pluginconf.d/versionlock.list /etc/yum/pluginconf.d/
    versionlock.list-`date +%Y%m%d`

cp /tmp/versionlock.list /etc/yum/pluginconf.d/versionlock.list
```

The initial version lock file should be empty. However, it is a good practice to back it up in case it is not and you need to refer to it later.

7. Run the update command.

```bash
# yum update
Loaded plugins: kernel-update-handler, security, ulninfo, versionlock
Setting up Update Process
---> Running transaction check
-----> Package kernel-uek.x86_64 0:4.1.12-112.14.13.el6uek will be installed
-----> Package kernel-uek-firmware.noarch 0:4.1.12-112.14.13.el6uek will be installed
-----> Package linux-firmware.noarch 0:20160616-44.git43e96ae.0.12.el6 will be updated
-------> Package linux-firmware.noarch 0:20171128-56.git17e62881.0.2.el6 will be an update
---> Finished Dependency Resolution
```

**Transaction Summary**

<table>
<thead>
<tr>
<th>Package</th>
<th>Arch</th>
<th>Repository</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kernel-uek</td>
<td>x86_64</td>
<td>ol6_UEKR4</td>
<td></td>
</tr>
<tr>
<td>4.1.12-112.14.13.el6uek</td>
<td>51 M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kernel-uek-firmware</td>
<td>noarch</td>
<td>ol6_UEKR4</td>
<td></td>
</tr>
<tr>
<td>4.1.12-112.14.13.el6uek</td>
<td>2.4 M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updating:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>linux-firmware</td>
<td>noarch</td>
<td>ol6_UEKR4</td>
<td></td>
</tr>
<tr>
<td>20171128-56.git17e62881.0.2.el6</td>
<td>74 M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total download size: 128 M
Is this ok [y/N]: y

Downloading Packages:
(1/3): kernel-uek-4.1.12-112.14.13.el6uek.x86_64.rpm | 51 MB 00:00
(2/3): kernel-uek-firmware-4.1.12-112.14.13.el6uek.noarch.rpm | 2.4 MB 00:00
(3/3): linux-firmware-20171128-56.git17e62881.0.2.el6.noarch.rpm | 74 MB 00:00
------------------------------------------------------------------------------------------------------------------------------------------------------
Total                                | 214 MB/s | 128 MB 00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
1/4
  Updating   : linux-firmware-20171128-56.git17e62881.0.2.el6.noarch
2/4
  Installing : kernel-uek-4.1.12-112.14.13.el6uek.x86_64
3/4
  Cleanup    : linux-firmware-20160616-44.git43e96a1e.0.12.el6.noarch
4/4
ol6_UEKR4/filelists                   | 18 MB 00:00
Uploading /boot/vmlinuz-4.1.12-112.14.13.el6uek.x86_64 to http://169.254.0.3/kernel
Uploading /boot/initramfs-4.1.12-112.14.13.el6uek.x86_64.img to http://169.254.0.3/initrd
Uploading /tmp/tmp5HjrRUcmdline to http://169.254.0.3/cmdline

Error activating kernel/initrd/cmdline: 502 - <html>
<head><title>502 Bad Gateway</title></head>
<body bgcolor="white">
<center><h1>502 Bad Gateway</h1></center>
</body>
</html>

Note:

- Ignore the error activating message that results from running the update.
- An update will occur only if a versionlock file has a valid update available to apply to the DB system.

8. Restart the system.

   $ sudo su -
   # reboot

9. Run the following command to validate the update:

   # uname -r
   4.1.12-112.14.13

In this example, then new kernel version is 4.1.12-112.14.13.

For information about applying Oracle database patches to a DB system, see Patching a DB System on page 1407.
**Configuring a DB System**

This topic provides information to help you configure your DB system.

**Network Time Protocol**

Oracle recommends that you run a Network Time Protocol (NTP) daemon on your 1-node DB systems to keep system clocks stable during rebooting. If you need information about an NTP daemon, see Setting Up “NTP (Network Time Protocol) Server” in RHEL/CentOS 7.

Oracle recommends that you configure NTP on both nodes in a 2-node RAC DB system to synchronize time across the nodes. If you do not configure NTP, then Oracle Clusterware configures and uses the Cluster Time Synchronization Service (CTSS), and the cluster time might be out-of-sync with applications that use NTP for time synchronization.

For information about configuring NTP on a version 12c database, see Setting Network Time Protocol for Cluster Time Synchronization. For a version 11g database, see Network Time Protocol Setting.

**Transparent Data Encryption**

All user-created tablespaces in a DB system database are encrypted by default, using Transparent Data Encryption (TDE).

- For version 12c databases, if you don’t want your tablespaces encrypted, you can set the `ENCRYPT_NEW_TABLESPACES` database initialization parameter to `DDL`.
- On a 1- or 2-node RAC DB system, you can use the TDE Commands on page 1542 command to update the master encryption key for a database.
- You must create and activate a master encryption key for any PDBs that you create. After creating or plugging in a new PDB on a 1- or 2-node RAC DB System, use the `dbcli update-tdekey` command to create and activate a master encryption key for the PDB. Otherwise, you might encounter the error `ORA-28374: typed master key not found in wallet when attempting to create tablespaces in the PDB`. In a multitenant environment, each PDB has its own master encryption key which is stored in a single keystore used by all containers. For more information, see “Overview of Managing a Multitenant Environment” in the Oracle Database Administrator’s Guide.
- For information about encryption on Exadata DB systems, see Using Tablespace Encryption in Exadata Cloud Service.
- For information on changing an existing TDE wallet password using the Oracle Cloud Infrastructure Console, see To manage administrator and TDE wallet passwords on page 1419.

For detailed information about database encryption, see the Oracle Database Security White Papers.

**Patching a DB System**

This topic describes the procedures to patch bare metal and virtual machine DB systems and database homes by using the Console, the API, or the database CLI (dbcli Integration Cloud). For information on patching or performing a version upgrade on databases within a bare metal or virtual machine DB system, see Patching a Database on page 1421.

**Note:**

This topic is not applicable to Exadata Cloud Service instances. For information and instructions on Exadata patching in Oracle Cloud Infrastructure, see the following topics:

- Patching an Exadata Cloud Service Instance on page 1284
- Patching an Exadata Cloud Service Instance Manually on page 1289.
Currently Available Patches

<table>
<thead>
<tr>
<th>Version</th>
<th>DB System Patch</th>
<th>Database Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.0.0.0</td>
<td>January 2021, October 2020</td>
<td>January 2021, October 2020, July 2020, April 2020</td>
</tr>
<tr>
<td>18.0.0.0</td>
<td>January 2021, October 2020</td>
<td>January 2021, October 2020, July 2020, April 2020</td>
</tr>
<tr>
<td>12.2.0.1</td>
<td>January 2021, October 2020</td>
<td>January 2021, October 2020, July 2020, April 2020</td>
</tr>
<tr>
<td>12.1.0.2</td>
<td>January 2021, October 2020</td>
<td>January 2021, October 2020, July 2020, April 2020</td>
</tr>
<tr>
<td>11.2.0.4</td>
<td>Not applicable</td>
<td>January 2021, October 2020, July 2020, April 2020</td>
</tr>
</tbody>
</table>

For information about operating system updates, see OS Updates on page 1397.

Required IAM Policy

You must have the required type of access in a policy to use Oracle Cloud Infrastructure, whether you're using the Console or the REST API with an SDK, CLI, or other tool. When running a command, if you see an error message that says you don’t have permission or are unauthorized, contact your administrator. Confirm the type of access you’ve been granted, and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 enables the specified group to do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. Details about writing policies for databases are located in Details for the Database Service on page 2240.

About Patching DB Systems

Planning and Preparation

Patching a DB system requires a reboot, which can take several minutes. To minimize the impact on users, run the patch at a time when the system has the fewest users. To avoid system interruption, consider implementing a high availability strategy such as Oracle Data Guard. For more information, see Using Oracle Data Guard with the Database CLI on page 1469.

Oracle recommends that you back up your database and test the patch on a test system before you apply the patch. See Backing Up a Database on page 1435 for more information.

Always patch a DB system before you patch the databases within that system. The Console displays the latest DB system patch and the previous patch. You can use either of these patches, but we recommend using the latest patch when possible.

Patch Availability for Older Oracle Database Software Versions

For the Oracle Database and Oracle Grid Infrastructure major version releases available in Oracle Cloud Infrastructure, patches are provided for the current version plus the two most recent older versions (N through N - 2). For example, if an instance is using Oracle Database 19c, and the latest version of 19c offered is 19.8.0.0.0, patches are available for versions 19.8.0.0.0, 19.7.0.0 and 19.6.0.0.
Prerequisites

DB systems require access to the Oracle Cloud Infrastructure Object Storage service, including connectivity to the applicable Swift endpoint for Object Storage. We recommend using a service gateway with the VCN to enable this access. For more information, see these topics:

- Network Setup for DB Systems on page 1359. This topic describes the procedure to set up your VCN for the DB system, including the service gateway.
- https://cloud.oracle.com/infrastructure/storage/object-storage/faq. This topic explains which Swift endpoints to use.

**Important:**

In addition to the prerequisites listed in this section, ensure that the following conditions are met to avoid patching failures:

- The `/u01` directory on the database host file system has at least 15 GB of free space to execute patching processes.
- The Oracle Cluster ware is running on the DB system.
- All DB system nodes are running.

See Patching Failures on Bare Metal and Virtual Machine DB Systems on page 1659 for details on problems that can result from not following these guidelines.

Using the Console

You can use the Console to:

- View the patch history of a DB system or an individual database.
- Apply patches
- Monitor the status of an operation.

We recommend that you use the pre-check action to ensure that your DB system or database home has met the requirements for the patch you want to apply.

**To patch a DB system**

1. Open the navigation menu. Click > Database > Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   
   A list of DB systems is displayed.
3. Find the DB system that you plan to patch.
4. Click the DB system name to display details about it.
5. Click Resources > Patches.
6. Review the list of patches.
7. Click Actions (three dots) for the patch you are interested in, and then select one of the following actions:
   - Pre-check: Check for any prerequisites to ensure that the patch can be successfully applied.
   - Apply: Performs the pre-check, and then applies the patch.
8. Confirm when prompted.
9. In the list of patches, click the patch name to display its patch request. Then monitor the progress of the patch operation.

   While a patch is being applied, the patch status displays as Applying and the DB system status displays as Updating. If the operation completes successfully, the patch's status changes to Applied and the DB system's status changes to Available.

**To view the patch history of a DB system**

1. Open the navigation menu. Click > Database > Bare Metal, VM, and Exadata.
2. Choose your **Compartment**.
   A list of DB systems is displayed.
3. To display details about the system you are interested in, locate the system name and click it.
4. Under **Resources**, click **Patch History**.
   The history of patch operations for that DB system is displayed.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs to manage patching DB systems:

- `ListDbSystemPatches`
- `ListDbSystemPatchHistoryEntries`
- `GetDbSystemPatch`
- `GetDbSystemPatchHistoryEntry`
- `UpdateDbSystem`

For the complete list of APIs for the Database service, see Database Service API.

**Using the Database CLI**

This topic explains how to use the command line interface on the DB system to patch a DB system. Patches are available from the Oracle Cloud Infrastructure Object Storage service. You use the `DBCLI` commands to download and apply patches to some or all components in your system.

**Prerequisites**

To connect to the DB system via SSH, you need the path to private key associated with the public key used when the DB system was launched.

You also need the public or private IP address of the DB system.

Use the private IP address to connect to the system from your on-premises network, or from within the virtual cloud network (VCN). This includes connecting from a host located on-premises connecting through a VPN or FastConnect to your VCN, or from another host in the same VCN. Use the Exadata system's public IP address to connect to the system from outside the cloud (with no VPN). You can find the IP addresses in the Oracle Cloud Infrastructure Console as follows:

- **Cloud VM clusters (new resource model):** On the Exadata VM Cluster Details page, click Virtual Machines in the **Resources** list.
- **DB systems:** On the DB System Details page, click **Nodes** in the **Resources** list.

The values are displayed in the **Public IP Address** and **Private IP Address & DNS Name** columns of the table displaying the **Virtual Machines** or **Nodes** of the Exadata Cloud Service instance.

To update the CLI with the latest commands

Update the CLI to ensure you have the latest patching commands (older DB systems might not include them).

1. SSH to the DB System.

   ```
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as `opc` and then sudo to the root user. Use `sudo su` – with a hyphen to invoke the root user’s profile, which will set the `PATH` to the `dbcli` directory (`/opt/oracle/dcs/bin`).

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```
3. Update the CLI by using the CLI Update Command on page 1483 command.

```bash
[root@dbsys ~]# cliadm update-dbcli
{
    "jobId" : "dc9ce73d-ed71-4473-99cd-9663b9d79bfd",
    "status" : "Created",
    "message" : "Dcs cli will be updated",
    "reports" : [ ],
    "createTimestamp" : "January 18, 2017 10:19:34 AM PST",
    "resourceList" : [ ],
    "description" : "dbcli patching",
    "updatedTime" : "January 18, 2017 10:19:34 AM PST"
}
```

4. Wait for the update job to complete successfully. Check the status of the job by using the Job Commands on page 1525 command.

```bash
[root@dbsys ~]# dbcli list-jobs
ID                                   Description    Created    Status
------------------------------------ -------------- --------- ----------
----------------------------------- ----------
dc9ce73d-ed71-4473-99cd-9663b9d79bfd dbcli patching January 18, 2017 10:19:34 AM PST    Success
```

To check for installed and available patches

1. SSH to the DB System.

```bash
ssh -i <private_key_path> opc@<db_system_ip_address>
```

2. Log in as opc and then sudo to the root user. Use sudo su - with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (/opt/oracle/dcs/bin).

```bash
login as: opc
[opc@dbsys ~]$ sudo su -
```

3. Display the installed patch versions by using the Component Command on page 1504 command. If the Available Version column indicates a version number for a component, you should update the component.

```bash
[root@dbsys ~]# dbcli describe-component
System Version
-------------
12.1.2.10.0

Component Name        Installed Version    Available Version
--------------------- -------------------- --------------------
OAK                   12.1.2.10.0          up-to-date
GI                    12.1.0.2.161018      up-to-date
ORADB12102_HOME1      12.1.0.2.160719      12.1.0.2.161018
```

4. Display the latest patch versions available in Object Storage by using the Latestpatch Command on page 1527 command.

```bash
[root@dbsys ~]# dbcli describe-latestpatch
componentType   availableVersion
--------------- -------------------
gi               12.1.0.2.161018
db               11.2.0.4.161018
```
**To patch server components**

You can patch the Grid Infrastructure (GI) and storage management kit (OAK) server components.

1. SSH to the DB System.

   ```bash
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as opc and then sudo to the root user. Use `sudo su -` with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (/opt/oracle/dcs/bin).

   ```bash
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. Update the server components by using the Server Command on page 1540 command.

   ```bash
   [root@dbsys ~]$ dbcli update-server
   {
   "jobId" : "9a02d111-e902-4e94-bc6b-9b820ddf6ed8",
   "status" : "Created",
   "reports" : [ ],
   "createTimestamp" : "January 19, 2017 09:37:11 AM PST",
   "resourceList" : [ ],
   "description" : "Server Patching",
   "updatedTime" : "January 19, 2017 09:37:11 AM PST"
   }
   ```

   Note the job ID in the above example.

4. Check the job output by using the Job Commands on page 1525 command with the job ID.

   ```bash
   [root@dbsys ~]$ dbcli describe-job -i 9a02d111-e902-4e94-bc6b-9b820ddf6ed8
   ```

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Patching Repository Directories</td>
<td>January 19, 2017 9:37:11 AM PST</td>
<td>Success</td>
</tr>
<tr>
<td>Download latest patch metadata</td>
<td>January 19, 2017 9:37:11 AM PST</td>
<td>Success</td>
</tr>
<tr>
<td>Update System version</td>
<td>January 19, 2017 9:37:11 AM PST</td>
<td>Success</td>
</tr>
<tr>
<td>Update Patching Repository</td>
<td>January 19, 2017 9:38:35 AM PST</td>
<td>Success</td>
</tr>
<tr>
<td>oda-hw-mgmt upgrade</td>
<td>January 19, 2017 9:38:58 AM PST</td>
<td>Success</td>
</tr>
<tr>
<td>Opatch updation</td>
<td>January 19, 2017 9:38:58 AM PST</td>
<td>Success</td>
</tr>
</tbody>
</table>
5. Verify that the server components were updated successfully by using the Component Command on page 1504 command. The Available Version column should indicate update-to-date.

To patch database home components

1. SSH to the DB System.

   \[ssh -i <private_key_path> opc@<db_system_ip_address>\]

2. Log in as opc and then sudo to the root user. Use `sudo su -` with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (`/opt/oracle/dcs/bin`).

   login as: opc

   [opc@dbsys ~]$ sudo su -

3. Get the ID of the database home by using the Dbhome Commands on page 1518 command.

   [root@dbsys ~]# dbcli list-dbhomes

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>DB Version</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>---------------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>b727bf80-c99e-4846-ac1f-28a81a725df6</td>
<td>OraDB12102_home1</td>
<td>12.1.0.2</td>
<td>/u01/app/orauser/product/12.1.0.2/dbhome_1</td>
</tr>
</tbody>
</table>

4. Update the database home components by using the Dbhome Commands on page 1518 command and providing the ID from the previous step.

   [root@dbsys ~]# dbcli update-dbhome -i b727bf80-c99e-4846-ac1f-28a81a725df6

   \{"jobId": "31b38f67-f993-4f2e-b7eb-5bccda9901ae",
   "status": "Created",
   "message": null,
   "reports": [],
   "createTimestamp": "January 20, 2017 10:08:48 AM PST",
   "resourceList": [],
   "description": "DB Home Patching: Home Id is b727bf80-c99e-4846-ac1f-28a81a725df6",
   "updatedTime": "January 20, 2017 10:08:48 AM PST"
   \}

   Note the job ID in the above example.

5. Check the job output by using the Job Commands on page 1525 command with the job ID.

   [root@dbsys ~]# dbcli describe-job -i 31b38f67-f993-4f2e-b7eb-5bccda9901ae

   Job details

   ID: 31b38f67-f993-4f2e-b7eb-5bccda9901ae
   Description: DB Home Patching: Home Id is b727bf80-c99e-4846-ac1f-28a81a725df6
   Status: Success
   Created: January 20, 2017 10:08:48 AM PST
6. Verify that the database home components were updated successfully by using the Component Command on page 1504 command. The Available Version column should indicate update-to-date.

Creating Databases

**Note:**

- This topic applies only to bare metal DB systems. Virtual machine DB systems can only contain a single database, which is created when the DB system is provisioned.
- Database backups on virtual machine DB systems can only be restored to an existing bare metal DB system or a newly-created virtual machine or bare metal DB system.

When you launch a bare metal DB system, an initial database is created in that system. After provisioning your system, you can create additional databases at any time by using the Console or the API. The database edition will be the edition of the DB system in which the database is created, and each new database is created in a separate database home. You can create an empty database or reproduce a database by using a backup.

**Options for Creating a Database from a Backup**

When creating a new database using a backup stored in Object Storage as the source, you have the following backup source options:

- **Daily automatic backup.** Requires that you have automatic backups enabled and an available backup to use. If you are creating a database from an automatic backup, you can choose any level 0 weekly backup, or a level 1 incremental backup created after the most recent level 0 backup. For more information on automatic backups, see Oracle Cloud Infrastructure Managed Backup Features on page 1436.
- **On-demand full backup.** See To create an on-demand full backup of a database on page 1439 for information on creating an on-demand backup.
- **Standalone backup.** For more information, see Standalone Backups on page 1438.
- **Last archived redo log backup.** Requires that you have automatic backups enabled. This backup combines data from the most recent daily automatic backup and data from archived redo logs, and represents the most current backup available. The time of the last archived redo log backup is visible on the database details page in the Last Backup Time field.
• **Point-in-time out of place restore.** Specify a timestamp to create a new copy of the database that included data up to a specified point in time. The timestamp must be earlier or equal to the **Last Backup Time** time displayed on the database details page. Note the following limitations when performing a point-in-time out of place restore:
  - The timestamp must be within the recovery window of the database
  - The timestamp must be available within the database **incarnation** of the available automatic backups
  - The timestamp cannot fall within two overlapping database incarnations
  - The create database operation will fail if the database has undergone structural changes since the specified timestamp. Structural changes include operations such as creating or dropping a tablespace.
  - The create database operation cannot be started if another point-in-time database copy operation is in progress.

For information on configuring your DB system to back up to Object Storage, see **Backing Up a Database to Oracle Cloud Infrastructure Object Storage** on page 1435.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators: The policy in **Let database admins manage Oracle Cloud database systems** on page 2150 lets the specified group do everything with databases and related Database resources.

If you’re new to policies, see **Getting Started with Policies** on page 2135 and **Common Policies** on page 2142. If you want to dig deeper into writing policies for databases, see **Details for the Database Service** on page 2240.

**Using the Console**

*To create a new database in an existing DB system*

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The database that you create will be the same edition as the initial database in your bare metal DB system.</td>
</tr>
<tr>
<td>• Virtual machine DB systems do not support the creation of additional databases after system provisioning.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
   
   A list of DB systems is displayed.
3. In the list of DB systems, find the DB system in which you want to create the database, and then click its name to display details about it.
4. Click **Create Database**.
5. In the **Create Database** dialog, enter the following:

- **Database name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
- **Database image:** Determines what Oracle Database version is used for the database. You can mix database versions on the DB system, but not editions. By default, the latest Oracle-published database software image is selected.

   Click **Change Database Image** to use an older Oracle-published image or a custom database software image that you have created in advance, then select an **Image Type**:

   - **Oracle Provided Database Software Images:** These images contain generally available versions of Oracle Database software.
   - **Custom Database Software Images:** These images are created by your organization and contain customized configurations of software updates and patches.

   After choosing a software image, click **Select** to return to the Create Database dialog.

- **PDB name:** (Optional) For version 12.1.0.2 and later, you can specify the name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of 8 alphanumeric characters. The only special character permitted is the underscore (_).
- **Create administrator credentials:** A database administrator SYS user will be created with the password you supply.
  - **Username:** SYS
  - **Password:** Supply the password for this user. The password must meet the following criteria:
    - A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.
  - **Confirm password:** Re-enter the SYS password you specified.
  - **Use the administrator password for the TDE wallet:** When this option checked, the password entered for the SYS user is also used for the TDE wallet. To set the TDE wallet password manually, uncheck this option and enter the TDE wallet password.
- **Select workload type:** Choose the workload type that best suits your application:
  - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
  - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
- **Configure database backups:** Specify the settings for backing up the database to Object Storage:
  - **Enable automatic backup:** Check the check box to enable automatic incremental backups for this database. If you are creating a database in a security zone compartment, you must enable automatic backups.
  - **Backup Retention Period:** If you enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
  - **Backup Scheduling:** If you enable automatic backups, you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See **Backup Scheduling** for more information.

6. Click **Show Advanced Options** to specify the following options for the database:

- **Character set:** The character set for the database. The default is AL32UTF8.
- **National character set:** The national character set for the database. The default is AL16UTF16.
- **Tags:** If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
7. Click **Create Database**.

When the database creation is complete, the status changes from Provisioning to Available.

**To create a database from a backup in an existing DB system**

<table>
<thead>
<tr>
<th><strong>Note:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine DB systems do not support the creation of additional databases after system provisioning. To create a new virtual machine DB system from a backup, see <strong>To create a DB system from a backup</strong> on page 1377.</td>
</tr>
</tbody>
</table>

You can create a new database from a database backup. See **Options for Creating a Database from a Backup** on page 1414 for details on backup source options.

Before you begin, note the following:

- When you create a database from a backup, you can choose a different DB system and compartment. However, the availability domain will be the same as where the source database is hosted.

<table>
<thead>
<tr>
<th><strong>Tip:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You can use the <strong>GetBackup</strong> API to obtain information about the availability domain of the backup.</td>
</tr>
</tbody>
</table>

- The DB system you specify must support the same type as the system from which the backup was taken. For example, if the backup is from a single-node database, then the target DB system must be a single-node shape.

- The version of the target DB system must be the same or higher than the version of the backup.

- If the backup being used to create a database is in a security zone compartment, the database cannot be created in a compartment that is not in a security zone. See the **Security Zone Policies** topic for a full list of policies that affect Database service resources.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.

   A list of DB systems is displayed.
3. Navigate to the backup or standalone backup you want to use to create the new DB system:

<table>
<thead>
<tr>
<th><strong>Tip:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are creating a database from an automatic backup, you may choose any level 0 weekly backup, or a level 1 incremental backup created after the most recent level 0 backup. For more information on automatic...</td>
</tr>
</tbody>
</table>
To select a daily automatic backup or on-demand full backup as the source

a. Click the DB system name that contains the specific database to display the DB System Details page.
b. From the Databases list, click the database name associated with the backup you want to use.
c. Find your desired backup in the Backups list. If you don't see the backups list on the database details page, click Backups in the Resources menu.
d. Click the Actions icon (three dots) for the backup, and then click Create Database.

To select the last archived redo log automatic backup as the source

a. Find the DB system where the database is located, and click the system name to display details about it.
b. Find the database associated with the backup you wish to use, and click its name to display details about it.
c. On the database details page, click Create Database from Last Backup.
d. In the Create Database from Backup dialog, select Create database from last backup.

To specify a timestamp for a point-in-time copy of the source

a. Click the DB system name that contains the specific database to display the DB System Details page.
b. From the Databases list, click the database name associated with the backup data you want to use as the source for the initial database in your new DB system.
c. On the database details page, click Create Database from Last Backup.
d. In the Create Database from Backup dialog, select Create database from specified timestamp.

To select a standalone backup as the source

a. Click Standalone Backups under Bare Metal, VM, and Exadata.
b. In the list of standalone backups, find the backup you want to use to create the database.
c. Click the Actions icon (three dots) for the backup you are interested in, and then click Create Database.

4. In the Create Database from Backup dialog, enter the following:

- **DB System:** The DB system in which you want to create the database. You must have the Use Existing DB System radio button selected to see the drop-down list of DB system choices.

  [Note:
  You cannot create a new database in the same DB system in which the database used to create the backup resides.]

- **Database Name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.

- **Database Admin Password:**
  A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.

  A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.

- **Confirm Database Admin Password:** Re-enter the Database admin password you specified.

- **Password for Transparent Data Encryption (TDE) Wallet or RMAN Encryption:**
  Enter either the TDE wallet password or the RMAN encryption password for the backup, whichever is applicable. The TDE wallet password is the SYS password provided when the database was created by using the Oracle Cloud Infrastructure Console, API, or CLI. The RMAN encryption password is typically required instead if the password was subsequently changed manually.

5. Click Create Database.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to create databases on bare metal DB systems.

Database homes:
- ListDbHomes
- GetDbHome
- CreateDbHome
- DeleteDbHome

Databases:
- CreateDatabase

For the complete list of APIs for the Database service, see Database Service API.

Managing Databases

This topic describes the following administrative tasks for databases in bare metal and virtual machine DB systems:

- Updating the administrator and TDE wallet passwords of a database in a bare metal or virtual machine DB system
- Deleting a database in a DB system (bare metal systems only)

Note:

Virtual machine DB systems can only contain a single database, which is created when the DB system is provisioned. To delete a database in a virtual machine DB system, terminate the virtual machine DB system resource.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for databases, see Details for the Database Service on page 2240.

Using the Console

To manage administrator and TDE wallet passwords

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the database:
   a. Click the DB system name that contains the specific database to display the DB System Details page.
   b. From the Databases list, click the database name you want to administer.
4. On the Database Details page, click More Actions, then Manage Passwords.
5. In the Manage Passwords dialog click Update Administrator Password or Update TDE Wallet Password, depending on which password you want to update.
6. Enter the new password:
   - For the administrator password, enter the new password in both the New administrator password and Confirm administrator password fields.
   - For the TDE wallet password, enter the current wallet password in the Enter existing TDE wallet password field, then enter the new password in both the New TDE wallet password and the Confirm TDE wallet password fields.

7. Click **Apply** to update your chosen password.

**To terminate a database**

When terminating a database in a bare metal DB system, you will be given the chance to back up the database prior to terminating it. This creates a standalone backup that can be used to create a database later. Oracle recommends that you create this final backup for any production (non-test) database.

![](Note)

Terminating a database removes all automatic incremental backups of the database from Oracle Cloud Infrastructure Object Storage. However, all full backups that were created on demand, including your final backup, will persist as standalone backups.

You cannot terminate a database that is assuming the primary role in a Data Guard association. To terminate it, you can switch it over to the standby role.

For information on terminating a database contained in a virtual machine DB system, see To terminate a DB system on page 1386. For virtual machine systems, a database can only be terminated as part of the terminate DB system operation.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. In the list of DB systems, find the DB system that contains the database you want to terminate, and then click its name to display details about it.
4. In the list of databases, find the database you want to terminate, and then click its name to display details about it.
5. Click **Actions**, and then click **Terminate**.
6. In the confirmation dialog, indicate whether you want to back up the database before terminating it, and type the name of the database to confirm the termination.
7. Click **Terminate Database**. The database's status indicates Terminating.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225. Use these API operations to manage databases.

Database homes:
- ListDbHomes
- GetDbHome
- UpdateDbHome
- DeleteDbHome

Databases:
- ListDatabases
- GetDatabase
- UpdateDatabase
Note:

See the DeleteDbHome API for information on deleting databases on bare metal DB systems. See the TerminateDbSystem for information on deleting virtual machine DB systems, including the database contained in the system.

For the complete list of APIs for the Database service, see Database Service API.

Additional Information

See the following topics for additional information on administering database resources in Oracle Cloud Infrastructure:

- Backing Up a Database on page 1435
- Recovering a Database on page 1446
- Patching a DB System on page 1407
- To patch a database on page 1422
- To view the patch history of a database on page 1422
- Using the Console to Clone a Virtual Machine DB System on page 1389

Patching a Database

This topic describes the procedures to apply patches to databases in bare metal and virtual machine DB systems by using the Console and the API. For information on patching DB systems and to see a list of currently available database patches, see Patching a DB System on page 1407.

Note:

This topic is not applicable to Exadata Cloud Service instances. For information and instructions on Exadata patching in Oracle Cloud Infrastructure, see the following topics:

- Patching an Exadata Cloud Service Instance on page 1284
- Patching an Exadata Cloud Service Instance Manually on page 1289.

Required IAM Policy

You must have the required type of access in a policy to use Oracle Cloud Infrastructure, whether you're using the Console or the REST API with an SDK, CLI, or other tool. When running a command, if you see an error message that says you don’t have permission or are unauthorized, contact your administrator. Confirm the type of access you’ve been granted, and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 enables the specified group to do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. Details about writing policies for databases are located in Details for the Database Service on page 2240.

About Patching Databases

For database patching, always patch a DB system before you patch the databases within that system. The Console displays the latest DB system patch and the previous patch. You can use either of these patches, but we recommend using the latest patch when possible. See Patching a DB System on page 1407 for more information.

You can also patch your database using a custom database software image. See Oracle Database Software Images on page 1567 for more information on creating and working with software images.

For a list of currently available database patches, see Currently Available Patches on page 1408.

Applying Interim Patches Using a Database Software Image

You can use custom database software images to easily apply interim (one-off) patches to virtual machine and bare metal DB systems in the Console. See the following topics for more information:
• Oracle Database Software Images on page 1567: An overview of the database software image feature.
• To create a database software image on page 1568 Provides information on how to create a custom image that includes one or more interim patches.
• To patch a database on page 1422: Once you have created a database software image with your interim patches, follow the instructions in this topic to patch using the image.

Using the Console

To patch a database

1. Open the navigation menu. Click > Database > Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of DB systems is displayed.
3. Find the DB system where the database is located, and click the system name to display details about it.
   A list of databases is displayed.
4. Find the database on which you want to perform the patch operation, and click its name to display details about it.
5. Under Resources, click Updates.
   The Oracle Provided Database Software Images tab displays generally-available Oracle Database software images that you can use to patch your database. Oracle images that can be used for patching have the update Type of "Patch".
   The Custom Database Software Images tab allows you to select a database software image that you have created in advance. Use the Select a Compartment selector to specify the compartment that contains the database software image. Custom images that can be used for patching have the update Type of "Patch".
6. Review the list of database software image s that you can use to patch your database. We recommend using the latest database software image patch when possible.
7. Click Actions (three dots) for the patch you are interested in, and then select one of the following actions:
   • Precheck: Check for any prerequisites to ensure that the patch can be successfully applied.
   • Apply: Performs the precheck, and then applies the patch.
8. Confirm when prompted.
9. In the list of patches, click the patch name to display its patch request and monitor the progress of the patch operation.
   While a patch is being applied, the patch's status displays as Applying and the database's status displays as Updating. If the operation completes successfully, the patch's status changes to Applied and the database's status changes to Available.

Viewing Patch History

Each patch history entry represents an attempted patch operation and indicates whether the operation was successful or failed. You can retry a failed patch operation. Repeating an operation results in a new patch history entry.

Patch history views in the Console do not show patches that were applied by using command line tools like dbcli or the Patch utility.

To view the patch history of a database

1. Open the navigation menu. Click > Database > Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of DB systems is displayed.
3. To display details about the DB system where the database is located, and click the system name.
   A list of databases is displayed.
4. To display details about the database you are interested in, locate the system name and click it.
5. Under **Resources**, click **Update History**.

   The history of patch and upgrade operations for that database is displayed.

### Using the API

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the following APIs to manage database patching.

- ListDbHomePatches
- ListDbHomePatchHistoryEntries
- GetDbHomePatch
- GetDbHomePatchHistoryEntry
- UpdateDbHome
- UpdateDatabase

For the complete list of APIs for the Database service, see **Database Service API**.

### Applying Interim Patches Manually

**Note:**

This topic applies only to database homes in 1-node and 2-node RAC DB systems.

To apply an interim patch (previously known as a “one-off” patch) to fix a specific defect, follow the procedure in this section. Use the Opatch utility to apply an interim patch to a database home.

In the procedure example, the database home directory is `/u02/app/oracle/product/12.1.0.2/dbhome_1` and the patch number is `26543344`.

**To apply an interim patch to a database home**

1. Obtain the applicable interim patch from My Oracle Support.
2. Review the information in the patch README.txt file. This file might contain additional and/or custom instructions to follow to apply the patch successfully.
3. Use SCP or SFTP to place the patch on your target database.
4. Shut down each database that is running in the database home.

   ```bash
   srvctl stop database -db <db name> -stopoption immediate -verbose
   ```

5. Set the Oracle home environment variable to point to the target Oracle home.

   ```bash
   sudo su - oracle
   export ORACLE_HOME=/u02/app/oracle/product/12.1.0.2/dbhome_1
   ```

6. Change to the directory where you placed the patch, and unzip the patch.

   ```bash
   cd <work_dir_where_opatch_is_stored>
   unzip p26543344_122010_Linux-x86-64.zip
   ```

7. Change to the directory with the unzipped patch, and check for conflicts.

   ```bash
   cd 26543344
   $ORACLE_HOME/OPatch/opatch prereq CheckConflictAgainstOHWithDetail -ph ./
   ```

8. Apply the patch.

   ```bash
   $ORACLE_HOME/OPatch/opatch apply
   ```
9. Verify that the patch was applied successfully.

   `$ORACLE_HOME/OPatch/opatch lsinventory -detail -oh $ORACLE_HOME`

10. If the database home contains databases, restart them.

    `$ORACLE_HOME/bin/srvctl start database -db <db_name>`

Otherwise, run the following command as root user.

    `# /u01/app/<db_version>/grid/bin/setasmgidwrap o=/u01/app/oracle/product/<db_version>/dbhome_1/bin/oracle`

11. If the readme indicates that the patch has a sqlpatch component, run the datapatch command against each database.

    Before you run datapatch, ensure that all pluggable databases (PDBs) are open. To open a PDB, you can use SQL*Plus to execute `ALTER PLUGGABLE DATABASE <pdb_name> OPEN READ WRITE;` against the PDB.

    `$ORACLE_HOME/OPatch/datapatch`

### Upgrading a Database

This topic describes the procedures to upgrade databases in bare metal and virtual machine DB systems by using the Console and the API. Currently upgrades to Oracle Database 19c (Long Term Release) are available.

**Note:**
This topic is not applicable to Exadata Cloud Service instances.

**Required IAM Policy**

You must have the required type of access in a policy to use Oracle Cloud Infrastructure, whether you're using the Console or the REST API with an SDK, CLI, or other tool. When running a command, if you see an error message that says you don’t have permission or are unauthorized, contact your administrator. Confirm the type of access you’ve been granted, and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud database systems on page 2150 enables the specified group to do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. Details about writing policies for databases are located in Details for the Database Service on page 2240.

**Prerequisites**

The following are required in order to upgrade a database on a bare metal or virtual machine DB system:

- The DB system must use Oracle Linux 7 (OL7)
- If your DB System uses ASM storage management software, the system must use Oracle Grid Infrastructure 19c

For databases on DB systems not meeting the minimum software version requirements, you can upgrade only after using the backup and restore operations to restore the database to a DB system that uses OL7 and version 19c Grid Infrastructure. See the following topics for more information on restoring a database to another DB system by using an on-demand full backup:

- Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435
- To create an on-demand full backup of a database on page 1439
- To create a new database in an existing DB system on page 1415
- To create a DB system from a backup on page 1377

Your Oracle database must be configured with the following settings in order to upgrade:
• The database must be in archivelog mode
• The database must have flashback enabled

See the Oracle Database documentation for your database's release version to learn more about these settings.

About Upgrading a Database
For database software version upgrades, note the following:

• Database upgrades involve some database downtime. Keep this in mind when scheduling your upgrade.
• Oracle recommends that you back up your database and test the new software version on a test system before you upgrade. See Backing Up a Database on page 1435 for information on creating an on-demand manual backup.
• Oracle recommends running an upgrade precheck operation for your database prior to attempting an upgrade so that you can discover any issues that need mitigation prior to the time you plan to perform the upgrade.
• If your databases uses Data Guard, you will need to disable or remove the Data Guard association prior to upgrading.
• An upgrade operation cannot take place while an automatic backup operation is underway. Before upgrading, Oracle recommends disabling automatic backups and performing a manual backup. See To configure automatic backups for a database on page 1438 and To create an on-demand full backup of a database on page 1439 for more information.
• After upgrading, you cannot use automatic backups taken prior to the upgrade to restore the database to an earlier point in time.
• If you are upgrading an database that uses version 11.2 software, the resulting version 19c database will be a non-container database.
• The upgrade operation cannot be performed using the dbcli utility.

How the Upgrade Operation Is Performed by the Database Service
During the upgrade process, the Database service does the following:

• Executes an automatic precheck. This allows the system to identify issues needing mitigation and to stop the upgrade operation.
• Sets a guaranteed restore point, enabling it to perform a flashback in the event of an upgrade failure.
• Creates a new Oracle Database Home based on the specified Oracle-published or custom database software image.
• Runs the Database Upgrade Assistant (DBUA) software to perform the upgrade.

Rolling Back an Unsuccessful Upgrade (Oracle Database Enterprise Editions Only)
If your upgrade does not complete successfully on a system using one of the Enterprise software editions, you have the option of performing a rollback. A rollback resets your database to the state prior to the upgrade. All changes to the database made during and after the upgrade will be lost. The rollback option is provided in a banner message displayed on the database details page of a database following an unsuccessful upgrade operation. See To roll back a failed database upgrade on page 1427 for more information.

After Your Upgrade Is Complete
After a successful upgrade, note the following:

• Oracle recommends that you remove the old Oracle Database Home using the dbcli utility. See Dbhome Commands on page 1518 in the dbcli reference for more information.
• Check that automatic backups are enabled for the database if you disabled them prior to upgrading. See To configure automatic backups for a database on page 1438 for more information.
• Edit the Oracle Database COMPATIBLE parameter to reflect the new Oracle Database software version. See What Is Oracle Database Compatibility? for more information.
• On virtual machine DB Systems, ensure that the .bashrc file in the home directory of the Oracle User has been updated to point to the 19c Database Home.
Using the Console

You can use the Console to:

- Upgrade your database
- View the update history of your database
- Roll back an unsuccessful upgrade

Oracle recommends that you use the precheck action to ensure that your database has met the requirements for the upgrade operation.

To upgrade a database

1. Open the navigation menu. Select Bare Metal, VM, and Exadata, then select DB Systems.
2. Choose your Compartment.
   - A list of DB systems is displayed.
3. Find the DB system where the database is located, and click the system name to display details about it.
   - A list of databases is displayed.
4. Find the database you want to upgrade, and click its name to display details about it.
5. Under Resources, click Updates.
   - The Oracle Provided Database Software Images tab displays generally-available Oracle Database software images that you can use to upgrade your database to a higher major release version. Oracle images that can be used for upgrading have the update Type of "Upgrade". Note that only the most recent patch level of Oracle Database 19c and the next-most recent patch level can be used for the upgrade operation.
   - The Custom Database Software Images tab allows you to select a database software image that you have created in advance. Use the Select a Compartment selector to specify the compartment that contains the database software image. Custom images that can be used for upgrading have the update Type of "Upgrade". Note that only the most recent patch level of Oracle Database 19c and the next-most recent patch level can be used for the upgrade operation.
6. Review the list of Oracle provided or custom database software images that you can use to upgrade your database, and identify an image you want to use for the upgrade.
7. Click Actions (three dots) on the row of the image you want to use for the upgrade, and then select one of the following actions:
   - Precheck: Check for any prerequisites to ensure that the upgrade can be successfully applied. Oracle recommends that you manually perform a precheck operation prior to upgrading to ensure that your database is ready to be upgraded.
   - Upgrade: Applies the selected database upgrade.
8. Confirm when prompted.
9. While an upgrade is being applied, the database’s status displays as Upgrading. If the operation completes successfully, the database’s status changes to Available.

To view the upgrade history of a database

1. Open the navigation menu. Select Bare Metal, VM, and Exadata, then select DB Systems.
2. Choose your Compartment.
   - A list of DB systems is displayed.
3. To display details about the DB system where the database is located, and click the system name.
   - A list of databases is displayed.
4. To display details about the database you are interested in, locate the system name and click it.
5. Under Resources, click Update History.
   - The history of patch and upgrade operations for that database is displayed.
To roll back a failed database upgrade

**Note:**

The upgrade rollback operation is only available for Enterprise software edition databases that were unsuccessfully upgraded and are currently in the "Failed" lifecycle state.

1. Open the navigation menu. Select **Bare Metal, VM, and Exadata**, then select **DB Systems**.
2. Choose your **Compartment**.
   
   A list of DB systems is displayed.
3. Find the DB system where the database is located, and click the system name to display details about it.
   
   A list of databases is displayed.
4. Find the database that was unsuccessfully upgraded, and click its name to display details about it. The database should display a banner at the top of the details page that includes a **Rollback** button.
5. Click **Rollback**. In the **Confirm rollback** dialog, confirm that you want to initiate a rollback to the previous Oracle Database version by clicking **Rollback**.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs to manage database upgrades:

- ListDatabaseUpgradeHistoryEntries
- UpgradeDatabase

For the complete list of APIs for the Database service, see Database Service API.

**Note:**

When using the UpgradeDatabase API to upgrade a database on a virtual machine or bare metal DB system, you must specify either DB_VERSION or DB_SOFTWARE_IMAGE as the upgrade source.

**Monitoring a Database**

This topic explains how to set up an:

- Enterprise Manager Express console to monitor a version 12.1.0.2 or later database
- Enterprise Manager Database Control console to monitor a version 11.2.0.4 database

Each console is a web-based database management tool inside the Oracle database. You can use the console to perform basic administrative tasks such as managing user security, memory, and storage, and view performance information.

**Required IAM Policy**

Some of the procedures below require permission to create or update security lists. For more information about security list policies, see Security Lists on page 2850.

**Monitoring a Database with Enterprise Manager Express**

On 1- and 2-node RAC DB Systems, by default, the EM Express console is not enabled on version 18.1.0.0, 12.2.0.1, and 12.1.0.2 databases. You can enable it for an existing database as described below, or you can enable it when you create a database by using the Database Commands on page 1505 command with the -co parameter.

You must also update the security list and iptables for the DB system as described later in this topic.

When you enable the console, you’ll set the port for the console. The procedure below uses port 5500, but each additional console enabled on the same DB system will have a different port.
To enable the EM Express console and determine its port number

1. SSH to the DB system, log in as opc, sudo to the oracle user, and log in to the database as SYS.

   ```
sudo su - oracle
. oraenv
<provide the database SID at the prompt>
sqlplus / as sysdba
   ```

2. Do one of the following:

   - To enable the console and set its port, use the following command.

     ```
     exec DBMS_XDB_CONFIG.SETHTTPSPORT(<port>);
     ```

     For example:

     ```
     SQL> exec DBMS_XDB_CONFIG.SETHTTPSPORT(5500);
     PL/SQL procedure successfully completed.
     ```

   - To determine the port for a previously enabled console, use the following command.

     ```
     select dbms_xdb_config.getHttpsPort() from dual;
     ```

     For example:

     ```
     SQL> select dbms_xdb_config.getHttpsPort() from dual;
     DBMS_XDB_CONFIG.GETHTTPSPORT()
     -----------------------------
     5500
     ```

3. Return to the operating system by typing `exit` and then confirm that the listener is listening on the port:

   ```
   lsnrctl status | grep HTTP
   ```

   (DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=xxx.us.oracle.com)(PORT=5500))
   (Security=(my_wallet_directory=/u01/app/oracle/admin/prod/xdb_wallet))
   (Presentation=HTTP) (Session=RAW))

4. If you're using a 2-node RAC DB system, see To set the required permissions on a 2-node RAC DB system on page 1428.

5. Open the console's port as described in Opening Ports on the DB System on page 1433.

6. Update the security list for the console's port as described in Updating the Security List for the DB System on page 1434.

To set the required permissions on a 2-node RAC DB system

If you're using a 2-node RAC DB system, you'll need to add read permissions for the asmadmin group on the wallet directory on both nodes in the system.

1. SSH to one of the nodes in the DB system, log in as opc, sudo to the grid user.

   ```
   [opc@dbsysHost1 ~]$ sudo su - grid
   [grid@dbsysHost1 ~]$
   ```

   ORACLE_SID = [+ASM1] ?
   The Oracle base has been set to /u01/app/grid

2. Get the location of the wallet directory, shown in red below in the command output.

   ```
   [grid@dbsysHost1 ~]$ lsnrctl status | grep xdb_wallet
   ```
3. Return to the opc user, switch to the oracle user, and change to the wallet directory.

```
[opc@dbsysHost1 ~]$ sudo su - oracle
[oracle@dbsysHost1 ~]$ cd /u01/app/oracle/admin/dbsys12_phx3wm/xdb_wallet
```

4. List the directory contents and note the permissions.

```
[oracle@dbsysHost1 xdb_wallet]$ ls -ltr
total 8
-rw------- 1 oracle asadmin 3881 Apr  6 16:32 ewallet.p12
-rw------- 1 oracle asadmin 3926 Apr  6 16:32 cwallet.sso
```

5. Change the permissions:

```
[oracle@dbsysHost1 xdb_wallet]$ chmod 640 /u01/app/oracle/admin/dbsys12_phx3wm/xdb_wallet/*
```

6. Verify that read permissions were added.

```
[oracle@dbsysHost1 xdb_wallet]$ ls -ltr
total 8
-rw-r----- 1 oracle asadmin 3881 Apr  6 16:32 ewallet.p12
-rw-r----- 1 oracle asadmin 3926 Apr  6 16:32 cwallet.sso
```

7. Important! Repeat the steps above on the other node in the cluster.

To connect to the EM Express console

After you’ve enabled the console and opened its port in the security list and iptables, you can connect as follows:

1. From a web browser, connect to the console using the following URL format:

```
https://<ip_address>[:port]/em
```

For example, https://129.145.0.164:5500/em

Use the DB system’s private or public IP address depending on your network configuration.

Use the private IP address to connect to the system from your on-premises network, or from within the virtual cloud network (VCN). This includes connecting from a host located on-premises connecting through a VPN or FastConnect to your VCN, or from another host in the same VCN. Use the Exadata system’s public IP address to connect to the system from outside the cloud (with no VPN). You can find the IP addresses in the Oracle Cloud Infrastructure Console as follows:

- **Cloud VM clusters (new resource model)**: On the **Exadata VM Cluster Details** page, click **Virtual Machines** in the Resources list.
- **DB systems**: On the **DB System Details** page, click **Nodes** in the Resources list.

The values are displayed in the **Public IP Address** and **Private IP Address & DNS Name** columns of the table displaying the **Virtual Machines** or **Nodes** of the Exadata Cloud Service instance.
2. A login page is displayed and you can log in with any valid database credentials.

The Database Home page is displayed.

To learn more about EM Express, see Introduction to Oracle Enterprise Manager Database Express.

**Note:**

If you're using a 1-node DB system, and you are unable to connect to the EM Express console, see Database Known Issues.

**Monitoring a Database with Enterprise Manager Database Control**

By default, the Enterprise Manager Database Control console is not enabled on version 11.2.0.4 databases. You can enable the console:

- when you create a database by using the Database Commands on page 1505 with the `–co` parameter
- for an existing database as described here.

Port 1158 is the default port used for the first console enabled on the DB system, but each additional console enabled on the DB system will have a different port.
Note:
For a version 11.2.0.4 database on a 2-node RAC DB system, see To enable the console for a version 11.2.0.4 database on a multi-node DB system on page 1432.

To determine the port for the Enterprise Manager Database Control console

1. SSH to the DB system, log in as opc, and sudo to the oracle user.
   
   ```
   sudo su - oracle
   . oraenv
   <provide the database SID at the prompt>
   ```

2. Use the following command to get the port number.
   
   ```
   emctl status dbconsole
   ```

   The port is in the URL, as shown in the following example:

   ```
   [oracle@dbsys ~]$ emctl status dbconsole
   Oracle Enterprise Manager 11g Database Control Release 11.2.0.4.0
   Copyright (c) 1996, 2013 Oracle Corporation.  All rights reserved.
   https://dbprod:1158/em/console/aboutApplication
   Oracle Enterprise Manager 11g is running.
   _____________________________________________________________________
   Logs are generated in directory /u01/app/oracle/product/11.2.0.4/dbhome_2/
   dbprod_db11/sysman/log
   ```

3. Open the console's port as described in Opening Ports on the DB System on page 1433.
4. Update the security list for the console's port as described in Updating the Security List for the DB System on page 1434.

To connect to the Enterprise Manager Database Control console

After you've enabled the console and opened its port in the security list and iptables, you can connect as follows:

1. From a web browser, connect to the console using the following URL format:
   
   ```
   https://<ip_address>:<port>/em
   ```

   For example, https://129.145.0.164:1158/em

   Use the DB system's private or public IP address depending on your network configuration.

   Use the private IP address to connect to the system from your on-premises network, or from within the virtual cloud network (VCN). This includes connecting from a host located on-premises connecting through a VPN or FastConnect to your VCN, or from another host in the same VCN. Use the Exadata system’s public IP address to connect to the system from outside the cloud (with no VPN). You can find the IP addresses in the Oracle Cloud Infrastructure Console as follows:

   - **Cloud VM clusters (new resource model):** On the Exadata VM Cluster Details page, click Virtual Machines in the Resources list.
   - **DB systems:** On the DB System Details page, click Nodes in the Resources list.

   The values are displayed in the Public IP Address and Private IP Address & DNS Name columns of the table displaying the Virtual Machines or Nodes of the Exadata Cloud Service instance.

2. A login page will be displayed and you can log in with any valid database credentials.

To learn more about Enterprise Manager Database Control, see Introduction to Oracle Enterprise Manager Database Control.
To enable the console for a version 11.2.0.4 database on a multi-node DB system

A few extra steps are required to enable the console for a version 11.2.0.4 database on a multi-node DB system.

Configure SSH Equivalency Between the Two Nodes

You'll create SSH keys on each node and copy the key to the other node, so that each node has the keys for both nodes. The following procedure uses the sample names node1 and node2.

1. SSH to node1, log in as opc, and sudo to the oracle user.

   ```
   sudo su - oracle
   ```

2. Create a directory called .ssh, set its permissions, create an RSA key, and add the public key to the authorized_keys file.

   ```
   mkdir .ssh
   chmod 755 .ssh
   ssh-keygen -t rsa
   cat id_rsa.pub > authorized_keys
   ```

3. Repeat the previous steps on the other node in the cluster.

4. On each node, add the id_rsa.pub key for the other node to the authorized_keys file.

   When you're done, you should see both keys in authorized_keys on each node.

5. On node1, create the known_hosts file by doing the following:

   - SSH to node1 and reply yes to the authentication prompt.
   - SSH to node2 and reply yes to the authentication prompt.

6. On node2, create the known_hosts file by doing the following:

   - SSH to node2 and reply yes to the authentication prompt.
   - SSH to node1 and reply yes to the authentication prompt.

7. On node1, verify that SSH equivalency is now configured by using the following Cluster Verification Utility (CVU) command.

   ```
   cluvfy stage -pre crsinst -n all -verbose
   ```

Configure the Console

1. On node1, create a file called emca.rsp with the following entries.

   ```
   DB_UNIQUE_NAME=<pdb_unique_name>
   SERVICE_NAME=<db_unique_name>.<db_domain>
   PORT=<scan listener port>
   LISTENER_OH=$GI_HOME
   SYS_PWD=<admin password>
   DBSNMP_PWD=<admin password>
   SYSMAN_PWD=<admin password>
   CLUSTER_NAME=<cluster name>  
   ASM_OH=$GI_HOME
   ASM_SID=+ASM1
   ASM_PORT=<asm listener port>
   ASM_USER_NAME=ASMSNMP
   ASM_USER_PWD=<admin password>
   ```

2. On node1, run Enterprise Manager Configuration Assistant (EMCA) using the emca.rsp file as input.

   ```
   $ORACLE_HOME/bin/emca -config dbcontrol db -repos create -cluster -silent -respFile <location of response file above>
   ```
3. On node2, configure the console so the agent in node1 reports to the console in node1, and the agent in node2 reports to the console in node2.

```
$ORACLE_HOME/bin/emca -reconfig dbcontrol -silent -cluster -EM_NODE <node2 host> -EM_NODE_LIST <node2 host> -DB_UNIQUE_NAME <db_unique_name> -SERVICE_NAME <db_unique_name>.<db_domain>
```

4. On each node, verify that console is working properly.

```
$ export ORACLE_UNQNAME=<db_unique_name>
$ emctl status agent
```

Update iptables and Security List

1. On each node, edit iptables to open the console's port as described in Opening Ports on the DB System on page 1433.

2. Update the security list for the console's port as described in Updating the Security List for the DB System on page 1434.

Opening Ports on the DB System

Open the following ports as needed on the DB system:

- 6200 - For Oracle Notification Service (ONS).
- 5500 - For EM Express. 5500 is the default port, but each additional EM Express console enabled on the DB system will have a different port. If you're not sure which port to open for a particular console, see Monitoring a Database with Enterprise Manager Express on page 1427.
- 1158 - For Enterprise Manager Database Control. 1158 is the default port, but each additional console enabled on the DB system will have a different port. If you're not sure which port to open for a particular console, see Monitoring a Database with Enterprise Manager Database Control on page 1430.

For important information about critical firewall rules, see Essential Firewall Rules on page 1397.
To open ports on the DB system

1. SSH to the DB System.
   ```
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as opc and then sudo to the root user.
   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. Save a copy of iptables as a backup.
   ```
   [root@dbsys ~]# iptables-save > /tmp/iptables.orig
   ```
   (If necessary, you can restore the original file by using the command `iptables-restore < /tmp/iptables.orig`.)

4. Dynamically add a rule to iptables to allow inbound traffic on the console port, as shown in the following sample. Change the port number and comment as needed.
   ```
   [root@dbsys ~]# iptables -I INPUT 8 -p tcp -m state --state NEW -m tcp --dport 5500 -j ACCEPT -m comment --comment "Required for EM Express."
   ```

5. Make sure the rule was added.
   ```
   [root@dbsys ~]# service iptables status
   ```

6. Save the updated file to `/etc/sysconfig/iptables`.
   ```
   [root@dbsys ~]# /sbin/service iptables save
   ```
   The change takes effect immediately and will remain in effect when the node is rebooted.

7. Update the DB system’s security list as described in Updating the Security List for the DB System on page 1434.

Updating the Security List for the DB System

Review the list of ports in Opening Ports on the DB System on page 1433 and for every port you open in iptables, update the security list used for the DB system, or create a new security list.

Note that port 1521 for the Oracle default listener is included in iptables, but should also be added to the security list.

To update an existing security list

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of DB systems is displayed.
3. Locate the DB system in the list.
4. Note the DB system’s Subnet name and click its Virtual Cloud Network.
5. Locate the subnet in the list, and then click its security list under Security Lists.
6. Click Edit All Rules and add an ingress rule with source type = CIDR, source CIDR=<source CIDR>, protocol=TCP, and port=<port number or port range>.
   The source CIDR should be the CIDR block that includes the ports you open for the client connection.

For detailed information about creating or updating a security list, see Security Lists on page 2850.
Database

Backing Up a Database

Backing up your DB system is a key aspect of any Oracle database environment. You can store backups in the cloud or in local storage. Each backup destination has advantages, disadvantages, and requirements that you should consider, as described below.

Object Storage (Recommended)
• Backups are stored in the Oracle Cloud Infrastructure Object Storage.
• Durability: High
• Availability: High
• Back Up and Recovery Rate: Medium
• Advantages: High durability, performance, and availability.

Local Storage
• Backups are stored locally in the Fast Recovery Area of the DB System.
• Durability: Low
• Availability: Medium
• Back Up and Recovery Rate: High
• Advantages: Optimized back up and fast point-in-time recovery.
• Disadvantages: If the DB System becomes unavailable, the backup is also unavailable.

Currently, Oracle Cloud Infrastructure does not provide the ability to attach block storage volumes to a DB System, so you cannot back up to network attached volumes.

For 1- and 2-node RAC DB Systems, see:
• Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435
• Backing Up a Database to Local Storage Using the Database CLI on page 1443

Backing Up a Database to Oracle Cloud Infrastructure Object Storage

Note:
This topic is not applicable to Exadata DB systems. For Exadata DB systems, see Managing Exadata Database Backups on page 1320.

This topic explains how to work with backups managed by Oracle Cloud Infrastructure. You do this by using the Console or the API. (For unmanaged backups, you can use RMAN or dbcli, and you must create and manage your own Object Storage buckets for backups. See Backing Up a Database to Object Storage Using RMAN on page 1440.)

Caution:
If you previously used RMAN or dbcli to configure backups and then you switch to using the Console or the API for backups, a new backup configuration is created and associated with your database. This means that you can no longer rely on your previously configured unmanaged backups to work.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.
Prerequisites

The DB system requires access to the Oracle Cloud Infrastructure Object Storage service, including connectivity to the applicable Swift endpoint for Object Storage. Oracle recommends using a service gateway with the VCN to enable this access. For more information, see these topics:

- **Network Setup for DB Systems** on page 1359: For information about setting up your VCN for the DB system, including the service gateway.
- **Can I use Oracle Cloud Infrastructure Object Storage as a destination for my on-premises backups?**: For information about the Swift endpoints to use.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that your database and DB system must be in an “Available” state for a backup operation to run successfully. Oracle recommends that you avoid performing actions that could interfere with availability (such as patching and Data Guard operations) while a backup operation is in progress. If an automatic backup operation fails, the Database service retries the operation during the next day’s backup window. If an on-demand full backup fails, you can try the operation again when the DB system and database availability are restored.</td>
</tr>
</tbody>
</table>

In addition to the prerequisites listed, ensure that the following conditions are met to avoid backup failures:

- The database's archiving mode is set to ARCHIVELOG (the default).
- The `/u01` directory on the database host file system has sufficient free space for the execution of backup processes.
- The `.bash_profile` file for the oracle user does not include any interactive commands (such as `oraenv` or one that could generate an error or warning message).
- (For automatic backups) No changes were made to the default `WALLET_LOCATION` entry in the `sqlnet.ora` file.
- No changes were made to `RMAN` backup settings by using standard `RMAN` commands.

See **Backup Failures on Bare Metal and Virtual Machine DB Systems** on page 1646 for details on problems that can result from not following these guidelines.

**Oracle Cloud Infrastructure Managed Backup Features**

The following information applies to managed backups configured using the Oracle Cloud Infrastructure Console or API.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases in a security zone compartment must have automatic backups enabled. See the <strong>Security Zone Policies</strong> topic for a full list of policies that affect Database service resources.</td>
</tr>
</tbody>
</table>

**Automatic Incremental and Archived Redo Log Backups**

When you enable the Automatic Backup feature for a database, the service creates the following on an on-going basis:

- Weekly level 0 backup, generally created on a specified weekend day. A level 0 backup is the equivalent of a full backup. Note that in the Console, weekly level 0 backups appear in the list of backups with backup type “incremental”, as do the daily level 1 backups.
• Daily level 1 backups, which are incremental backups created on each day for the six days following the level 0 backup day.

Level 0 and level 1 backups are stored in Object Storage and have an assigned OCID.

• Ongoing archived redo log backups (with a minimum frequency of every 60 minutes). The Last Backup Time field on the database details page in the Oracle Cloud Infrastructure Console displays the time of the last archived redo logs. This backup differs from the level 0 and level 1 automatic backups in that it is based on log data and does not have an assigned OCID. The last archived redo log backup can be used to create a new database or to recover a database with minimal data loss.

The automatic backup process used to create level 0 and level 1 backups can run at any time within the daily backup window (between midnight and 6:00 AM). See note for backup window time zone information. Automatic incremental backups (level 0 and level 1) are retained in Object Storage for 30 days by default.

Backup Retention

If you choose to enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The system automatically deletes your incremental backups at the end of your chosen retention period.

Audit and Trace File Retention for Databases Using Automatic Backups

Oracle Database writes audit and trace files to your database's local storage in the /u01 directory. These files are retained for 30 days by default, though you can change this interval. Once a day, audit and trace files older than 30 days (or the user-specified interval, if applicable) are discarded by a Oracle Scheduler job. You can also disable the Scheduler job if you want to retain these files permanently. Use the following dbcli commands to make changes to this Scheduler job.

• To change the retention period from the default setting of 30 days:

```
dbcli update-database -in <dbName> -lr <number_of_days_to_retain_files>
```

For example:

```
dbcli update-database -in inventorydb -lr 15
```

• To disable the daily discard Scheduler job for older audit and trace files:

```
dbcli update-schedule -i <schedulerID> -d
```

For example:

```
dbcli update-schedule -i 5678 -d
```

Backup Scheduling

The automatic backup process starts at any time during your daily backup window. You can optionally specify a 2-hour scheduling window for your database during which the automatic backup process will begin. There are 12 scheduling windows to choose from, each starting on an even-numbered hour (for example, one window runs from 4:00-6:00 AM, and the next from 6:00-8:00 AM). Backups jobs do not necessarily complete within the scheduling window.

The default backup window of 00:00 to 06:00 in the time zone of the DB system's region is assigned to your database if you do not specify a window. Note that the default backup scheduling window is six hours long, while the windows you specify are two hours long. See note for backup window time zone information.

```
Note:

• Backup Window Time Zone - Automatic backups enabled for the first time after November 20, 2018 on any database will run between midnight
```
and 6:00 AM in the time zone of the DB system's region. If you have enabled automatic backups on a database before this date, the backup window for the database will continue to be between midnight and 6:00 AM UTC. You can create a My Oracle Support service request to have your automatic backups run in a backup window of your choice.

- **Data Guard** - You can enable the Automatic Backup feature on a database with the standby role in a Data Guard association. However, automatic backups for that database will not be created until it assumes the primary role.
- **Retention Period Changes** - If you shorten your database’s automatic backup retention period in the future, existing backups falling outside the updated retention period are deleted by the system.
- **Object Storage Costs** - Automatic backups incur Object Storage usage costs.

**On-Demand Full Backups**

You can create a full backup of your database at any time unless your database is assuming the standby role in a Data Guard association.

**Standalone Backups**

When you terminate a DB system or a database, all of its resources are deleted, along with any automatic backups. Full backups remain in Object Storage as standalone backups. You can use a standalone backup to create a new database.

**Using the Console**

You can use the Console to enable automatic incremental backups, create full backups on demand, and view the list of managed backups for a database. The Console also allows you to delete full backups.

**Note:**

The list of backups you see in the Console does not include any unmanaged backups (backups created directly by using RMAN or dbcli).

All backups are encrypted with the same master key used for Transparent Data Encryption (TDE) wallet encryption.

To navigate to the list of standalone backups for your current compartment

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Click **Standalone Backups** under **Bare Metal, VM, and Exadata**.

To configure automatic backups for a database

When you launch a DB system, you can optionally enable automatic backups for the initial database. Use this procedure to configure or disable automatic backups after the database is created.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
   
   A list of DB systems is displayed.
3. Find the DB system where the database is located, and click the system name to display details about it.
   
   A list of databases is displayed.
4. Find the database for which you want to enable or disable automatic backups, and click its name to display database details. The details indicate whether automatic backups are enabled. When backups are enabled, the details also indicate the chosen backup retention period.
5. Click **Configure Automatic Backups**.
6. In the **Configure Automatic Backups** dialog, check or uncheck **Enable Automatic Backup**, as applicable.

   If you are enabling automatic backups, you can choose to configure the following:

   • **Backup Retention Period**: If you enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, 60 days, or 90 days. The default selection is 30 days.
   • **Backup Scheduling**: If you enable automatic backups, you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See **Backup Scheduling** on page 1437 for more information.

7. Click **Save Changes**.

To create an on-demand full backup of a database

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
3. In the list of DB systems, click the name of the system that contains the database that you want to work with.
4. On the DB system details page, find the database you want to work with in list of databases and click the display name of the database to view the database details.
5. Under **Resources**, click **Backups**.
   
   A list of backups is displayed.
6. Click **Create Backup**.

To delete full backups from Object Storage

   **Note:**

   You cannot explicitly delete automatic backups. Unless you terminate the database, automatic backups remain in Object Storage for 30 days, after which time they are automatically deleted.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**.
   
   A list of DB systems is displayed.
3. Find the DB system where the database is located and click the DB system name to display details.
   
   A list of databases is displayed.
4. Find the database you are interested in and click its name to display database details.
5. Under **Resources**, click **Backups**.
   
   A list of backups is displayed.
6. Click the Actions icon (three dots) for the backup you are interested in, and then click **Delete**.
7. Confirm when prompted.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage database backups:

• **ListBackups**
• **GetBackup**
• **CreateBackup**
• **DeleteBackup**
• **UpdateDatabase** - To enable and disable automatic backups.

For the complete list of APIs for the Database service, see **Database Service API**.
What's Next?

See Recovering a Database from Object Storage on page 1446 for information on restoring your database.

See To create a database from a backup in an existing DB system on page 1417 for information on creating a new database from a backup. You have the choice of using a daily incremental backup, a Standalone Backups on page 1438, the latest archive redo log backup, or a timestamp for a point-in-time copy.

See To create a DB system from a backup on page 1377 for information on creating a new DB system using a backup as the source for the initial database. You have the choice of using a daily incremental backup, a Standalone Backups on page 1438, the latest archive redo log backup, or a timestamp for a point-in-time copy.

Backing Up a Database to Object Storage Using RMAN

This topic is not applicable to Exadata DB systems. For Exadata DB systems, see Managing Exadata Database Backups by Using bkup_api on page 1323.

This topic explains how to use Recovery Manager (RMAN) to manage backups of your Bare Metal or Virtual Machine DB system database to your own Object Storage. For backups managed by Oracle Cloud Infrastructure, see Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435.

To back up to the service you'll need to create an Object Storage bucket for the backups, generate a password for the service, install the Oracle Database Cloud Backup Module, and then configure RMAN to send backups to the service. The backup module is a system backup to tape (SBT) interface that’s tightly integrated with RMAN, so you can use familiar RMAN commands to perform backup and recovery operations.

You'll notice Swift mentioned in the Console and in the endpoint URL for the service. That's because the backup module is typically used to back up to the Oracle Database Backup Cloud Service, which is an OpenStack Swift object store.

Tip:

On a 1-node DB system, you can use the database command line interface (dbcli) to back up to Object Storage. This is an alternative to installing the backup module and using RMAN for backups. For more information, see Objectstoreswift Commands on page 1533. Note that the dbcli commands are not available for a 2-node RAC DB system.

Prerequisites

You'll need the following:

• A DB system and a database to back up. For more information, see Creating Bare Metal and Virtual Machine DB Systems on page 1370.

• The DB system's cloud network (VCN) must be configured with access to Object Storage:
  • For Object Storage access in the same region as the DB system: Oracle recommends using a service gateway. For more information, see Service Gateway for the VCN on page 1365.
  • For Object Storage access in a different region than the DB system: Use an internet gateway. Note that the network traffic between the DB system and Object Storage does not leave the cloud and never reaches the public internet. For more information, see Internet Gateway on page 3243.

• An existing Object Storage bucket to use as the backup destination. You can use the Console or the Object Storage API to create the bucket. For more information, see Managing Buckets on page 3398.

• An auth token generated by Oracle Cloud Infrastructure. You can use the Console or the IAM API to generate the password. For more information, see Working with Auth Tokens.

• The user name (specified when you install and use the backup module) must have tenancy-level access to Object Storage. An easy way to do this is to add the user name to the Administrators group. However, that allows access...
to all of the cloud services. Instead, an administrator should create a policy like the following that limits access to only the required resources in Object Storage for backing up and restoring the database:

```plaintext
Allow group <group_name> to manage objects in compartment <compartment_name> where target.bucket.name = '<bucket_name>'
Allow group <group_name> to read buckets in compartment <compartment_name>
```

For more information about adding a user to a group, see Managing Groups on page 2419. For more information about policies, see Getting Started with Policies on page 2135.

**Installing the Backup Module on the DB System**

1. SSH to the DB system, log in as opc, and sudo to the oracle user.

   ```bash
   ssh -i <SSH_key_used_when-launching_the_DB_system> opc@<DB_system_IP_address_or_hostname> login as: opc sudo su - oracle
   ```

2. Change to the directory that contains the backup module `opc_install.jar` file.

   ```bash
   cd /opt/oracle/oak/pkgrepos/oss/odbcs
   ```

3. Use the following command syntax to install the backup module.

   ```bash
   java -jar opc_install.jar -opcId <user_id> -opcPass '<auth_token>' -container <bucket_name> -walletDir ~/hsbtwallet/ -libDir ~/lib/ -configfile ~/config - host https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/<object_storage_namespace>
   ```

The parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-opcId</code></td>
<td>The user name for the Oracle Cloud Infrastructure user account, for example: <code>opcId -opcId &lt;username&gt;@&lt;example&gt;.com</code> This is the user name you use to sign in to the Console. The user name must be a member of the Administrators group, as described in Prerequisites on page 1440. You can also specify the user name in single quotes. This might be necessary if the name contains special characters, for example: <code>opcId 'j~smith@example.com'</code> Make sure to use straight single quotes and not slanted apostrophes.</td>
</tr>
<tr>
<td><code>-opcPass</code></td>
<td>The auth token generated by using the Console or IAM API, in single quotes, for example: <code>opcPass -opcPass '&lt;password&gt;'</code> Make sure to use straight single quotes and not slanted apostrophes. For more information, see Managing User Credentials on page 2456. This is not the password for the Oracle Cloud Infrastructure user.</td>
</tr>
<tr>
<td><code>-container</code></td>
<td>The name of an existing bucket in Object Storage to use as the backup destination, for example: <code>container -container DBBackups</code></td>
</tr>
</tbody>
</table>
### Database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| walletDir | The directory where the install tool will create an Oracle Wallet containing the Oracle Cloud Infrastructure user auth token. 
- `walletDir ~/hsbtwallet` creates the wallet in the current user (oracle) home directory. |
| libDir | The directory where the SBT library is stored. The directory must already exist before you run the command. This parameter causes the latest SBT library to be downloaded. 
- `libDir ~/lib/` downloads the `libopc.so` file to the current user's home directory, for example, `/home/oracle/lib/libopc.so`. |
| configfile | The name of the initialization parameter file that will be created by the install tool. This file will be referenced by your RMAN jobs. 
- `configfile ~/config` creates the file in the current user's home directory, for example, `/home/oracle/config`. |
| host | The endpoint URL to which backups are to be sent:

```text
https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/<object_storage_namespace>
```

where `<object_storage_namespace>` is your tenancy's Object Storage namespace. 
Do not add a slash after the Object Storage namespace. 
See [Regions and Availability Domains](#) on page 180 to look up the region name. |

### Configuring RMAN

This section describes how to configure RMAN to use the bucket as the default backup destination. The following assumes you are still logged in to the DB system.

1. On the DB system, set the ORACLE_HOME and ORACLE_SID environment variables using the oraenv utility.

   ```sql
   . oraenv
   ```

2. Connect to the database using RMAN.

   ```sql
   rman target /
   ```

3. Configure RMAN to use the SBT device and point to the `config` file that was created when you installed the backup module. A sample command for a version 12 database is shown here.

   ```sql
   RMAN> CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/home/oracle/lib/libopc.so, SBT_PARMS=(OPC_PFILE=/home/oracle/config)';
   ```

4. Configure RMAN to use SBT_TAPE by default. The following sample enables the controlfile and spfile autobackup to SBT_TAPE and configures encryption (recommended). There are other settings that may apply to your installation such as compression, number of backup and recovery channels to use, backup retention policy, archived log deletion policy, and more. See the Oracle Backup and Recovery documentation for your version of Oracle for more information on choosing the appropriate settings.

   ```sql
   RMAN> CONFIGURE DEFAULT DEVICE TYPE TO SBT_TAPE;
   RMAN> CONFIGURE BACKUP OPTIMIZATION ON;
   RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
   RMAN> CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%F';
   RMAN> CONFIGURE ENCRYPTION FOR DATABASE ON;
   ```
Once the RMAN configuration is complete, you can use the same RMAN commands that you regularly use for tape backups.

**Backing up the Database**

This section provides examples of commonly used backup commands.

1. Set the database encryption:

   ```
   RMAN> SET ENCRYPTION IDENTIFIED BY "password" ONLY;
   ```

   Note that this setting is not permanent; you must set it for each new RMAN session.

2. Back up the database and archivelogs. Below are some example commands. See the Oracle Backup and Recovery documentation for your version of Oracle for more information about choosing a back up procedure that meets your needs. Be sure to back up regularly to minimize potential data loss and always include a copy of the spfile and controlfile. Note that the example below uses multi-section incremental backups, which is a feature introduced in 12c. When using 11g, omit the `section size` clause.

   ```
   RMAN> BACKUP INCREMENTAL LEVEL 0 SECTION SIZE 512M DATABASE PLUS ARCHIVELOG;
   
   RMAN> BACKUP INCREMENTAL LEVEL 1 SECTION SIZE 512M DATABASE PLUS ARCHIVELOG;
   
   RMAN> BACKUP INCREMENTAL LEVEL 1 CUMULATIVE SECTION SIZE 512M DATABASE PLUS ARCHIVELOG;
   ```

3. Backup archivelogs frequently to minimize potential data loss, and keep multiple backup copies as a precaution.

   ```
   RMAN> BACKUP ARCHIVELOG ALL NOT BACKED UP 2 TIMES;
   ```

When the backup job completes, you can display the backup files in your bucket in the Console on the Storage page, by selecting Object Storage.

**What's Next?**

See Recovering a Database from Object Storage on page 1446.

**Backing Up a Database to Local Storage Using the Database CLI**

**Note:**

This topic is not applicable to virtual machine DB systems because they have no local storage. For Exadata DB systems, see Managing Exadata Database Backups on page 1320.

This topic explains how to back up to the local Fast Recovery Area on a bare metal DB system by using the database CLI (dbcli). Some sample dbcli commands are provided below. For complete command syntax, see the Oracle Database CLI Reference on page 1483.

**Note:**

Backing up to local storage is fast and provides for fast point-in-time recovery, however, if the DB system becomes unavailable, the backup also becomes unavailable. For information about more durable backup destinations, see Backing Up a Database on page 1435.
Database

**Backing Up the Database to Local Storage**

You’ll use the dbcli commands to create a backup configuration, associate the backup configuration with the database, initiate the backup operation, and then review the backup job.

1. **SSH to the DB System.**

   ```bash
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. **Log in as opc and then sudo to the root user. Use sudo su – with a hyphen to invoke the root user’s profile, which will set the PATH to the dbcli directory (/opt/oracle/dcs/bin).**

   ```bash
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. **Create a backup configuration by using the Backupconfig Commands on page 1491 command and specify local disk storage as the backup destination.**

   The following example creates a backup configuration named prodbackup and specifies a disk backup destination and a disk recovery window of 5 (backups and archived redo logs will be maintained in local storage for 5 days).

   ```bash
   [root@dbsys ~]# dbcli create-backupconfig --name prodbackup --
   backupdestination disk --recoverywindow 5
   {
   "jobId" : "e7050756-0d83-48ce-9336-86592be59827",
   "status" : "Success",
   "message" : null,
   "reports" : [ {
   "taskId" : "TaskParallel_471",
   "taskName" : "persisting backup config metadata",
   "taskResult" : "Success",
   "startTime" : 1467774813141,
   "endTime" : 1467774813207,
   "status" : "Success",
   "taskDescription" : null,
   "parentTaskId" : "TaskSequential_467",
   "jobId" : "e7050756-0d83-48ce-9336-86592be59827",
   "reportLevel" : "Info",
   "updatedAt" : 1467774813207
   } ],
   "createTimestamp" : 1467774781851,
   "description" : "create backup config:prodbackup",
   "updatedAt" : 1467774813236
   }
   ``

   The example above uses full parameter names for demonstration purposes, but you can abbreviate the parameters like this:

   ```bash
   dbcli create-backupconfig -n prodbackup -d disk -w 5
   ```

4. **Get the ID of the database you want to back up by using the Database Commands on page 1505 command.**

   ```bash
   [root@dbsys ~]# dbcli list-databases
   ID           Class  Shape  Storage  Status       DB Name     DB Version     CDB
   ------------------------- ---------- ---------- ---------- --------- --- ---------- ----------
   71ec8335-113a-46e3-b81f-235f4db6fde prod 12.1.0.2 true
   OLTP  odb1 ACFS Configured
   ```
5. Get the ID of the backup configuration by using the **Backupconfig Commands** on page 1491 command.

   ```bash
   [root@dbsbackup backup]# /opt/oracle/dcs/bin/dbcli list-backupconfigs
   ID                      Name                      DiskRecoveryWindow BackupDestination createTime              
   ---------------        ---------------------      ------------------------------ ---------------
   78a2a5f0-72b1-448f-bd86-cf41b30b64ee prodbackup        5        Disk            July 6, 2016 3:13:01 AM UTC
   
   ID
   ---------------
   78a2a5f0-72b1-448f-bd86-cf41b30b64ee
   
   Name
   ---------------------
   prodbackup
   
   CreateTime
   ------------------------------
   July 6, 2016 3:13:01 AM UTC
   ```

6. Associate the backup configuration ID with the database ID by using the **Database Commands** on page 1505 command.

   ```bash
   [root@dbsys ~]# dbcli update-database --backupconfigid 78a2a5f0-72b1-448f-bd86-cf41b30b64ee --dbid 71ec8335-113a-46e3-b81f-235f4d1b6fde
   {
     "jobId": "2b104028-a0a4-4855-b32a-b97a37f5f9c5",
     "status": "Created",
     "message": null,
     "reports": [],
     "createTimestamp": 1467775842977,
     "description": "update database id:71ec8335-113a-46e3-b81f-235f4d1b6fde",
     "updatedTime": 1467775842978
   }
   
   You can view details about the update job by using the **Job Commands** on page 1525 command and specifying the job ID from the `dbcli update-database` command output, for example:

   ```bash
   dbcli describe-job --jobid 2b104028-a0a4-4855-b32a-b97a37f5f9c5
   ```

7. Initiate the database backup by using the **Backup Commands** on page 1487 command. The backup operation is performed immediately.

   The following example creates a backup of the specified database.

   ```bash
   [root@dbsys ~]# dbcli create-backup --dbid 71ec8335-113a-46e3-b81f-235f4d1b6fde
   {
     "createTimestamp": 1467792576854,
     "description": "Backup service creation with db name: prod",
     "jobId": "d6c9edaa-fc80-40a9-bcdd-056430c56c",
     "message": null,
     "reports": [],
     "status": "Created",
     "updatedTime": 1467792576855
   }
   
   Or you can abbreviate the command parameters like this:

   ```bash
   dbcli create-backup -i 71ec8335-113a-46e3-b81f-235f4d1b6fde
   
   You can view details about the backup job by using the **Job Commands** on page 1525 command and specifying the job ID from the `dbcli create-backup` command output, for example:

   ```bash
   dbcli describe-job --jobid d6c9edaa-fc80-40a9-bcdd-056430c56c
   ```

8. **Important!** Manually back up any TDE password-based wallets to your choice of a safe location, preferably not on the DB system. The wallets are required to restore the backup to a new host.
After the backup command completes, the database backup files are available in the Fast Recovery Area on the DB system.

**Recovering a Database**

For information on restoring a database on a bare metal or virtual machine DB system, see the following topics:

- Recovering a Database from Object Storage on page 1446
- Recovering a Database from the Oracle Cloud Infrastructure Classic Object Store on page 1452

**Recovering a Database from Object Storage**

Note:

This topic is not applicable to Exadata DB systems.

This topic explains how to recover a database from a backup stored in Object Storage. The service is a secure, scalable, on-demand storage solution in Oracle Cloud Infrastructure. For information on using Object Storage as a backup destination, see Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435.

You can recover a database using the Console, API, or by using RMAN.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Prerequisites**

The DB system requires access to the Oracle Cloud Infrastructure Object Storage service, including connectivity to the applicable Swift endpoint for Object Storage. Oracle recommends using a service gateway with the VCN to enable this access. For more information, see these topics:

- Network Setup for DB Systems on page 1359: For information about setting up your VCN for the DB system, including the service gateway.
- Can I use Oracle Cloud Infrastructure Object Storage as a destination for my on-premises backups?: For information about the Swift endpoints to use.

**Using the Console**

You can use the Console to restore the database from a backup in the Object Storage that was created by using the Console or the API. You can restore to the last known good state of the database, or you can specify a point in time or an existing System Change Number (SCN). You can also create a new database by using a standalone backup.

Note:

The list of backups you see in the Console does not include any unmanaged backups (backups created directly by using RMAN or dbcli).

Restoring a database with Data Guard enabled is not supported. You must first remove the Data Guard association by terminating the standby database before you can restore the database.

**Restoring an Existing Database**

To restore a database

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.

A list of DB systems is displayed.
3. Find the DB system where the database is located, and click the system name to display details about it.
   A list of databases is displayed.
4. Find the database you want to restore, and click its name to display details about it.
   A list of backups is displayed in the default view of the database details. You can also access the list of backups for a database by clicking on Backups under Resources.
5. Click Restore.
6. Select one of the following options, and then click Restore Database:
   • Restore to the latest: Restores the database to the last known good state with the least possible data loss.
   • Restore to the timestamp: Restores the database to the timestamp specified.
   • Restore to System Change Number (SCN): Restores the database using the SCN specified. This SCN must be valid.
   
   **Tip:**
   You can determine the SCN number to use either by accessing and querying your database host, or by accessing any online or archived logs.
7. Confirm when prompted.
   If the restore operation fails, the database will be in a "Restore Failed" state. You can try restoring again using a different restore option. However, Oracle recommends that you review the RMAN logs on the host and fix any issues before reattempting to restore the database.

To restore a database using a specific backup from Object Storage
1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
   A list of DB systems is displayed.
3. Find the DB system where the database is located, and click the system name to display details about it.
   A list of databases is displayed.
4. Find the database you want to restore, and click its name to display details about it.
5. Click Restore.
6. In the Restore Database dialog, select Restore to the latest, Restore to timestamp, or Restore to System Change Number (SCN). Specify a timestamp or System Change Number if you are using an option that requires either.
7. Click Restore Database.

**Creating a New Database from a Backup**

You can use a backup to create a database in an existing DB system or to launch a new DB system. See the following procedures for more information:
• To create a database from a backup in an existing DB system on page 1417
• To create a DB system from a backup on page 1377

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to recover a database:
• ListBackups
• GetBackup
• RestoreDatabase
• CreateDbHome - For creating a DB system database from a standalone backup.

For the complete list of APIs for the Database service, see Database Service API.
Using an RMAN Backup

This topic explains how to recover a Recovery Manager (RMAN) backup stored in Object Storage.

Prerequisites

You’ll need the following:

- A new DB system to restore the database to (see assumptions below). For more information, see Creating Bare Metal and Virtual Machine DB Systems on page 1370.
- The Oracle Database Cloud Backup Module must be installed on the DB system. For more information, see Installing the Backup Module on the DB System on page 1441.

Assumptions

The procedures below assume the following:

- A new DB system has been created to host the restored database and no other database exists on the new DB system. It is possible to restore to a DB system that has existing databases, but that is beyond the scope of this topic.
- The original database is lost and all that remains is the latest RMAN backup. For virtual machine DB systems, the procedure assumes the DB system (inclusive of the database) no longer exists.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any data not included in the most recent backup will be lost.</td>
</tr>
</tbody>
</table>

- The Oracle Wallet and/or encryption keys used by the original database at the time of the last backup is available.
- The RMAN backup contains a copy of the control file and spfile as of the most recent backup as well as all of the datafile and archivelog backups needed to perform a complete database recovery.
- An RMAN catalog will not be used during the restore.

Setting Up Storage on the DB system

1. SSH to the DB System.

   ```
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as opc and then sudo to the root user. Use `sudo su -` with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (`/opt/oracle/dcs/bin`).

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. You can use an existing empty database home or create a new one for the restore. Use the applicable commands to help you complete this step.

   If you will be using an existing database home:

   - Use the Dbhome Commands on page 1518 command to list the database homes.

     ```
     [root@dbsys ~]# dbcli list-dbhomes
     ID   Home Location
     Name          DB Version
     ```

Oracle Cloud Infrastructure User Guide

1448
• Use the Database Commands on page 1505 command to ensure the database home is not associated with any database.

If necessary, use the Dbhome Commands on page 1518 command to create a database home for the restore.

4. Use the Dbstorage Commands on page 1521 to set up directories for DATA, RECO, and REDO storage. The following example creates 10GB of ACFS storage for the rectest database.

```bash
[root@dbsys ~]# dbcli create-dbstorage --dbname rectest --dataSize 10 --dbstorage ACFS
```

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When restoring a version 11.2 database, ACFS storage must be specified.</td>
</tr>
</tbody>
</table>

Performing the Database Restore and Recovery

1. SSH to the DB system, log in as opc, and then become the oracle user.

   ```bash
   sudo su - oracle
   ```

2. Create an entry in /etc/oratab for the database. Use the same SID as the original database.

   ```bash
dbl:/u01/app/oracle/product/12.1.0.2/dbhome_1:N
   ```

3. Set the ORACLE_HOME and ORACLE_SID environment variables using the oraenv utility.

   ```bash
   . oraenv
   ```

4. Obtain the DBID of the original database. This can be obtained from the file name of the controlfile autobackup on the backup media. The file name will include a string that contains the DBID. The typical format of the string is `c-DDDDDDDDDDDD-YYYYMMDD-NN` where `DDDDDDDDDDDD` is the `DBID`, `YYYYMMDD` is
the date the backup was created, and NN is a sequence number to make the file name unique. The DBID in the following examples is 1508405000. Your DBID will be different.

Use the following curl syntax to perform a general query of Object Storage. The parameters in red are the same parameters you specified when installing the backup module as described in Installing the Backup Module on the DB System on page 1441.

```
curl -u '<user_ID>.com:<auth_token>' -v https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/object_storage_namespace
```

See Regions and Availability Domains on page 180 to look up the region name.

For example:

```
curl -u 'djones@mycompany.com:1cnk!d0++ptETd&C;thR' -v https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/myobjectstoragenamespace
```

To get the DBID from the control file name, use the following syntax:

```
curl -u '<user_id>.com:<auth_token>' -v https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/object_storage_namespace/<bucket_name>?prefix=sbt_catalog/c-
```

For example:

```
curl -u 'djones@mycompany.com:1cnk!d0++ptETd&C;thR' -v https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/myobjectstoragenamespace/dbbackups/?prefix=sbt_catalog/c-
```

In the sample output below, 1508405000 is the DBID.

```
{
   "bytes": 1732,
   "content_type": "binary/octet-stream",
   "hash": "f1b61f08892734ed7af4f1d3a8be317",
   "last_modified": "2016-08-11T20:28:34.438000",
   "name": "sbt_catalog/c-1508405000-20160811-00/metadata.xml"
}
```

5. Run RMAN and connect to the target database. There is no need to create a spfile or spfile or use a backup controlfile. These will be restored in the following steps. Note that the target database is (not started). This is normal and expected at this point.

```
rman target /
```

RMAN target /
Recovery Manager: Release 12.1.0.2.0 - Production on Wed Jun 22 18:36:40 2016
Copyright (c) 1982, 2014, Oracle and/or its affiliates. All rights reserved.
connected to target database (not started)

6. Set the DBID using the value obtained above.

```
RMAN> set dbid 1508405000;
executing command: SET DBID
7. Run the STARTUP NOMOUNT command. If the server parameter file is not available, RMAN attempts to start the instance with a dummy server parameter file. The ORA-01078 and LRM-00109 errors are normal and can be ignored.

```
RMAN> STARTUP NOMOUNT

startup failed: ORA-01078: failure in processing system parameters
LRM-00109: could not open parameter file '/u01/app/oracle/product/12.1.0.2/dbhome_1/dbs/initdb1.ora'

starting Oracle instance without parameter file for retrieval of spfile
Oracle instance started

Total System Global Area 2147483648 bytes
Fixed Size 2944952 bytes
Variable Size 847249480 bytes
Database Buffers 1254096896 bytes
Redo Buffers 43192320 bytes
```

8. Restore the server parameter file from autobackup.

The SBT_LIBRARY is the same library specified with the -libDir parameter when the Backup Module was installed, for example /home/oracle/lib/.

The OPC_PFILE is the same file specified with the -configfile parameter when the Backup Module was installed, for example /home/oracle/config.

```
set controlfile autobackup format for device type sbt to '%F';
run {
    allocate channel c1 device type sbt PARMS 'SBT_LIBRARY=/home/oracle/lib/libopc.so, SBT_PARMS=(OPC_PFILE=/home/oracle/config)';
    restore spfile from autobackup;
}
```

9. Create the directory for audit_file_dest. The default is /u01/app/oracle/admin/$ORACLE_SID/adump.

You can see the setting used by the original database by searching the spfile for the string, audit_file_dest.

```
strings ${ORACLE_HOME}/dbs/spfile${ORACLE_SID}.ora | grep audit_file_dest
*.audit_file_dest='/u01/app/oracle/admin/db1/adump'
mkdir -p /u01/app/oracle/admin/db1/adump
```

10. If block change tracking was enabled on the original database, create the directory for the block change tracking file. This will be a directory under db_create_file_dest. Search the spfile for the name of the directory.

```
strings ${ORACLE_HOME}/dbs/spfile${ORACLE_SID}.ora | grep db_create_file_dest
*.db_create_file_dest='/u02/app/oracle/oradata/db1'
mkdir -p /u02/app/oracle/oradata/db1/<$ORA_UNQNAME if available or database name>/changetracking
```

11. Restart the instance with the restored server parameter file.

```
STARTUP FORCE NOMOUNT;
```

12. Restore the controlfile from the RMAN autobackup and mount the database.

```
set controlfile autobackup format for device type sbt to '%F';
run {
```
allocate channel c1 device type sbt PARMS 'SBT_LIBRARY=/home/oracle/lib/
libopc.so, SBT_PARMS=(OPC_PFILE=/home/oracle/config)';
  restore controlfile from autobackup;
  alter database mount;
}

13. Restore and recover the database.

    RESTORE DATABASE;
    RECOVER DATABASE;

14. RMAN will recover using archived redo logs until it can't find any more. It is normal for an error similar to the
    one below to occur when RMAN has applied the last archived redo log in the backup and can't find any more logs.

    unable to find archived log
    archived log thread=1 sequence=29
    RMAN-00571: =============== ERROR MESSAGE STACK FOLLOWS ===============
    RMAN-00569: -----------------------------------------
    RMAN-00571: -----------------------------------------
    RMAN-03002: failure of recover command at 06/28/2016 00:57:35
    RMAN-06054: media recovery requesting unknown archived log for thread 1
    with sequence 29 and starting SCN of 2349563

15. Open the database with resetlogs.

    ALTER DATABASE OPEN RESETLOGS;

The recovery is complete. The database will have all of the committed transactions as of the last backed up archived
redo log.

Recovering a Database from the Oracle Cloud Infrastructure Classic Object Store

Note:

This topic is not applicable to Exadata DB systems.

This topic explains how to recover a database using a backup created by the Oracle Database Backup Module and
stored in Oracle Cloud Infrastructure Object Storage Classic.

The following terms are used throughout this topic:

• Source database: The database backup in Object Storage Classic.
• Target database: The new database on a DB system in Oracle Cloud Infrastructure.

Prerequisites

You'll need the following:

• The service name, identity name, container, user name, and password for Oracle Cloud Infrastructure Object
  Storage Classic.
• The backup password if password-based encryption was used when backing up to Object Storage Classic.
• The source database ID, database name, database unique name (required for setting up storage).
• If the source database is configured with Transparent Data Encryption (TDE), you'll need a backup of the wallet
  and the wallet password.
• Tnsnames to setup for any database links.
• The output of Opatch lsinventory for the source database Oracle_home, for reference.
• A copy of the sqlpatch directory from the source database home. This is required for rollback in case the target
database does not include these patches.
**Setting Up Storage on the DB System**

1. SSH to the DB System.

   ```bash
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as opc and then sudo to the root user. Use `sudo su -` with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (`/opt/oracle/dcs/bin`).

   ```bash
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. Use the **Dbstorage Commands** on page 1521 command to set up directories for DATA, RECO, and REDO storage. The following example creates 10GB of ACFS storage for the tdetest database.

   ```bash
   [root@dbsys ~]$ dbcli create-dbstorage --dbname tdetest --dataSize 10 --dbstorage ACFS
   ```

   **Note:**
   When migrating a version 11.2 database, ACFS storage must be specified.

4. Use the **Dbstorage Commands** on page 1521 command to list the storage ID. You'll need the ID for the next step.

   ```bash
   [root@dbsys ~]$ dbcli list-dbstorages
   ID                  Type   DBUnique Name   Status
   ------------------- ------- ----------------- ------
   9dcdfb8e-e589-4d5f-861a-e5ba981616ed Acfs   tdetest   Configured
   ```

5. Use the **Dbstorage Commands** on page 1521 command with the storage ID from the previous step to list the DATA, RECO and REDO locations.

   ```bash
   [root@dbsys ~]$ dbcli describe-dbstorage --id 9dcdfb8e-e589-4d5f-861a-e5ba981616ed
   DBStorage details
   --------------------------------------------------------
   ID: 9dcdfb8e-e589-4d5f-861a-e5ba981616ed
   DB Name: tdetest
   DBUnique Name: tdetest
   DB Resource ID:
   Storage Type: Acfs
   DATA Location: /u02/app/oracle/oradata/tdetest
   RECO Location: /u03/app/oracle/fast_recovery_area/
   REDO Location: /u03/app/oracle/redo/
   State: ResourceState(status=Configured)
   Created: August 24, 2016 5:25:38 PM UTC
   UpdatedTime: August 24, 2016 5:25:53 PM UTC
   ```

6. Note the DATA, RECO and REDO locations. You'll need them later to set the `db_create_file_dest`, `db_create_online_log_dest`, and `db_recovery_file_dest` parameters for the database.

**Choosing an ORACLE_HOME**

Decide which ORACLE_HOME to use for the database restore and then switch to that home with the correct ORACLE_BASE, ORACLE_HOME, and PATH settings. The ORACLE_HOME must not already be associated with a database.
To get a list of existing ORACLE_HOMEs and to ensure that the ORACLE_HOME is empty, use the Dbhome Commands on page 1518 and the Database Commands on page 1505 commands, respectively. To create a new ORACLE_HOME, use the Dbhome Commands on page 1518 command.

**Copying the Source Database Wallets**

Skip this section if the source database is **not** configured with TDE.

1. On the DB system, become the oracle user:
   ```bash
   sudo su - oracle
   ```

2. Create the following directory, if it does not already exist:
   ```bash
   mkdir /opt/oracle/dcs/commonstore/wallets/tde/<db_unique_name>
   ```

3. Copy the ewallet.p12 file from the source database to the directory you created in the previous step.

4. On the target host, make sure that `$ORACLE_HOME/network/admin/sqlnet.ora` contains the following line:
   ```ora
   ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/opt/oracle/dcs/commonstore/wallets/tde/$ORACLE_UNQNAME))
   ```

   Add the line if it doesn't exist in the file. (The line might not be there if this is a new home and no database has been created yet on this host.)

5. Create the autologin wallet from the password-based wallet to allow auto-open of the wallet during restore and recovery operations.

   For a version 12.1 or later database, use the `ADMINISTER KEY MANAGEMENT` command:
   ```bash
   $ cat create_autologin_12.sh
   #!/bin/sh
   if [ $# -lt 2 ]; then
     echo "Usage: $0 <dbuniquename><remotewalletlocation>"
     exit 1;
   fi
   mkdir /opt/oracle/dcs/commonstore/wallets/tde/$1
   cp $2/ewallet.p12* /opt/oracle/dcs/commonstore/wallets/tde/$1
   rm -f autokey.ora
   echo "db_name=$1" > autokey.ora
   autokeystoreLog="autologinKeystore_`date +%Y%m%d_%H%M%S_%N`.log"
   echo "Enter Keystore Password:"
   read -s keystorePassword
   echo "Creating AutoLoginKeystore -> "
   sqlplus "/ as sysdba" <<EOF
   spool $autokeystoreLog
   set echo on
   startup nomount pfile=autokey.ora
   ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE
   FROM KEYSTORE '/opt/oracle/dcs/commonstore/wallets/tde/$1' -- Keystore location
   IDENTIFIED BY "$keystorePassword';
   shutdown immediate;
   EOF
   ```

   Adjust the `cwallet.sso` permissions from `oracle:asmadmin` to `oracle:oinstall`.
   ```bash
   $ ls -ltr /opt/oracle/dcs/commonstore/wallets/tde/<db_unique_name>
   total 20
   ```
For a version 11.2 database, use the orapki command:

```
orapki wallet create -wallet wallet_location -auto_login [-pwd password]
```

### Installing the Oracle Database Backup Module

The backup module JAR file is included on the DB system but you need to install it.

1. SSH to the DB system, log in as opc, and then become the oracle user.

   ```
   ssh -i <path to SSH key used when launching the DB System> opc@<DB System IP address or hostname>
   sudo su - oracle
   ```

2. Change to the directory that contains the backup module opc_install.jar file.

   ```
   cd /opt/oracle/oak/pkgrepos/orapkgs/oss/＜version＞/
   ```

3. Use the command syntax described in Installing the Oracle Database Cloud Backup Module to install the backup module.

### Setting Environment Variables

Set the following environment variables for the RMAN and SQL*Plus sessions for the database:

```
ORACLE_HOME=<path of Oracle Home where the database is to be restored>
ORACLE_SID=<database instance name>
ORACLE_UNQNAME=<db_unique_name in lower case>
NLS_DATE_FORMAT="mm/dd/yyyy hh24:mi:ss"
```

### Allocating an RMAN SBT Channel

For each restore operation, allocate an SBT channel and set the SBT_LIBRARY parameter to the location of the libopc.so file and the OPC_FILE parameter to the location of the opc_sbt.ora file, for example:

```
ALLOCATE CHANNEL c1 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U'
PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/<ORACLE_HOME>/dbs/opc_sbt.ora)';
```

(For more information about these files, see Files Created When the Backup Module is Installed.)

### Ensuring Decryption is Turned On

Make sure that decryption is turned on for all the RMAN restore sessions.

```
set decryption wallet open identified by <keystore password> ;
```

For more information, see Providing Password Required to Decrypt Encrypted Backups.

### Restoring Spfile

The following sample shell script restores the spfile. Set the $dbID variable to the dbid of the database being restored. By default, spfile is restored to $ORACLE_HOME/dbs/spfile$<sid>.ora.

```
 rman target / <<EOF
spool log to "\date +%Y%m%d%H%M%S\_dbid_$(dbID)_restore_spfile.log"
startup nomount
```
Setting the Database Parameters

1. Start the database in nomount mode.

   ```
   startup nomount
   ```

2. Update spfile and modify the following parameters.

   - If the database storage type is ACFS, use the DATA, RECO, and REDO locations obtained from the `dbcli describe-dbstorage` command output, as described in Setting Up Storage on the DB System on page 1453:

     ```
     alter system set db_create_file_dest='/u02/app/oracle/oradata/' scope = spfile;
     alter system set db_create_online_log_dest_1='/u03/app/oracle/redo' scope = spfile;
     alter system set db_recovery_file_dest='/u03/app/oracle/fast_recovery_area' scope = spfile;
     ```

   - If the database storage type is ASM:

     ```
     alter system set db_create_file_dest='+DATA' scope = spfile;
     alter system set db_create_online_log_dest_1='+RECO' scope = spfile;
     alter system set db_recovery_file_dest='+RECO' scope = spfile;
     ```

   - Set `db_recovery_file_dest_size` is not set or is set incorrectly:

     ```
     alter system set db_recovery_file_dest_size=<sizeG> scope=spfile;
     ```

   - Set `audit_file_dest` to the correct value:

     ```
     alter system set audit_file_dest=/u01/app/oracle/admin/<db_unique_name in lower case>/adump
     ```

3. Remove the `control_files` parameter. The Oracle Managed Files (OMF) parameters will be used to create the control file.

   ```
   alter system reset control_files scope=spfile;
   ```

4. Restart the database in nomount mode using the newly added parameters.

   ```
   shutdown immediate
   startup nomount
   ```

Restoring the Control File

Modify the following sample shell script for your environment to restore the control file. Set the `$dbID` variable to the dbid of the database being restored. Set `SBT_LIBRARY` to the location specified in the `-libDir` parameter when you installed the Backup Module. Set `OPC_PFILE` to the location specified in the `-configFile` parameter, which defaults to `ORACLE_HOME/dbs/opcSID.ora`.

```
rman target / <<EOF
spool log to "`date +%Y%m%d_%H%M%S_%N`_dbid_${dbID}_restore_controlfile.log"
```
Restoring the Database

1. Preview and validate the backup. The database is now mounted and RMAN should be able to locate the backup from the restored controlfile. This step helps ensure that the list of archivelogs is present and that the backup components can be restored.

   In the following examples, modify SBT_LIBRARY and OPC_PFILE as needed for your environment.

   ```
   rman target / <<EOF
   spool log to "`date +%Y%m%d_%H%M%S_%N`_restore_database_preview.log"
   set echo on
   run {
   ALLOCATE CHANNEL c1 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U' PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/tmp/oss/opc_sbt.ora)';
   ALLOCATE CHANNEL c2 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U' PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/tmp/oss/opc_sbt.ora)';
   ALLOCATE CHANNEL c3 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U' PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/tmp/oss/opc_sbt.ora)';
   restore database validate header preview;
   }
   EOF
   ```

   Review the output and if there are error messages, investigate the cause of the problem.

2. Redirect the restore using `set newname` to restore the data files in OMF format and use `switch datafile all` to allow the control file to update with the new data file copies.

   ```
   rman target / <<EOF
   spool log to "`date +%Y%m%d_%H%M%S_%N`_restore_database_preview.log"
   set echo on
   run {
   ALLOCATE CHANNEL c1 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U' PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/tmp/oss/opc_sbt.ora)';
   ALLOCATE CHANNEL c2 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U' PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/tmp/oss/opc_sbt.ora)';
   ALLOCATE CHANNEL c3 DEVICE TYPE sbt MAXPIECESIZE 2 G FORMAT '%d_%I_%U' PARMS 'SBT_LIBRARY=/tmp/oss/libopc.so ENV=(OPC_PFILE=/tmp/oss/opc_sbt.ora)';
   set newname for database to new;
   restore database;
   switch datafile all;
   switch tempfile all;
   recover database;
   ```
This recovery will attempt to use the last available archive log backup and then fail with an error, for example:

RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of recover command at 07/20/2016 12:09:02
RMAN-06054: media recovery requesting unknown archived log for thread 1
with sequence 22 and starting SCN of 878327

3. To complete the incomplete recovery, run a recovery using the sequence number and thread number shown in the RMAN-06054 message, for example:

Recover database until sequence 22 thread 1;

Resetting the Logs
Reset the logs.

alter database open resetlogs;

Preparing to Register the Database
Before you register the database:

1. Make sure the database COMPATIBLE parameter value is acceptable. If the value is less than the minimum, the database cannot be registered until you upgrade the database compatibility.

   The minimum compatibility values are as follows:
   • For a version 18.1 database - 18.0.0.0
   • For a version 12.2 or 12.1 database - 12.1.0.2
   • For a version 11.2 database - 11.2.0.4

2. Verify that the database has registered with the listener and the service name.

   lsnrctl services

3. Make sure the password file was restored or created for the new database.

   ls -ltr $ORACLE_HOME/dbs/orapw<oracle sid>

   If the file does not exist, create it using the orapwd utility.

   orapwd file=$ORACLE_HOME/dbs/orapw<ORACLE_SID> password=<sys password>

4. Make sure the restored database if open in read write mode.

   select open_mode from v$database;

   The command output should indicate read write mode. The dbcli register-database command will attempt to run datapatch, which requires read write mode. If there are PDBs, they should also be in read write mode to ensure that datapatch runs on them.

5. From oracle home on the restored database, use the following command verify the connection to SYS:

   conn sys/<password>@//<hostname>:1521/<database service name>

   This connection is required to register the database later. Fix any connection issues before continuing.
6. Make sure the database is running on spfile by using the SQL*Plus command.

```
SHOW PARAMETERS SPFILE
```

7. (Optional) If you would like to manage the database backup with the dbcli command line interface, you can associate a new or existing backup configuration with the migrated database when you register it or after you register it. A backup configuration defines the backup destination and recovery window for the database. Use the following commands to create, list, and display backup configurations:

- **Backupconfig Commands** on page 1491
- **Backupconfig Commands** on page 1491
- **Backupconfig Commands** on page 1491

8. Copy the folder `$ORACLE_HOME/sqlpatch` from source database to the target database. This will enable the `dbcli register-database` command to roll back any conflicting patches.

```
Note:
If you are migrating a version 11.2 database, additional steps are required after you register the database. For more information, see **Rolling Back Patches on a Version 11.2 Database** on page 1459.
```

### Registering the Database on the DB System

The **Database Commands** on page 1505 command registers the restored database to the dcs-agent so it can be managed by the dcs-agent stack.

```
Note:
The dbcli register-database command is not available on 2-node RAC DB systems.
```

As the root user, use the `dbcli register-database` command to register the database on the DB system, for example:

```
[root@dbsys ~]# dbcli register-database --dbclass OLTP --dbshape odb1 --servicename tdetest --syspassword
Password for SYS:
{
   "jobId" : "317b430f-ad5f-42ae-bb07-13f053d266e2",
   "status" : "Created",
   "message" : null,
   "reports" : [
   ],
   "createTimestamp" : "August 08, 2016 05:55:49 AM EDT",
   "description" : "Database service registration with db service name: tdetest",
   "updatedTime" : "August 08, 2016 05:55:49 AM EDT"
}
```

### Updating tnsnames.ora

Check the `tnsnames.ora` in the backup location, check the database links used in the cloned database, and then add any relevant connection strings to the cloned database file at `$ORACLE_HOME/network/admin/tnsnames.ora`.

### Rolling Back Patches on a Version 11.2 Database

For version 11.2 databases, the `sqlpatch` application is not automated, so any interim patches (previously known as a "one-off" patches) applied to the source database that are not part of the installed PSU must be rolled back manually in the target database. After registering the database, execute the `catbundle.sql` script and then the `postinstall.sql` script with the corresponding PSU patch (or the overlay patch on top of the PSU patch), as described below.
Tip:

Some interim patches may include files written to the $ORACLE_HOME/rdbms/admin directory as well as the $ORACLE_HOME/sqlpatch directory. Oracle recommends that you roll back these patches in the source database using the instructions in the patch read-me prior to migrating the database to OCI environment. Contact Oracle Support if you need assistance with rolling back these patches.

1. On the DB System, use the `dbcli list-dbhomes` command to find the PSU patch number for the version 11.2 database home. In the following sample command output, the PSU patch number is the second number in the DB Version column:

   ![Command Output]

   (The first patch number, 23054319 in the example above, is for the OCW component in the database home.)

2. Find the overlay patch, if any, by using the `lsinventory` command. In the following example, patch number 24460960 is the overlay patch on top of the 23054359 PSU patch.

   ![Inventory Output]

3. Start SQL*Plus and execute the `catbundle.sql` script, for example:

   ![SQL Execution]

4. Apply the sqlpatch, using the overlay patch number from the previous step, for example:

   ![SQL Execution]
Note:

If the source database has one-off patches installed and those patches are not part of the installed PSU in the cloud environment, then the SQL changes that correspond to those one-off patches need to be rolled back. To rollback the SQL changes, copy the $ORACLE_HOME/sqlpatch/<patch#>/postdeinstall.sql script from the source environment to the cloud environment and execute the postdeinstall.sql script.

Post Restore Checklist

After the database is restored and registered on the DB system, use the following checklist to verify the results and perform any post-restore customizations.

1. Make sure the database files were restored in OMF format.
2. Make sure the database is listed in the Database Commands on page 1505 command output.
3. Check for the following external references in the database and update them if necessary:
   - External tables: If the source database uses external tables, back up that data and migrate it to the target host.
   - Directories: Customize the default directories as needed for the restored database.
   - Database links: Make sure all the required TNS entries are updated in the tnsnames.ora file in ORACLE_HOME.
   - Email and URLs: Make sure any email addresses and URLs used in the database are still accessible from the DB system.
   - Scheduled jobs: Review the jobs scheduled in source database and schedule similar jobs as needed in the restored database.
4. If you associated a backup configuration when you registered the database, run a test back up using the Backup Commands on page 1487 command.
5. If the restored database contains a CDB and PDBs, verify that patches have been applied to all PDBs.

Using Oracle Data Guard

Note:

This procedure is only applicable to bare metal and virtual machine DB systems. To use Oracle Data Guard with Exadata, see Using Oracle Data Guard with Exadata Cloud Service on page 1339.

This topic explains how to use the Console to manage Oracle Data Guard associations in your DB system.

For complete information on Oracle Data Guard, see the Data Guard Concepts and Administration documentation in the Oracle Help Center.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you are new to policies, then see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Prerequisites

An Oracle Data Guard implementation requires two DB systems, one containing the primary database and one containing the standby database. When you enable Oracle Data Guard for a virtual machine DB system database, a new DB system with the standby database is created and associated with the primary database. For a bare metal DB
system, the DB system with the database that you want to use as the standby must already exist before you enable Oracle Data Guard.

**Tip:**

An Oracle Data Guard configuration on the Oracle Cloud Infrastructure is limited to one standby database for each primary database.

Requirement details are as follows:

- Both DB systems must be in the same compartment.
- The DB systems must be the same shape type (for example, if the shape of the primary database is a virtual machine, then the shape of the standby database can be any other virtual machine shape).
- The database versions and editions must be identical. Oracle Data Guard does not support Oracle Database Standard Edition. (Active Data Guard requires Enterprise Edition - Extreme Performance.)
- The database version determines whether Active Data Guard is enabled. If you are using the BYOL licensing model and if your license does not include Active Data Guard, then you must either use Oracle Database Enterprise Edition - High Performance or set up Oracle Data Guard manually. See Using Oracle Data Guard with the Database CLI on page 1469.
- If your primary and standby databases are in the same region, then both must use the same virtual cloud network (VCN).
- If your primary and standby databases are in different regions, then you must peer the virtual cloud networks (VCNs) for each database. See Remote VCN Peering (Across Regions) on page 3280.
- Configure the security list ingress and egress rules for the subnets of both DB systems in the Oracle Data Guard association to enable TCP traffic to move between the applicable ports. Ensure that the rules you create are stateful (the default).

For example, if the subnet of the primary DB system uses the source CIDR 10.0.0.0/24 and the subnet of the standby DB system uses the source CIDR 10.0.1.0/24, then create rules as shown in the subsequent example.

**Note:**

The egress rules in the example show how to enable TCP traffic only for port 1521, which is a minimum requirement for Oracle Data Guard to work. If TCP traffic is already enabled on all of your outgoing ports (0.0.0.0/0), then you do not need to explicitly add these specific egress rules.

**Security List for Subnet on the Primary DB System**

**Ingress Rules:**

- Stateless: No
- Source: 10.0.1.0/24
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Allows: TCP traffic for ports: 1521

**Egress Rules:**

- Stateless: No
- Destination: 10.0.1.0/24
- IP Protocol: TCP
- Source Port Range: All
- Destination Port Range: 1521
- Allows: TCP traffic for ports: 1521

**Security List for Subnet on the Standby DB System**

**Ingress Rules:**

- Stateless: No
For information about creating and editing rules, see Security Lists on page 2850.

**Availability Domain and Fault Domain Considerations for Oracle Data Guard**

Oracle recommends that the DB system that contains the standby database be in a different availability domain from that of the DB system containing the primary database to improve availability and disaster recovery. If you enable Oracle Data Guard for a database and your standby database is in the same availability domain as the primary database (either by choice, or because you are working in a single availability domain region), then Oracle recommends that you place the standby database in a different fault domain from that of the primary database.

**Note:**

If your primary and standby databases are two-node Oracle RAC databases and both are in the same availability domain, then only one of the two nodes of the standby database can be in a fault domain that does not include any other nodes from either the primary or standby database. This is because each availability domain has only three fault domains, and the primary and standby databases have a combined total of four nodes. For more information on availability domains and fault domains, see Regions and Availability Domains on page 180.

**Working with Oracle Data Guard**

Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data. The Oracle Cloud Infrastructure Database Data Guard implementation requires two databases: one in a primary role and one in a standby role. The two databases make an Oracle Data Guard association. Most of your applications access the primary database, while the standby database is a transactionally consistent copy of the primary database.

Oracle Data Guard maintains the standby database by transmitting and applying redo data from the primary database. If the primary database becomes unavailable, then you can use Oracle Data Guard to switch or fail over the standby database to the primary role.

**Tip:**

The standby databases in Oracle Cloud Infrastructure Database are physical standbys.

**Switchover**

A switchover reverses the primary and standby database roles. Each database continues to participate in the Oracle Data Guard association in its new role. A switchover ensures no data loss. Performing planned maintenance on a DB system with an Oracle Data Guard association is typically done by switching the primary database to the standby role, performing maintenance on the standby database, and then switching it back to the primary role.
Failover
A failover transitions the standby database into the primary role after the existing primary database fails or becomes unreachable. A failover might result in some data loss when you use Maximum Performance protection mode.

Reinstate
Reinstates a database into the standby role in an Oracle Data Guard association. You can use the reinstate command to return a failed database into service after correcting the cause of failure.

Note:
You cannot terminate a primary database that has an Oracle Data Guard association with a standby database until you first delete the standby database. Alternatively, you can switch over the primary database to the standby role, and then terminate it.
You cannot terminate a DB system that includes databases that have Oracle Data Guard enabled. To remove the Oracle Data Guard association:
• For a bare metal DB system database you can terminate the standby database.
• For a virtual machine DB system database you can terminate the standby DB system.

Terminating a DB System with Data Guard
If you want to terminate a DB system that has Data Guard enabled, you must terminate the standby DB system before terminating the primary DB system. If you try to terminate a primary DB system that has a standby, the terminate operation will not complete. See To terminate a DB system on page 1386 for instructions on terminating a DB system.

Using the Console
Use the Console to enable an Oracle Data Guard association between databases, change the role of a database in an Oracle Data Guard association using either a switchover or a failover operation, and reinstate a failed database.

When you enable Oracle Data Guard, a separate Oracle Data Guard association is created for the primary and the standby databases.

To enable Oracle Data Guard on a bare metal DB system

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the Compartment that contains a DB system with a database for which you want to enable Oracle Data Guard.
3. Click the name of a DB system that contains a database you want to assume the primary role.
4. On the DB System Details page, in the Databases section, click the name of the database you want to make primary.
5. On the Database Details page, in the Resources section, click Data Guard Associations.
6. In the Data Guard Associations section, click Enable Data Guard.
7. On the **Enable Data Guard** page, configure the Oracle Data Guard association.
   - The settings in the **Data Guard association details** section are read only and cannot be changed.
   - **Protection mode**: The protection mode used for this Oracle Data Guard association is set to **Maximum Performance**.
   - **Transport type**: The redo transport type used for this Oracle Data Guard association is set to **Async** (asynchronous).
   - In the **Select peer DB system** section, provide the following information for the standby database to obtain a list of available DB systems in which to locate the standby database:
     - **Region**: Select a region where you want to locate the standby database. The region where the primary database is located is selected, by default. You can choose to locate the standby database in a different region. The hint text associated with this field tells you in which region the primary database is located.
     - **Availability domain**: Select an availability domain for the standby database. The hint text associated with this field tells you in which availability domain the primary database is located.

   **Note:**
   If your standby database is in a region with only one availability domain, or if you choose to provision your standby database in the same availability domain as your primary database, then the system asks you to specify a number of optional fault domains from the **Fault domain** drop-down for your standby database. Oracle recommends that you locate your standby database in a different fault domain from your primary database. For more information on fault domains, see **Regions and Availability Domains** on page 180.

     - **Shape**: Select the shape of the DB system in which to locate the standby database. The shape can be another bare metal DB system shape.
     - **Peer DB system**: Select a DB system in which to locate the standby database.
   - In the **Configure standby database** section, enter the database administrator password of the primary database in the **Database password** field. Use this same database administrator password for the standby database.

8. Click **Enable Data Guard**.

When you create the association, the details for a database and its peer display their respective roles as **Primary** or **Standby**.

### To enable Oracle Data Guard on a virtual machine DB system

If you do not already have a virtual machine DB system with a database that will assume the primary role, then create a database as described in **Creating Bare Metal and Virtual Machine DB Systems** on page 1370. A new DB system includes an initial database. When you enable Oracle Data Guard on the primary database, a virtual machine DB system gets created for the standby database.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose the **Compartment** that contains a DB system with a database for which you want to enable Oracle Data Guard.
3. Click the name of a DB system that contains a database you want to assume the primary role.
4. On the DB System Details page, in the **Databases** section, click the name of the database you want to make primary.
5. On the Database Details page, in the Resources section, click **Data Guard Associations**.
6. In the **Data Guard Associations** section, click **Enable Data Guard**.
7. On the **Enable Data Guard** page, configure your Oracle Data Guard association.

- The settings in the **Data Guard association details** section are read only and cannot be changed.
  - **Protection mode**: The protection mode used for this Oracle Data Guard association is set to **Maximum Performance**.
  - **Transport type**: The redo transport type used for this Oracle Data Guard association is set to **Async** (asynchronous).
- Specify the following values in the **Create peer DB system** section for the standby database:
  - **Display name**: Enter a non-unique display name for the DB system containing the standby database. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system. Avoid entering confidential information.
  - **Region**: Select a region where you want to locate the standby database. The region where the primary database is located is selected, by default. You can choose to locate the standby database in a different region. The hint text associated with this field tells you in which region the primary database is located.
  - **Availability domain**: Select an availability domain for the standby database. The hint text associated with this field tells you in which availability domain the primary database is located.

  **Note:**

  If your standby database is in a region with only one availability domain, or if you choose to provision your standby database in the same availability domain as your primary database, then the system asks you to specify a number of optional fault domains from the **Fault domain** drop-down for your standby database. Oracle recommends that you locate your standby database in a different fault domain from your primary database. For more information on fault domains, see **Regions and Availability Domains** on page 180.

  - **Select a shape**: Choose a shape to use to create the standby DB system. To specify a shape other than the default, click **Change Shape** and select an available virtual machine shape from the list.

  - In the **Specify the network information** section:
    - **Virtual cloud network in compartment**: Select a virtual cloud network from the drop-down in which to create the DB system containing the standby database. Click **Change Compartment** to select a virtual cloud network in a different compartment.
    - **Subnet in compartment**: The subnet to which the DB system containing the standby database attaches. Click **Change Compartment** to select a subnet in a different compartment.

      Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.

    - **Configure network security groups (NSGs)**: Select to add a number of network security groups, which function as virtual firewalls, enabling you to apply a set of security rules that control inbound and outbound traffic for the DB system containing the standby database. For more information, see **Network Security Groups** on page 2841 and **Network Setup for DB Systems** on page 1359.

      **Note:**

      - If you choose a subnet with a security list, then the security rules for the DB system will be a combination of the rules in the security list and the network security groups.
      - You must select a virtual cloud network to be able to assign network security groups to your DB system.

    - **Hostname prefix**: Enter a host name prefix for the DB system that contains the standby database. The host name must begin with an alphabetic character, and can contain only alphanumeric characters.
and hyphens (-). The maximum number of characters allowed for bare metal and virtual machine DB systems is 16.

**Important:**

If the host name within the subnet is not unique, then provisioning of the DB system fails.

- **Host domain name:** The domain name for the DB system. If the subnet you selected uses the Oracle-provided internet and virtual cloud network resolver for DNS name resolution, then this field displays the domain name for the subnet, which you cannot change. Otherwise, you can enter a domain name. Hyphens (-) are not permitted.

- **Host and domain URL:** Combines the host and domain names to display the fully-qualified domain name for the database. The maximum length is 64 characters.

- In the **Configure standby database** section, enter the database administrator password of the primary database in the **Database password** field. Use this same database administrator password for the standby database.

- **Database Admin Password:** Enter the primary database admin password.

  The same password is used for the standby database.

- **Confirm Database Admin Password:** Re-enter the Database Admin Password you specified.

8. Click **Enable Data Guard**.

When you create the association, the details for a database and its peer display their respective roles as **Primary** or **Standby**.

**Virtual machine shapes**

**Virtual machine X7 shapes:**

- VM.Standard2.1: Provides a 1-node DB system with 1 core.
- VM.Standard2.2: Provides a 1- or 2-node DB system with 2 cores.
- VM.Standard2.4: Provides a 1- or 2-node DB system with 4 cores.
- VM.Standard2.8: Provides a 1- or 2-node DB system with 8 cores.
- VM.Standard2.16: Provides a 1- or 2-node DB system with 16 cores.
- VM.Standard2.24: Provides a 1- or 2-node DB system with 24 cores.

**Virtual machine X5 shapes:**

- VM.Standard1.1: Provides a 1-node DB system with 1 core.
- VM.Standard1.2: Provides a 1- or 2-node DB system with 2 cores.
- VM.Standard1.4: Provides a 1- or 2-node DB system with 4 cores.
- VM.Standard1.8: Provides a 1- or 2-node DB system with 8 cores.
- VM.Standard1.16: Provides a 1- or 2-node DB system with 16 cores.

**Note:**

- X5-based shapes availability is limited to monthly universal credit customers existing on or before November 9th, 2018, in the US West (Phoenix), US East (Ashburn), and Germany Central (Frankfurt) regions.
- VM.Standard1.1 and VM.Standard2.1 shapes cannot be used for 2-node RAC clusters.

**To perform a database switchover**

You initiate a switchover operation by using the Data Guard association of the primary database.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Choose the **Compartment** that contains the DB system with the primary database you want to switch over.
3. Click the DB system name, and then click the name of the primary database.
4. Under **Resources**, click **Data Guard Associations**.
5. For the Data Guard association on which you want to perform a switchover, click the Actions icon (three dots), and then click **Switchover**.

6. In the **Switchover Database** dialog box, enter the database admin password, and then click **OK**.

   This database should now assume the role of the standby, and the standby should assume the role of the primary in the Data Guard association.

**To perform a database failover**

You initiate a failover operation by using the Data Guard association of the standby database.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose the **Compartment** that contains the DB system with the primary database's peer standby you want to fail over to.

3. Click the DB system name, and then click the name of the standby database.

4. Under **Resources**, click **Data Guard Associations**.

5. For the Data Guard association on which you want to perform a failover, click **Failover**.

6. In the **Failover Database** dialog box, enter the database admin password, and then click **OK**.

   This database should now assume the role of the primary, and the old primary's role should display as **Disabled Standby**.

**To reinstate a database**

After you fail over a primary database to its standby, the standby assumes the primary role and the old primary is identified as a disabled standby. After you correct the cause of failure, you can reinstate the failed database as a functioning standby for the current primary by using its Data Guard association.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before you can reinstate a 12.2 database, you must perform some steps on the database host to stop the database or start it in MOUNT mode.</td>
</tr>
<tr>
<td>Set your ORACLE_UNQNAME environment variable to the value of the Database Unique Name (as seen in the Console), and then run these commands:</td>
</tr>
<tr>
<td>srvctl stop database -d db-unique-name -o abort</td>
</tr>
<tr>
<td>srvctl start database -d db-unique-name -o mount</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose the **Compartment** that contains the DB system with the failed database you want to reinstate.

3. Click the DB system name, and then click the database name.

4. Under **Resources**, click **Data Guard Associations**.

5. For the Data Guard association on which you want to reinstate this database, click the Actions icon (three dots), and then click **Reinstate**.

6. In the **Reinstate Database** dialog box, enter the database admin password, and then click **OK**.

   This database should now be reinstated as the standby in the Data Guard association.

**To terminate a Data Guard association on a bare metal DB system**

On a bare metal DB system, you remove a Data Guard association by terminating the standby database.

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.

2. Choose the **Compartment** that contains the DB system that includes the standby database you want to terminate.

3. Click the DB system name.

4. For the standby database you want to terminate, click the Actions icon (three dots), and then click **Terminate**.

5. In the **Terminate Database** dialog box, enter the name of the database, and then click **OK**.
To terminate a Data Guard association on a virtual machine DB system

On a virtual machine DB system, you remove a Data Guard association by terminating the standby DB system.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the Compartment that contains the standby DB system that you want to terminate.
3. Click the DB system name, click the Actions icon (three dots), and then click Terminate.
4. Confirm when prompted.

The DB system's icon indicates Terminating.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage Data Guard associations:

• CreateDataGuardAssociation
• GetDataGuardAssociation
• ListDataGuardAssociations
• SwitchDataGuardAssociation
• FailoverDataGuardAssociation
• RevertDataGuardAssociation
• DeleteDbHome - To terminate a bare metal DB system Data Guard association, delete the standby database.
• TerminateDbSystem - To terminate a virtual machine DB system Data Guard association, terminate the standby DB system.

For the complete list of APIs for the Database service, see Database Service API.

Using Oracle Data Guard with the Database CLI

Oracle recommends that you use the Console instead of the database CLI to set up and work with Data Guard in Oracle Cloud Infrastructure. See Using Oracle Data Guard on page 1461 for information and instructions.

Note:

This topic is not applicable to Exadata DB systems. You can manually configure Data Guard on Exadata DB systems using native Oracle Database utilities and commands, however this topic explains how set up primary and standby databases using dbcli, which is not available on Exadata DB systems. For more information, see Data Guard Concepts and Administration for version 18.1, 12.2, 12.1, or 11.2.

This topic explains how to use the database CLI to set up Data Guard with Fast-Start Failover (FSFO) in Oracle Cloud Infrastructure. The following sections explain how to prepare the primary and standby databases, and then configure Data Guard to transmit redo data from the primary database and apply it to the standby database.

Note:

This topic assumes that you are familiar with Data Guard and FSFO. To learn more about them, see documentation at the Oracle Document Portal.

Prerequisites

To perform the procedures in this topic, you'll need the following information for the primary and standby databases.

• db_name (or oracle_sid)
• db_unique_name
• oracle home directory (or database home)
To find the database information

After you’ve launched the primary and standby DB systems and created databases as described later in this topic, you can use the CLI on those systems to find the needed database information.

1. SSH to the DB System.

   ```
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as opc and then sudo to the root user. Use `sudo su -` with a hyphen to invoke the root user’s profile, which will set the PATH to the dbcli directory (/opt/oracle/dcs/bin).

   ```
   login as: opc
   [opc@dbsys ~]$ sudo su -
   ```

3. To find the db_name (or oracle_sid) and db_uniqueName, run the `dbcli list-databases -j` command.

   ```
   [root@dbsys ~]# dbcli list-databases -j
   [ {
   "id" : "80ad855a-5145-4f8f-a08f-406c5e4684ff",
   "name" : "dbtst",
   "dbName" : "dbtst",
   "databaseUniqueName" : "dbtst_phx1cs",
   "dbVersion" : "12.1.0.2",
   "dbHomeId" : "2efe7af7-0b70-4e9b-ba8b-71f1c6fe287",
   "instanceOnly" : false,
   .
   .
   }
   ```

4. To find the oracle home directory (or database home), run the `dbcli list-dbhomes` command. If there are multiple database homes on the DB system, use the one that matches the "dbHomeId" in the `dbcli list-databases -j` command output shown above.

   ```
   [root@dbtst ~]# dbcli list-dbhomes
   ID                                       Name                 DB Version     Home Location
   Status
   ----------- ------------------ ------------------ ------------------ 
   2efe7af7-0b70-4e9b-ba8b-71f1c6fe287     OraDB12102_home1   12.1.0.2.160719 (23739960, 23144544) /u01/app/oracle/product/12.1.0.2/dbhome_1 Configured
   33ae99fe-5413-4392-88da-997f3cd24c0f     OraDB11204_home1   11.2.0.4.160719 (23054319, 23054359) /u01/app/oracle/product/11.2.0.4/dbhome_1 Configured
   ```

Creating a Primary DB System

If you don’t already have a primary DB system, create one as described in Creating Bare Metal and Virtual Machine DB Systems on page 1370. The DB system will include an initial database. You can create additional databases by using the Database Commands on page 1505 command available on the DB system.

Creating a Standby DB System

**Note:**

The standby database must have the same db_name as the primary database, but it must have a different db_unique_name. If you use the same database
name for the standby and primary, you will have to delete the database from the standby DB system by using the dbcli delete-database command before you can run the dbcli create-database command described below. Deleting and creating the database will take several minutes to complete. The dbcli commands must be run as the root user.

1. Create a standby DB system as described in Creating Bare Metal and Virtual Machine DB Systems on page 1370 and wait for the DB system to finish provisioning and become available.

   You can create the standby DB system in a different availability domain from the primary DB system for availability and disaster recovery purposes (this is strongly recommended). You can create the standby DB system in the primary DB system's cloud network so that both systems are in a single, routable network.

2. SSH to the DB System.

   ssh -i <private_key_path> opc@<db_system_ip_address>

3. Log in as opc and then sudo to the root user. Use sudo su - with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (/opt/oracle/dcs/bin).

   login as: opc
   [opc@dbsys ~]$ sudo su -

4. The DB system will include an initial database, but you'll need to create a standby database by using the dbcli create-database command with the --instanceonly parameter. This parameter creates only the database storage structure and starts the database in nomount mode (no other database files are created).

   When using --instanceonly, both the --dbname and --adminpassword parameters are required and they should match the dbname and admin password of the primary database to avoid confusion.

   The following sample command prompts for the admin password and then creates a storage structure for a database named dbname.

   [root@dbsys ~]# dbcli create-database --dbname <same as primary dbname> --databaseUniqueName <different from primary uniquename> --instanceonly --adminpassword

   If you are using pluggable databases, also specify the --cdb parameter.

   For complete command syntax, see Database Commands on page 1505.

5. Wait a few minutes for the dbcli create-database command to create the standby database.

   You can use the dbcli list-jobs command to verify that the creation job ran successfully, and then the dbcli list-databases command verify that the database is configured.

Preparing the Primary DB System

To prepare the primary DB system, you'll need to configure static listeners, update tnsnames.ora, and configure some database settings and parameters.

Configuring the Static Listeners

Create static listeners to be used by RMAN and Data Guard Broker.

1. SSH to the primary DB system, log in as the opc or root user, and sudo to the grid OS user.

   sudo su - grid
2. Edit `/u01/app/<version>/grid/network/admin/listener.ora` and add the following content to it. The first static listener shown here is optional. The second DGMGRL static listener is optional for version 12.1 or later databases, but required for version 11.2 databases.

```sql
SID_LIST_LISTENER=
 (SID_LIST=
  (SID_DESC=
   (GLOBAL_DBNAME = <primary_db_unique_name>,<primary_db_domain>)
   (SID_NAME = <primary_oracle_sid>)
   (ORACLE_HOME=<oracle_home_directory>)
   (ENVS="TNS_ADMIN=<oracle_home_directory>/network/admin")
  )
  (SID_DESC=
   (GLOBAL_DBNAME = <primary_db_unique_name>_DGMGRL,<primary_db_domain>)
   (SID_NAME = <primary_oracle_sid>)
   (ORACLE_HOME=<oracle_home_directory>)
   (ENVS="TNS_ADMIN=<oracle_home_directory>/network/admin")
  )
)
```

3. Save your changes and then restart the listener.

```
$ srvctl stop listener
$ srvctl start listener
```

### Adding Net Service Names to tnsnames.ora

As the oracle user, edit `$ORACLE_HOME/network/admin/tnsnames.ora` and add the standby database net service name to it.

```sql
<standby db_unique_name> =
 (DESCRIPTION =
   (SDU=65535)
   (ADDRESS = (PROTOCOL = TCP)(HOST = <standby_server>.<domain>) (PORT = 1521))
   (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = <standby db_unique_name>.<standby db_domain>)
   )
)
```

The sample above assumes that name resolution is working and that the `<standby_server>.<domain>` is resolvable at the primary database. You can also use the private IP address of the standby server if the IP addresses are routable within a single cloud network (VCN).

### Configuring Primary Database Parameters

**Tip:**

If the primary and standby hosts have different directory structures, you might need to set additional parameters that are not discussed here, such as the `log_file_name_convert` parameter. See the RMAN documentation for more information about how to create standbys for hosts with different directory structures.

1. As the oracle user, enable automatic standby file management.

```
SQL> alter system set standby_file_management=AUTO;
```
2. Identify the Broker configuration file names and locations. The commands used for this depend on the type of database storage. If you're not sure of the database storage type, use the Database Commands on page 1505 command on the DB system.

For ACFS database storage, use the following commands to set the Broker configuration files.

```
SQL> alter system set dg_broker_config_file1='/u02/app/oracle/oradata/<Primary db_unique_name>/dbs/dr1<Primary db_unique_name>.dat';
SQL> alter system set dg_broker_config_file2='/u02/app/oracle/oradata/<Primary db_unique_name>/dbs/dr2<Primary db_unique_name>.dat';
```

For ASM database storage, use the following commands to set the Broker configuration files.

```
SQL> alter system set dg_broker_config_file1='+DATA/<Primary db_unique_name>/dr1<db_unique_name>.dat';
SQL> alter system set dg_broker_config_file2='+DATA/<Primary db_unique_name>/dr2<db_unique_name>.dat';
```

3. Enable Broker DMON process for the database.

```
SQL> alter system set dg_broker_start=true;
```

4. Force database logging for all database transactions.

```
SQL> alter database force logging;
```

5. Add Standby Redo Logs (SRLs), based on the Online Redo Logs (ORLs). On a newly launched DB system, there will be three ORLs of size 1073741824, so create four SRLs of the same size.

You can use the query below to determine the number and size (in bytes) of the ORLs.

```
SQL> select group#, bytes from v$log;
GROUP#    BYTES
--------- ----------
1 1073741824
2 1073741824
```
All of the ORLs must be the same size.

The SRLs must be the same size as the ORLs, but there must be at least one more SRL than the ORLs. In the example above, there are three ORLs, so four SRLs are required. So specify the current redo logs plus one, and use the same size as the redo logs.

```
SQL> alter database add standby logfile thread 1 size <size>;
```

There should be only one member in the SRL group (by default, a DB system is created with only one member per SRL group). To ensure this, you can name the file with the following syntax.

```
alter database add standby logfile thread 1 group 4 (logfile name with full path) size 1073741824, group 5 (logfile name with full path) size 1073741824 ...
```

For ASM/OMF configurations, the above command uses the diskgroup instead of `logfile name with full path`.

```
alter database add standby logfile thread 1 group 4 (+RECO) size 1073741824, group 5 (+RECO) size 1073741824 ...
```

**Tip:**

ORLs and SRLs should be sized so that log switches do not occur more frequently than every 10 minutes. This requires knowledge of the application and may need to be adjusted after deployment. For more information, see Use Standby Redo Logs and Configure Size Appropriately.

6. Verify that you created the correct number of SRLs.

```
SQL> select group#, bytes from v$standby_log;
```

7. Make sure the database is in ARCHIVELOG mode.

```
SQL> archive log list
```

8. Enable database FLASHBACK. The minimum recommended value for db_flashback_retention_target is 120 minutes.

```
SQL> alter database flashback on;
SQL> alter system set db_flashback_retention_target=120;
```

9. Perform a single switch redo log to activate archiving if database is newly created. (At least one log must be archived prior to running the RMAN duplicate.)

```
SQL> alter system switch logfile;
```

**Preparing the Standby Database**

Before you prepare the standby database, make sure the database home on the standby is the same version as on the primary. (If the primary and standby databases are both newly created with the same database version, the database homes will be the same.) If it is not, create a database home that is the same version. You can use the `Dbhome Commands` on page 1518 command to verify the versions and the `Dbhome Commands` on page 1518 command to create a new database home as needed.

To prepare the standby DB system, you'll need to configure static listeners, update tnsnames.ora, configure TDE Wallet, create a temporary password file, verify connectivity, run RMAN DUPLICATE, enable FLASHBACK, and then create the database service.
Configuring the Static Listeners

Create static listeners to be used by RMAN and Data Guard Broker.

1. SSH to the standby DB system, log in as the opc or root user, and sudo to the grid OS user.

   ```
sudo su - grid
   ```

2. Append the following content to /u01/app/<db_version>/grid/network/admin/listener.ora.

   The first static listener shown below is required for RMAN DUPLICATE. The second DGMGRL static listener is optional for database versions 12.2.0.1 and 12.1.0.2, but required for database version 11.2.0.4.

   ```
SID_LIST_LISTENER=
   (SID_LIST=
     (GLOBAL_DBNAME = <standby db_unique_name>.<standby db_domain>)
     (SID_NAME = <standby oracle_sid>)
     (ORACLE_HOME=<oracle home directory>)
     (ENVS="TNS_ADMIN=<oracle home directory>/network/admin")
   )
   (SID_DESC=--
     (GLOBAL_DBNAME = <standby db_unique_name>_DGMGRL.<standby db_domain>)
     (SID_NAME = <standby oracle_sid>)
     (ORACLE_HOME=<oracle home directory>)
     (ENVS="TNS_ADMIN=<oracle home directory>/network/admin")
   )
   )
   ```

3. Restart the listener.

   ```
$ srvctl stop listener
$ srvctl start listener
   ```

4. Verify that the static listeners are available. The sample output below is for database version 12.1.0.2. Note that the ...status UNKNOWN messages are expected at this point.

   ```
$ lsnrctl status
LSNRCTL for Linux: Version 12.1.0.2.0 - Production on 29-SEP-2016 21:09:25
Copyright (c) 1991, 2014, Oracle. All rights reserved.
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=LISTENER)))
STATUS of the LISTENER
--------------------------
Alias LISTENER
Version TNSLSNR for Linux: Version 12.1.0.2.0 -
Production
Start Date 29-SEP-2016 21:09:19
Uptime 0 days 0 hr. 0 min. 5 sec
Trace Level off
Security ON: Local OS Authentication
SNMP OFF
Listener Parameter File /u01/app/12.1.0.2/grid/network/admin/listener.ora
Listener Log File /u01/app/grid/diag/tns1snr/dg2/listener/alert/log.xml
Listening Endpoints Summary...
   (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=LISTENER)))
   (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=10.0.1.24)(PORT=1521)))
Services Summary...
   ```
Adding Net Service Names to tnsnames.ora

As the oracle user, add the standby database net service name to $ORACLE_HOME/network/admin/tnsnames.ora. $ORACLE_HOME is the database home where the standby database is running.

```xml
<Primary db_unique_name> =
  (DESCRIPTION =
    (SDU=65535)
    (ADDRESS = (PROTOCOL = TCP)(HOST = <primary_server>.<domain>) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = <primary db_unique_name>.<primary db_domain>)
    )
  )

<Standby db_unique_name> =
  (DESCRIPTION =
    (SDU=65535)
    (ADDRESS = (PROTOCOL = TCP)(HOST = <standby_server>.<domain>) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = <standby db_unique_name>.<db_domain>)
    )
  )
```

Copying the TDE Wallets to the Standby System

Copy the TDE wallet files from the primary DB system to standby DB system using SCP. The following sample command assumes the SCP command is being run by the oracle OS user and that the private key for oracle has been created and exists on the host where SCP is being run.

```bash
$ scp -i <private key> primary_server:/opt/oracle/dcs/commonstore/wallets/tde/<primary db_unique_name>/* standby_server:/opt/oracle/dcs/commonstore/wallets/tde/<standby db_unique_name>
```

Setting Up the Standby System Configuration

As the oracle user, create the following directory for database version 11.2.0.4. This step is optional for version 12.2.0.1 and version 12.1.0.2.

```bash
[oracle@dbsys ~]$ mkdir -pv /u03/app/oracle/redo/<standby db_unique_name>uppercase)/controlfile
```

Creating the Audit File Destination

As the oracle user, create the following directory to use as the audit file destination.

```bash
[oracle@dbsys ~]$ mkdir -p /u01/app/oracle/admin/<db_name>/adump
```

Otherwise, the RMAN duplicate command used later will fail.
Creating a Temporary Password File

As the oracle user, create a temporary password file.

```bash
[oracle@dbsys ~]$ orapwd file=$ORACLE_HOME/dbs/orapw<standby oracle_sid>
password=<admin password for primary> entries=5
```

The password **must** be the same as the admin password of the primary database. Otherwise, the RMAN duplicate step below will fail with: RMAN-05614: Passwords for target and auxiliary connections must be the same when using active duplicate.

Verifying the Standby Database is Available

1. As the oracle user, set the environment variables.

   ```bash
   [oracle@dbsys ~]$ . oraenv
   <enter the db_name>
   ```

2. Replace `$ORACLE_HOME/dbs/init<standby sid_name>.ora` with the following content:

   ```
   db_name=<Primary db_name>
   db_unique_name=<standby db_unique_name>
   db_domain=<standby db_domain>
   ```

3. Remove the spfile from the standby.

   ```bash
   /u02/app/oracle/oradata/<standby db_unique_name>/dbs/spfile
   $ORACLE_SID.ora
   ```

   The database needs to be started in nomount mode with no spfile specified, but the original init file contains an spfile parameter which will prevent the RMAN duplicate step from working.

4. Set the `ORACLE_UNQNAME` environment variable to point to your `DB_UNIQUE_NAME`.

   ```bash
   $ export ORACLE_UNQNAME =db_unique_name
   ```

   **Important:**
   If you do not perform this step, the wallet will not be opened, and running the RMAN DUPLICATE command in the subsequent step will fail.

5. The `dbcli create-database --instanceonly` command used earlier opens the standby database as a primary in read/write mode, so the database needs to be brought down before proceeding to the nomount step below.

   ```bash
   $ sqlplus / as sysdba
   SQL> shutdown immediate
   ```

6. Start the database in nomount mode.

   ```bash
   SQL> startup nomount
   ```

Verifying the Database Connections

Verify the connection between the primary and standby databases.

1. Make sure that the listener port 1521 is open in the security list(s) used for the primary and standby DB systems. For more information, see [Updating the Security List for the DB System](#) on page 1434.
2. From the primary database, connect to standby database.

   $ sqlplus sys/<password>@<standby net service name> as sysdba

3. From standby database, connect to primary database.

   $ sqlplus sys/<password>@<primary net service name> as sysdba

**Running the RMAN DUPLICATE Command**

Run the RMAN DUPLICATE command on the standby DB system, as the oracle user.

If the primary database is large, you can allocate additional channels to improve performance. For a newly installed database, one channel typically runs the database duplication in a couple of minutes.

Make sure that there are no errors generated by the RMAN DUPLICATE command. If errors occur, restart the database using the init.ora file (not spfile) in case it is generated under $ORACLE_HOME/dbs as part of RMAN DUPLICATE.

In the following examples, use lowercase for the `<Standby db_unique_name>` unless otherwise specified.

For ACFS storage layout, run the following commands.

```
$ rman target sys/<password>@<primary alias> auxiliary
sys/<password>@<standby alias> log=rman.out
RMAN> run { allocate channel prim1 type disk;
 allocate auxiliary channel sby type disk;
duplicate target database for standby from active database
dorecover
spfile
 parameter_value_convert '/<Primary db_unique_name>','/<Standby
db_unique_name>','<Primary db_unique_name uppercase>','/<Standby
db_unique_name uppercase>'
 set db_unique_name='<Standby db_unique_name>'
 set db_create_file_dest='/u02/app/oracle/oradata/<Standby
db_unique_name>'
 set dg_broker_config_file1='/u02/app/oracle/oradata/<Standby
db_unique_name>/dr1/<Standby db_unique_name>.dat'
 set dg_broker_config_file2='/u02/app/oracle/oradata/<Standby
db_unique_name>/dr2/<Standby db_unique_name>.dat'
 set dispatchers ='(PROTOCOL=TCP) (SERVICE=<Standby
db_unique_name>XDB)'
 set instance_name='<Standby db_unique_name>'
}
```

For ASM storage layout, run the following commands.

```
$ rman target sys/<password>@<primary alias> auxiliary
sys/<password>@<standby alias> log=rman.out
RMAN> run { allocate channel prim1 type disk;
 allocate auxiliary channel sby type disk;
duplicate target database for standby from active database
dorecover
spfile
 parameter_value_convert '/<Primary db_unique_name>','/<Standby
db_unique_name>','<Primary db_unique_name uppercase>','/<Standby
db_unique_name uppercase>'
 set db_unique_name='<Standby db_unique_name>'
 set dg_broker_config_file1='+DATA/<Standby db_unique_name>/dr1/<Standby
db_unique_name>.dat'
```
Enabling Database FLASHBACK

1. As a Data Guard best practice, enable flashback and set `db_flashback_retention_target` to at least 120 minutes on both the primary and standby databases.

   ```sql
   SQL> alter database flashback on;
   SQL> alter system set db_flashback_retention_target=120;
   ```

2. Verify that the standby database is created properly.

   ```sql
   SQL> select FORCE_LOGGING, FLASHBACK_ON, OPEN_MODE, DATABASE_ROLE, SWITCHOVER_STATUS, DATAGUARD_BROKER, PROTECTION_MODE from v$database ;
   ```

Creating a Database Service

Oracle recommends creating a database service for the standby database by using `srvctl`.

For ACFS storage layout.

1. Create a shared directory and copy the spfile file to it.

   ```sh
   $ mkdir -pv /u02/app/oracle/oradata/<Standby db_unique_name>/dbs
   $ cp $ORACLE_HOME/dbs/spfile<standby oracle_sid>.ora /u02/app/oracle/oradata/<Standby db_unique_name>/dbs
   ```

2. Stop and remove the existing database service.

   ```sh
   $ srvctl stop database -d <standby db_unique_name>
   $ srvctl remove database -d <standby db_unique_name>
   ```

3. Create the database service.

   ```sh
   $ srvctl add database -d <standby db_unique_name> -n <standby db_name> -o $ORACLE_HOME -c SINGLE -p '/u02/app/oracle/oradata/<Standby db_unique_name>/dbs/spfile<standby db_name>.ora' -x <standby hostname> -s "READ ONLY" -r PHYSICAL_STANDBY -i <db_name>
   $ srvctl setenv database -d <standby db_unique_name> -t "ORACLE_UNQNAME=<standby db_unique_name>"
   $ srvctl config database -d <standby db_unique_name>
   ```

4. Start the database service.

   ```sh
   $ srvctl start database -d <standby db_unique_name>
   ```

5. Clean up the files from $ORACLE_HOME/dbs.

   ```sh
   $ rm $ORACLE_HOME/dbs/spfile<standby oracle_sid>.ora
   $ rm $ORACLE_HOME/dbs/init<standby oracle_sid>.ora
   ```
6. Create the $ORACLE_HOME/dbs/init<standby oracle_sid>.ora file to reference the new location of the spfile file.

   SPFILE='/u02/app/oracle/oradata/<standby db_unique_name>/dbs/spfile<standby db_name>.ora'

7. Stop the standby database and then start it by using srvctl.

   srvctl stop database -d <standby db_unique_name>
srvctl start database -d <standby db_unique_name>

For ASM storage layout.

1. Consider generating the spfile file under +DATA.

   SQL> create pfile='init<standby oracle_sid>.ora' from spfile ;
   SQL> create spfile='+DATA' from pfile='init<standby oracle_sid>.ora' ;

2. Stop and remove the existing database service.

   $ srvctl stop database -d <standby db_unique_name>
   $ srvctl remove database -d <standby db_unique_name>

3. Create the database service.

   $ srvctl add database -d <standby db_unique_name> -n <standby db_name>
   -o $ORACLE_HOME -c SINGLE -p '+DATA/<standby db_unique_name>/PARAMETERFILE/spfile.xxx.xxxxxx'
   -x <standby hostname> -s "READ ONLY" -r PHYSICAL_STANDBY -i <db_name>
   $ srvctl setenv database -d <standby db_unique_name> -t "ORACLE_UNQNAME=<standby db_unique_name>"
   $ srvctl config database -d <standby db_unique_name>

4. Start the database service.

   $ srvctl start database -d <standby db_unique_name>

5. Clean up the files from $ORACLE_HOME/dbs.

   $ rm $ORACLE_HOME/dbs/init<standby oracle_sid>.ora
   $ rm $ORACLE_HOME/dbs/spfile<standby oracle_sid>.ora

6. Create $ORACLE_HOME/dbs/init<standby oracle_sid>.ora file to reference the new location of the spfile file.

   SPFILE='+DATA/<standby db_unique_name>/PARAMETERFILE/spfile.xxx.xxxxxx'

7. Stop the database and start the standby database by using srvctl.

   $ srvctl start database -d <standby db_unique_name>

Configuring Data Guard

Perform the following steps to complete the configuration of Data Guard and enable redo transport from the primary database and redo apply in the standby database.
1. Run the dgmgrl command line utility from either the primary or standby DB system and connect to the primary database using sys credentials.

   DGMGRL> connect sys/<sys password>@<primary tns alias>

2. Create the Data Guard configuration and identify for the primary and standby databases.

   DGMGRL> create configuration mystby as primary database is <primary db_unique_name>
   connect identifier is <primary tns alias>
   add database <standby db_unique_name> as connect identifier is <standby tns alias> maintained as physical;

3. Enable Data Guard configuration.

   DGMGRL> enable configuration;

4. Verify that Data Guard setup was done properly. Run the following SQL in both the primary and standby databases.

   SQL> select FORCE_LOGGING, FLASHBACK_ON, OPEN_MODE, DATABASE_ROLE,
   SWITCHOVER_STATUS, DATAGUARD_BROKER, PROTECTION_MODE from v$database;

5. Verify that Data Guard processes are initiated in the standby database.

   SQL> select PROCESS,PID,DELAY_MINS from V$MANAGED_STANDBY;

6. Verify parameter configuration on primary and standby.

   SQL> show parameter log_archive_dest_
   SQL> show parameter log_archive_config
   SQL> show parameter fal_server
   SQL> show parameter log_archive_format

7. Verify that the Data Guard configuration is working. Specifically, make sure redo shipping and redo apply are working and that the standby is not unreasonably lagging behind the primary.

   DGMGRL> show configuration verbose
   DGMGRL> show database verbose <standby db_unique_name>
   DGMGRL> show database verbose <primary db_unique_name>

   Any discrepancies, errors, or warnings should be resolved. You can also run a transaction on the primary and verify that it's visible in the standby.

8. Verify that the Data Guard configuration is functioning as expected by performing switchover and failover in both directions. Run show configuration after each operation and make sure there are no errors or warnings.

   Caution:

   This step is optional, based on your discretion. If for any reason the configuration is not valid, the switchover and/or failover will fail and it might be difficult or impossible to start the primary database. A recovery of the primary might be required, which will affect availability.

   DGMGRL> switchover to <standby db_unique_name>
   DGMGRL> switchover to <primary db_unique_name>
   #connect to standby before failover:

   DGMGRL> connect sys/<sys password>@<standby db_unique_name>
   DGMGRL> failover to <standby db_unique_name>
   DGMGRL> reinstate database <primary db_unique_name>
   #connect to primary before failover:
Configuring Observer (Optional)

The best practice for high availability and durability is to run the primary, standby, and observer in separate availability domains. The observer determines whether or not to failover to a specific target standby database. The server used for observer requires the Oracle Client Administrator software, which includes the Oracle SQL NET and Broker.

1. Configure TNS alias names for both the primary and standby databases as described previously, and verify the connection to both databases.

2. Change protection mode to either maxavailability or maxperformance (maxprotection is not supported for FSFO).

   To enable maxavailability:

   ```
   DGMGRL> edit database <standby db_unique_name> set property 'logXptMode'='SYNC';
   DGMGRL> edit database <primary db_unique_name> set property 'logXptMode'='SYNC';
   DGMGRL> edit configuration set protection mode as maxavailability;
   ```

   To enable maxperformance:

   ```
   DGMGRL> edit configuration set protection mode as maxperformance;
   DGMGRL> edit database <standby db_unique_name> set property 'logXptMode'='ASYNC';
   DGMGRL> edit database <primary db_unique_name> set property 'logXptMode'='ASYNC';
   ```

   For maxperformance, the FastStartFailoverLaglimit property limits the maximum amount of permitted data loss to 30 seconds by default.

3. The following properties should also be considered. Run `show configuration verbose` to see their current values.

   - FastStartFailoverPmyShutdown
   - FastStartFailoverThreshold
   - FastStartFailoverTarget
   - FastStartFailoverAutoReinstate

   (Running `show configuration` will result in the following error until the observer is started: Warning : ORA-16819: fast-start failover observer not started.)

4. Enable fast-start failover from Broker:

   ```
   DGMGRL> Enable fast_start failover
   ```

5. Verify the fast-start failover and associated settings.

   ```
   DGMGRL> show fast_start failover
   ```

6. Start the observer from Broker (it will run in the foreground, but can also be run in the background).

   ```
   DGMGRL> start observer
   ```

7. Verify fast-start failover is enabled and without errors or warnings.

   ```
   DGMGRL> show configuration verbose
   ```
8. Always test failover in both directions to ensure that everything is working as expected. Verify that FSFO is running properly by performing a shutdown abort of the primary database.

The observer should start the failover to the standby database. If protection mode is set to maxprotection, some loss of data can occur, based on the FastStartFailoverLaglimit value.

**Oracle Database CLI Reference**

The database CLI (dbcli) is a command line interface available on bare metal and virtual machine DB systems. After you connect to the DB system, you can use the database CLI to perform tasks such as creating Oracle database homes and databases.

**Note:**
The database CLI is **not** for use on Exadata DB systems.

**Operational Notes**

- The database CLI commands must be run as the root user.
- `dbcli` is in the `/opt/oracle/dcs/bin/` directory.
  This directory is included in the path for the root user's environment.
- Oracle Database maintains logs of the `dbcli` command output in the `dcscli.log` and `dcs-agent.log` files in the `/opt/oracle/dcs/log/` directory.
- The database CLI commands and most parameters are case sensitive and should be typed as shown. A few parameters are not case sensitive, as indicated in the parameter descriptions, and can be typed in uppercase or lowercase.

**Caution:**
Oracle recommends that you avoid specifying parameter values that include confidential information when you use the database CLI commands.

**Syntax**
The database CLI commands use the following syntax:

```
 dbcli command [parameters]
```

where:

- **command** is a verb-object combination such as `create-database`.
- **parameters** include additional options for the command. Most parameter names are preceded with two dashes, for example, `--help`. Abbreviated parameter names are preceded with one dash, for example, `-h`.
- User-specified parameter values are shown in red text within angle brackets, for example, `<db_home_id>`. Omit the angle brackets when specifying these values.
- The help parameter is available with every command.

The remainder of this topic contains syntax and other details about the commands.

**CLI Update Command**
Occasionally, new commands are added to the database CLI and other commands are updated to support new features. You can use the following command to update the database CLI:

```
 cliadm update-dbcli
```

Use the `cliadm update-dbcli` command to update the database CLI with the latest new and updated commands.
On RAC DB systems, execute the `cliadm update-dbcli` command on each node in the cluster.

**Syntax**

```
cliadm update-dbcli [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command updates the `dbcli`:

```
[root@dbsys ~]# cliadm update-dbcli
{
    "jobId": "dc9ce73d-ed71-4473-99cd-9663b9d79b7d",
    "status": "Created",
    "message": "Dcs cli will be updated",
    "reports": [],
    "createTimestamp": "January 18, 2017 10:19:34 AM PST",
    "resourceList": [],
    "description": "dbcli patching",
    "updatedTime": "January 18, 2017 10:19:34 AM PST"
}
```

**Agent Commands**

The following commands are available to manage agents:

- `dbcli ping-agent`
- `dbcli list-agentConfigParameters`
- `dbcli update-agentConfigParameters`

**dbcli ping-agent**

Use the `dbcli ping-agent` command to test the reachability of an agent.

**Syntax**

```
dbcli ping-agent [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
**dbcli list-agentConfigParameters**

Use the `dbcli list-agentConfigParameters` command to list agent configuration parameters.

**Syntax**

```
dbcli list-agentConfigParameters [-n] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>-name</td>
<td>(Optional) Parameter name.</td>
</tr>
</tbody>
</table>

**dbcli update-agentConfigParameters**

Use the `dbcli update-agentConfigParameters` command to update agent configuration parameters.

**Syntax**

```
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>--append</td>
<td>(Optional) Appends the specified values to the specified parameters. Example with multiple parameter names and values: <code>-n p1 -v v1 -n p2 -v v2 -a</code></td>
</tr>
<tr>
<td>-c</td>
<td>--comment</td>
<td>(Optional) Adds a comment for the parameter. Default: []</td>
</tr>
<tr>
<td>-d</td>
<td>--description</td>
<td>(Optional) Adds a description for the parameter. Default: []</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--name</td>
<td>Parameter name. Example with multiple parameter names and values: <code>-n p1 -v v1 -n p2 -v v2 Default: []</code></td>
</tr>
<tr>
<td>-r</td>
<td>--reset</td>
<td>(Optional) Resets the parameter to the default value. Example resetting multiple parameters: <code>-n p1 -n p2 -r Default: false</code></td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-u</td>
<td>--update</td>
<td>(Optional) Replaces the specified parameter values as directed. Example with multiple parameter names and values: <code>-n p1 -v v1 -n p2 -v v2 -u</code> Default: false</td>
</tr>
<tr>
<td>-v</td>
<td>--value</td>
<td>(Optional) Parameter value. Example with multiple parameter names and values: <code>-n p1 -v v1 -n p2 -v v2</code> Default: []</td>
</tr>
</tbody>
</table>

**Autologcleanpolicy Commands**

The following commands are available to manage policies for automatic cleaning (purging) of logs.

- `dbcli create-autoLogCleanPolicy`
- `dbcli list-autoLogCleanPolicy`

**dbcli create-autoLogCleanPolicy**

Use the `dbcli create-autoLogCleanPolicy` command to create policies for automatic cleaning (purging) of logs.

**Syntax**

```
dbcli create-autoLogCleanPolicy [-c {gi|database|dcs}] [-f <number>] [-o <number>] [-u {Day|Hour|Minute}] [-uMB <number>] [-uPer <number>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--components</td>
<td>(Optional) Components to purge. Possible values are gi, database, and dcs. Separate multiple values with commas. Example: <code>gi,dcs</code></td>
</tr>
<tr>
<td>-f</td>
<td>--freeSpaceBelowPercentage</td>
<td>(Optional) Purges logs when the free disk space is below the specified percentage of the total partition size. Valid range: 20-50. Default: 20.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-o</td>
<td>--olderthan</td>
<td>(Optional) Quantity portion of time interval. Default: 30. Cleans logs older than the specified time interval (<code>-o</code> and <code>-u</code>).</td>
</tr>
</tbody>
</table>
### Parameter List

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>--olderThanUnit</td>
<td>(Optional) Unit portion of time interval. Possible values: Day, Hour, or Minute. Default: Day. Cleans logs older than the specified time interval (-o and -u).</td>
</tr>
<tr>
<td>-uMB</td>
<td>--usageOverMB</td>
<td>(Optional) Purges logs when log usage exceeds the specified number of MegaBytes (MB). Valid range: 10 to 50% of total partition size.</td>
</tr>
<tr>
<td>-uPer</td>
<td>--usageOverPercentage</td>
<td>(Optional) Purges logs when log usage exceeds the specified percentage of the total partition size. Valid range: 10-50.</td>
</tr>
</tbody>
</table>

#### dbcli list-autoLogCleanPolicy

Use the `dbcli list-autoLogCleanPolicy` command to list policies for automatic cleaning of logs.

**Syntax**

```
  dbcli list-autoLogCleanPolicy [-c {gi|database|dcs}] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--components</td>
<td>(Optional) Components. Possible values are gi, database, and dcs. Separate multiple values with commas. Example: gi,dcs</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

#### Backup Commands

The following commands are available to back up databases:

- `dbcli create-backup`
- `dbcli getstatus-backup`
- `dbcli schedule-backup`

**Note:**

Instead of using `dbcli`, you can use the Console or the API to manage backing up your bare metal or virtual machine DB system databases to Object Storage. However, if you switch from using `dbcli` to using managed backups, a new backup configuration is created and associated with your database, and backups you created by using `dbcli` will not be accessible from the managed backup interfaces. For information about managed backups, see [Backing Up a Database to Oracle Cloud Infrastructure Object Storage](#) on page 1435.
Before you can back up a database by using the `dbcli create-backup` command, you'll need to:

1. Create a backup configuration by using the `dbcli create-backupconfig` command.
2. Associate the backup configuration with the database by using the `dbcli update-database` command.

After a database is associated with a backup configuration, you can use the `dbcli create-backup` command in a cron job to run backups automatically. You can use a cron utility such as CronMaker to help build expressions. For more information, see [http://www.cronmaker.com](http://www.cronmaker.com).

**dbcli create-backup**

Use the `dbcli create-backup` command to create a backup of a database.

**Syntax**

```
    dbcli create-backup -in <db_name> -i <db_id> [-bt {Regular-L0|Regular-L1|Longterm|ArchiveLog}] [-c {Database|TdeWallet}] [-k <n>] [-t <tag>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-bt</td>
<td>--backupType</td>
<td>(Optional) Backup type. Possible values are Regular-L0, Regular-L1, Longterm, and ArchiveLog. Regular-L0 and Regular L1 correspond to incremental L0 and L1 backups. Longterm corresponds to Full backup. ArchiveLog corresponds to archived redo logs backup. The default value is Regular-L1. Values are not case-sensitive. If omitted, the default value is used.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-c</td>
<td>--component</td>
<td>(Optional) Component. Possible values are Database and TdeWallet. The default value is Database. The value TdeWallet backs up TDE wallets. Values are not case-sensitive. If omitted, the default value is used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TDE wallets are automatically backed up in the following situations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A database is created with an Object Storage backup configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A database that has an Object Storage backup configuration is updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An Object Storage backup configuration is updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A backup of the type Longterm is created.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The TDE key for a database is rotated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A database is backed up and no TDE wallet backups exist yet.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>The ID of the database to back up. Use the <code>dbcli list-databases</code> command to get the database's ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>The name of the database to back up. Use the <code>dbcli list-databases</code> command to get the database's name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
### Examples

The following command creates a backup of the specified database using the database ID.

```
[root@dbsys ~]# dbcli create-backup -i 573cadb2-0cc2-4c1c-9c31-595ab8963d5b
```

The following command creates a backup of the specified database using the database name ("mydb").

```
[root@dbsys ~]# dbcli create-backup -in mydb
```

**dbcli getstatus-backup**

Use the `dbcli getstatus-backup` command to display the status of a backup.

**Syntax**

```
dbcli getstatus-backup -t <backup_type> [i <id>] [-in <name>] [-l] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbId</td>
<td>(Optional) Database Resource ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>(Optional) Database Resource Name.</td>
</tr>
</tbody>
</table>
Use the `dbcli schedule-backup` command to schedule a backup of a database.

### Syntax

```
dbcli schedule-backup -t <backup_type> -f <number> [i <id>] [-in <name>] [-h] [-j]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>--frequency</td>
<td>Frequency in minutes.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbId</td>
<td>(Optional) Database Resource ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>(Optional) Database Resource Name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-t</td>
<td>--backupType</td>
<td>Backup type.</td>
</tr>
</tbody>
</table>

### Backupconfig Commands

A backup configuration determines the backup destination and recovery window for database backups. You create the backup configuration and then associate it with a database by using the `dbcli update-database` command.

#### Caution:
Backups that were configured using the Console may become unusable if you make changes using these commands. For backups configured using the Console, use these commands with support guidance only.

#### Note:
Instead of using `dbcli`, you can use the Console or the API to manage backing up your bare metal or virtual machine DB system databases to Object Storage. For information about managed backups, see Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435.

After a database is associated with a backup configuration, you can use the `dbcli create-backup` command in a cron job to run backups automatically. You can use a cron utility such as CronMaker to help build expressions. For more information, see [http://www.cronmaker.com](http://www.cronmaker.com).

The following commands are available to manage backup configurations:

- `dbcli create-backupconfig`
- `dbcli list-backupconfigs`
- `dbcli describe-backupconfig`
- dbcli update-backupconfig
- dbcli delete-backupconfig

**dbcli create-backupconfig**

Use the `dbcli create-backupconfig` command to create a backup configuration that defines the backup destination and recovery windows.

**Syntax**

```bash
dbcli create-backupconfig -d {DISK|OBJECTSTORE|NONE} -c <bucket> -o <object_store_swift_id> -on <object_store_swift_name> -w <n> -n <name> [-cr|-no-cr] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--container</td>
<td>The name of an existing bucket in the Oracle Cloud Infrastructure Object Storage service. You can use the Console or the Object Storage API to create the bucket. For more information, see Managing Buckets on page 3398. You must also specify --backupdestination objectstore and the --objectstoreswiftId parameter.</td>
</tr>
<tr>
<td>-cr</td>
<td>--crosscheck</td>
<td>(Optional) Indicates whether to enable the crosscheck operation. This operation determines if the files on the disk or in the media management catalog correspond to data in the RMAN repository. If omitted, the default setting is used (crosscheck is enabled by default).</td>
</tr>
<tr>
<td>-no-cr</td>
<td>--no-crosscheck</td>
<td></td>
</tr>
<tr>
<td>-d</td>
<td>--backupdestination</td>
<td>The backup destination as one of the following (these values are <strong>not</strong> case sensitive): DISK - The local Fast Recovery Area. OBJECTSTORE - The Oracle Cloud Infrastructure Object Storage service. You must also specify the --container and --objectstoreswiftId parameters. NONE - Disables the backup.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--name</td>
<td>The name of the backup configuration.</td>
</tr>
<tr>
<td>-o</td>
<td>--objectstoreswiftId</td>
<td>The ID of the object store that contains the endpoint and credentials for the Oracle Cloud Infrastructure Object Storage service. Use the <code>dbcli list-objectstoreswifts</code> command to get the object store ID. Use the <code>dbcli create-objectstoreswift</code> command to create an object store. You must also specify <code>--backupdestination objectstore</code> and the <code>--container</code> parameter.</td>
</tr>
<tr>
<td>-on</td>
<td>--objectstoreswiftName</td>
<td>The name of the object store that contains the endpoint and credentials for the Oracle Cloud Infrastructure Object Storage service. Use the <code>dbcli list-objectstoreswifts</code> command to get the object store ID. Use the <code>dbcli create-objectstoreswift</code> command to create an object store. You must also specify <code>--backupdestination objectstore</code> and the <code>--container</code> parameter.</td>
</tr>
<tr>
<td>-w</td>
<td>--recoverywindow</td>
<td>The number of days for which backups and archived redo logs are maintained. The interval always ends with the current time and extends back in time for the number of days specified. For a DISK backup destination, specify 1 to 14 days. For an OBJECTSTORE backup destination, specify 1 to 30 days.</td>
</tr>
</tbody>
</table>
Example

The following command creates a backup configuration named dbbkcfg1:

```
[root@dbsys ~]# dbcli create-backupconfig -d Disk -w 7 -n dbbkcfg1
{
   "jobId" : "4e0e6011-db53-4142-82ef-eb561658a0a9",
   "status" : "Success",
   "message" : null,
   "reports" : [ {
      "taskId" : "TaskParallel_919",
      "taskName" : "persisting backup config metadata",
      "taskResult" : "Success",
      "startTime" : "November 18, 2016 20:21:25 PM UTC",
      "endTime" : "November 18, 2016 20:21:25 PM UTC",
      "status" : "Success",
      "taskDescription" : null,
      "parentTaskId" : "TaskSequential_915",
      "jobId" : "4e0e6011-db53-4142-82ef-eb561658a0a9",
      "tags" : [ ],
      "reportLevel" : "Info",
      "updatedTime" : "November 18, 2016 20:21:25 PM UTC"
   } ],
   "createTimestamp" : "November 18, 2016 20:21:25 PM UTC",
   "description" : "create backup config:dbbkcfg1",
   "updatedTime" : "November 18, 2016 20:21:25 PM UTC"
}
```

dbcli list-backupconfigs

Use the `dbcli list-backupconfigs` command to list all the backup configurations in the DB system.

Syntax

```
dbcli list-backupconfigs [-h] [-j]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

Example

The following command lists a backup configuration:

```
[root@dbsys ~]# dbcli list-backupconfigs

ID                                       Name                 RecoveryWindow
---------------------------------------- -------------------- -----------------------------
------------------ ----------------- -----------------------------
ccdd56fe-a40b-4e82-b38d-5f76c265282d     dbbkcfg1             7
Disk              July 10, 2016 12:24:08 PM UTC
```


**dbcli describe-backupconfig**

Use the `dbcli describe-backupconfig` command to show details about a specific backup configuration.

**Syntax**

```
dbcli describe-backupconfig -i <id> -in <name> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--backupconfigid</td>
<td>The backup configuration ID. Use the <code>dbcli list-backupconfigs</code> command to get the ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--backupconfigname</td>
<td>The backup configuration name. Use the <code>dbcli list-backupconfigs</code> command to get the name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays details about a backup configuration:

```
[root@dbsys ~]# dbcli describe-backupconfig -i ccdd56fe-a40b-4e82-b38d-5f76c265282d
Backup Config details
------------------------------------------
   ID: ccdd56fe-a40b-4e82-b38d-5f76c265282d
   Name: dbbkcfg1
   RecoveryWindow: 7
   BackupDestination: Disk
   CreatedTime: July 10, 2016 12:24:08 PM UTC
   UpdatedTime: July 10, 2016 12:24:08 PM UTC
```

**dbcli update-backupconfig**

Use the `dbcli update-backupconfig` command to update an existing backup configuration.

**Syntax**

```
dbcli update-backupconfig -i <id> -in <name> -w <n>
```

- `d {DISK|OBJECTSTORE|NONE}`
- `c <bucket> -o <object_store swift_id> -on <object_store swift_name> [-cr|no-cr] [-h] [-j]`
## Database Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--container</td>
<td>The name of an existing bucket in the Oracle Cloud Infrastructure Object Storage service. You can use the Console or the Object Storage API to create the bucket. For more information, see Managing Buckets on page 3398. You must also specify --backupdestination objectstore and the --objectstoreswiftId parameter.</td>
</tr>
<tr>
<td>-cr</td>
<td>--crosscheck</td>
<td>(Optional) Indicates whether to enable the crosscheck operation. This operation determines if the files on the disk on in the media management catalog correspond to data in the RMAN repository. If omitted, the default setting is used (crosscheck is enabled by default).</td>
</tr>
<tr>
<td>-no-cr</td>
<td>--no-crosscheck</td>
<td></td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--backupconfigid</td>
<td>The ID of the backup configuration to update. Use the dbcli list-backupconfigs command to get the ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--backupconfigname</td>
<td>The name of the backup configuration to update. Use the dbcli list-backupconfigs command to get the name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-o</td>
<td>--objectstoreswiftId</td>
<td>The ID of the object store that contains the endpoint and credentials for the Oracle Cloud Infrastructure Object Storage service. Use the dbcli list-objectstoreswifts command to get the object store ID. Use the dbcli create-objectstoreswift command to create an object store. You must also specify --backupdestination objectstore and the --container parameter.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-on</td>
<td>--objectstoreswiftname</td>
<td>The name of the object store that contains the endpoint and credentials for the Oracle Cloud Infrastructure Object Storage service. Use the <code>dbcli list-objectstoreswifts</code> command to get the object store ID. Use the <code>dbcli create-objectstoreswift</code> command to create an object store. You must also specify <code>--backupdestination objectstore</code> and the <code>--container</code> parameter.</td>
</tr>
<tr>
<td>-w</td>
<td>--recoverywindow</td>
<td>The new disk recovery window. For a DISK backup destination, specify 1 to 14 days. For an OBJECTSTORE backup destination, specify 1 to 30 days.</td>
</tr>
</tbody>
</table>

**Example**

The following command updates the recovery window for a backup configuration:

```
[root@dbsys ~]# dbcli update-backupconfig -i ccdd56fe-a40b-4e82-b38d-5f76c265282d -w 5
{
    "jobId" : "0e849291-e1e1-4c7a-8dd2-62b522b9b807",
    "status" : "Created",
    "message" : null,
    "reports" : [ ],
    "createTimestamp" : 1468153731699,
    "description" : "update backup config: dbbkcfg1",
    "updatedTime" : 1468153731700
}
```

**dbcli delete-backupconfig**

Use the `dbcli delete-backupconfig` command to delete a backup configuration.

**Syntax**

```
dbcli delete-backupconfig -i <id> -in <name> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>
### Parameter | Full Name | Description
--- | --- | ---
-i | --id | The backup configuration ID to delete. Use the `dbcli list-backupconfigs` command to get the ID.
-in | --backupconfigname | The name of the backup configuration to delete. Use the `dbcli list-backupconfigs` command to get the name.
-j | --json | (Optional) Displays JSON output.

### Example
The following command deletes the specified backup configuration:

```
[root@dbsys ~]# dbcli delete-backupconfig -i ccdd56fe-a40b-4e82-b38d-5f76c265282d
```

### Bmccredential Commands
The following commands are available to manage credentials configurations, which are required for downloading DB system patches from the Oracle Cloud Infrastructure Object Storage service. For more information, see Patching a DB System on page 1407.

- `dbcli create-bmccredential`
- `dbcli list-bmccredentials`
- `dbcli describe-bmccredential`
- `dbcli delete-bmccredential`
- `dbcli update-bmccredential`

### Note:
The `bmccredential` commands are not available on 2-node RAC DB systems.

### dbcli create-bmccredential
Use the `dbcli create-bmccredential` command to create a credentials configuration.

### Prerequisites
Before you can create a credentials configuration, you'll need these items:

- An RSA key pair in **PEM format** (minimum 2048 bits). See How to Generate an API Signing Key on page 4180.
- The fingerprint of the public key. See How to Get the Key's Fingerprint on page 4183.
- Your tenancy's **OCID** and user name's OCID. See Where to Get the Tenancy's OCID and User's OCID on page 4184.

Then you'll need to upload the public key in the Console. See How to Upload the Public Key on page 4184.

### Syntax
```
dbcli create-bmccredential -c [backup|patching|other] -t <tenant_ocid> -u <user_ocid> -f <fingerprint> -k <private_key_path> -p|-hp <passphrase> [-n <credentials_name>] [-e <object_store_url>] [-h] [-j]
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--credentialsType</td>
<td>The type of Object Storage credentials configuration to create (these values are <strong>not</strong> case sensitive):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BACKUP - Reserved for the future use.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PATCHING - For downloading patches from the service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OTHER - Reserved for the future use.</td>
</tr>
<tr>
<td>-e</td>
<td>--objectStoreUrl</td>
<td>(Optional) The Object Storage endpoint URL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Omit this parameter when --credentialsType PATCHING is specified. The following URL is assumed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://objectstorage">https://objectstorage</a>.&lt;region_name&gt;.oraclecloud.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See <a href="https://docs.oracle.com/en-us/iaas/Content/Home.htm">Regions and Availability Domains</a> for region name strings.</td>
</tr>
<tr>
<td>-f</td>
<td>--fingerPrint</td>
<td>The public key fingerprint. You can find the fingerprint in the Console by clicking your user name in the upper right corner and then clicking User Settings. The fingerprint looks something like this:</td>
</tr>
<tr>
<td>-k</td>
<td>--privateKey</td>
<td>The path to the private key file in PEM format, for example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-k /root/.ssh/privkey</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--name</td>
<td>(Optional) The name for the new credentials configuration. The name is useful for tracking the configuration.</td>
</tr>
</tbody>
</table>
## Database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>--passPhrase</td>
<td>The passphrase for the public/private key pair, if you specified one when creating the key pair. Specify <code>-p</code> (with no passphrase) to be prompted. Specify <code>-hp &lt;passphrase&gt;</code> to provide the passphrase in the command.</td>
</tr>
<tr>
<td>-hp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-t</td>
<td>--tenantOcid</td>
<td>Your tenancy OCID. See Where to Find Your Tenancy’s OCID on page 198. The tenancy OCID looks something like this: ocid1.tenancy.oc1..&lt;unique_ID&gt;</td>
</tr>
<tr>
<td>-u</td>
<td>--userOcid</td>
<td>The user name OCID for your Oracle Cloud Infrastructure user account. You can find the OCID in the Console: Open the Profile menu (👤) and click User Settings. The user name OCID looks something like this: ocid1.user.oc1..&lt;unique_ID&gt;</td>
</tr>
</tbody>
</table>

### Example

The following command creates a credentials configuration:

```
[root@dbsys ~]# dbcli create-bmccredential -c patching -hp mypass -t ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsdfsq -u ocid1.user.oc1..aaaaaaalhdxviuxqi7xevqsksccl6edokgldvuf6raskcioq4x2z7watsfa-f 60:9e:56:26:4b:dd:46:dc:8c:a8:05:6d:9f:0a:30:d2 -k /root/.ssh/privkey

{
  "jobId" : "f8c80510-b717-4ee2-a47e-cd380480b28b",
  "status" : "Created",
  "message" : null,
  "reports" : [ ],
  "createTimestamp" : "December 26, 2016 22:46:38 PM PST",
  "resourceList" : [ ],
  "description" : "BMC Credentials Creation",
  "updatedTime" : "December 26, 2016 22:46:38 PM PST"
}
```

### dbcli list-bmccredentials

Use the `dbcli list-bmccredentials` command to list the credentials configurations on the DB system.

Oracle Cloud Infrastructure User Guide 1500
Syntax

dbcli list-bmccredentials [-h] [-j]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

Example

The following command lists the credentials configurations on the DB system:

```
[root@dbsys ~]# dbcli list-bmccredentials
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>f19d7c8b-d0d5-4jhf-852b-eb2a81cb7ce5</td>
<td>patch1</td>
<td>Patching</td>
<td></td>
</tr>
<tr>
<td><a href="https://objectstorage.us-phoenix-1.oraclecloud.com">https://objectstorage.us-phoenix-1.oraclecloud.com</a></td>
<td></td>
<td>Configured</td>
<td></td>
</tr>
<tr>
<td>f1a8741c-b0c4-4jhf-239b-ab2a81jhfd64</td>
<td>patch2</td>
<td>Patching</td>
<td></td>
</tr>
<tr>
<td><a href="https://objectstorage.us-phoenix-1.oraclecloud.com">https://objectstorage.us-phoenix-1.oraclecloud.com</a></td>
<td></td>
<td>Configured</td>
<td></td>
</tr>
</tbody>
</table>

**dbcli describe-bmccredential**

Use the dbcli describe-bmccredential command to display details about a credentials configuration.

Syntax

```
dbcli describe-bmccredential -i <credentials_id> [-h] [-j]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--id</td>
<td>The ID for the credentials configuration. Use the dbcli list-bmccredentials on page 1500 command to get the ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

Example

The following command displays details about the specified credentials configuration:

```
[root@dbsys ~]# dbcli describe-bmccredential -i 09f9988e-ee5d-4dfe-8814-890828d1c763
```

BMC Credentials details

```
```

Oracle Cloud Infrastructure User Guide 1501
**Database**

| ID: 09f9988e-eed5-4dde-8814-890678d1c763 |
| Name: patch23 |
| Tenant OCID: ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqaef44n2b2m2yt2j6x32uzr4h25vqstifsfdq |
| User OCID: ocid1.user.oc1..aaaaaaaahhjhiuxqi7xe5vqscc16edokgldvuf6raskcioq4x2z7watjhf |
| Credentials Type: Patching |
| objectStore URL: https://objectstorage.us-phoenix-1.oraclecloud.com |
| Status: Configured |
| Created: January 9, 2017 1:19:11 AM PST |
| UpdatedTime: January 9, 2017 1:41:46 AM PST |

**dbcli delete-bmccredential**

Use the `dbcli delete-bmccredential` command to delete a credentials configuration.

**Syntax**

```
dbcli delete-bmccredential -i <credentials_id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--id</td>
<td>The ID for the credentials configuration. Use the <code>dbcli list-bmccredentials</code> command to get the ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command deletes the specified credentials configuration:

```
[root@dbsys ~]# dbcli delete-bmccredential -i f19d7c8b-d0d5-4jhf-852b-eb2a81cb7ce5
```

**dbcli update-bmccredential**

Use the `dbcli update-bmccredential` command to update a credentials configuration.

**Syntax**

```
dbcli update-bmccredential -i <credentials_id> -n <credentials_name> -c [backup|patching|other] -p|-hp <passphrase> -f <fingerprint> -k <private_key_path> [-h] [-j]
```
## Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--credentialsType</td>
<td>The type of Object Storage credentials configuration (these values are <strong>not</strong> case sensitive): BACKUP - Reserved for the future use. PATCHING - For downloading patches from the service. OTHER - Reserved for the future use.</td>
</tr>
<tr>
<td>-i</td>
<td>--id</td>
<td>The ID for the credentials configuration. Use the <code>dbcli list-bmccredentials</code> command to get the ID.</td>
</tr>
<tr>
<td>-f</td>
<td>--fingerPrint</td>
<td>The public key fingerprint, for example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td>-k</td>
<td>--privateKey</td>
<td>The path to the private key file in PEM format, for example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="example.png" alt="Example" /></td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--name</td>
<td>(Optional) The name for the credentials configuration. Use the <code>dbcli list-bmccredentials</code> command to get the name.</td>
</tr>
<tr>
<td>-p</td>
<td>--passPhrase</td>
<td>The passphrase for the public/private key pair, if you specified one when creating the key pair. Specify <code>-p</code> (with no passphrase) to be prompted. Specify <code>-hp &lt;passphrase&gt;</code> to provide the passphrase in the command.</td>
</tr>
<tr>
<td></td>
<td>-hp</td>
<td></td>
</tr>
</tbody>
</table>
Example

The following command updates a credentials configuration:

```
[root@dbsys ~]# dbcli update-bmccredential -c OTHER -i 6f921b29-61b6-56f4-889a-ce9270621956
{
    "jobId" : "6e95a69e-cf73-4e51-a444-c7e4b9631c27",
    "status" : "Created",
    "message" : null,
    "reports" : [ ],
    "createTimestamp" : "January 19, 2017 12:01:10 PM PST",
    "resourceList" : [ ],
    "description" : "Update BMC Credentials of object 6f921b29-61b6-48f4-889a-ce9270621945",
    "updatedTime" : "January 19, 2017 12:01:10 PM PST"
}
```

Component Command

dbcli describe-component

<table>
<thead>
<tr>
<th>Tip:</th>
<th>Your DB system might not include this newer command. If you have trouble running the command, use the CLI Update Command on page 1483 command to update the database CLI and then retry the command.</th>
</tr>
</thead>
</table>

Note: The dbcli describe-component command is not available on 2-node RAC DB systems. Patching 2-node systems from Object Storage is not supported.

Use the dbcli describe-component command to show the installed and available patch versions for the server, storage, and/or database home components in the DB system.

This command requires a valid Object Storage credentials configuration. Use the Bmccredential Commands on page 1498 command to create the configuration if you haven’t already done so. If the configuration is missing or invalid, the command fails with the error: Failed to connect to the object store. Please provide valid details.

For more information about updating the CLI, creating the credentials configuration, and applying patches, see Patching a DB System on page 1407.

Syntax

dbcli describe-component [-s <server_group>] [-d <db_group>] [-h] [-j]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>--dbhomes</td>
<td>(Optional) Lists the installed and available patch versions for only the database home components.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
Database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>--server</td>
<td>(Optional) Lists the installed and available patch versions for only the server components.</td>
</tr>
</tbody>
</table>

**Example**

The following command to show the current component versions and the available patch versions in the object store:

```
[root@dbsys ~]# dbcli describe-component
```

```
System Version
--------------
12.1.2.10.0

Component                                Installed Version    Available
Version ---------------------------------------- -------------------
----------------------
OAK                                      12.1.2.10.0          up-to-date
GI                                       12.1.0.2.161018      up-to-date
ORADB12102_HOME1                         12.1.0.2.161018      up-to-date
ORADB12102_HOME2, ORADB12102_HOME3       12.1.0.2.160719
  12.1.0.2.161018
```

**Database Commands**

The following commands are available to manage databases:

- `dbcli clone-database`
- `dbcli create-database`
- `dbcli delete-database`
- `dbcli describe-database`
- `dbcli list-databases`
- `dbcli modify-database`
- `dbcli recover-database`
- `dbcli register-database`
- `dbcli update-database`

**dbcli clone-database**

Use the `dbcli clone-database` command to clone a database.

**Syntax**

```
dbcli clone-database -f <name> -u <name> -n <name> [-s <shape>] [-t <type>] [m <sys_password>] [-p <tde_password>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>--sourcedbname</td>
<td>Source database name.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>-m</td>
<td>--syspassword</td>
<td>(Optional) Password for SYS.</td>
</tr>
<tr>
<td>-n</td>
<td>--dbname</td>
<td>Database name.</td>
</tr>
<tr>
<td>-p</td>
<td>--tdepassword</td>
<td>(Optional) Password for source TDE wallet.</td>
</tr>
<tr>
<td>-s</td>
<td>--dbshape</td>
<td>(Optional) Database shape.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Examples: odb1, odb2.</td>
</tr>
<tr>
<td>-t</td>
<td>--dbtype</td>
<td>(Optional) Database Type: SI</td>
</tr>
<tr>
<td>-u</td>
<td>--databaseUniqueName</td>
<td>Database unique name.</td>
</tr>
</tbody>
</table>

**dbcli create-database**

Use the `dbcli create-database` command to create a new database. You can create a database with a new or existing Oracle Database home, however each database home can have only one database.

It takes a few minutes to create the database. After you run the `dbcli create-database` command, you can use the `dbcli list-jobs` command to check the status of the database creation job.

**Tip:**

Wait for the database creation job to complete before you attempt to create another database. Running multiple `dbcli create-database` commands at the same time can result in some of the creation jobs not completing.

Once the database is created, you can use the `dbcli list-databases -j` command to see additional information about the database.

**Note:**

The `dbcli create-database` command is available on bare metal DB systems only.

You must create and activate a master encryption key for any PDBs that you create. After creating or plugging in a new PDB on a 1- or 2-node RAC DB System, use the `dbcli update-tdekey` command to create and activate a master encryption key for the PDB. Otherwise, you might encounter the error `ORA-28374: typed master key not found in wallet` when attempting to create tablespaces in the PDB. In a multitenant environment, each PDB has its own master encryption key which is stored in a single keystore used by all containers. For more information, see "Overview of Managing a Multitenant Environment" in the Oracle Database Administrator’s Guide.

**Syntax**

```
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-bi</td>
<td>--backupconfigid</td>
<td>Defines the backup configuration identifier for future use. Use the dbcli list-backupconfigs command to get the ID.</td>
</tr>
<tr>
<td>-bn</td>
<td>--backupconfigname</td>
<td>Defines the backup configuration name for future use. Use the dbcli list-backupconfigs command to get the name.</td>
</tr>
<tr>
<td>-c</td>
<td>--cdb</td>
<td>(Optional) Indicates whether to create a Container Database. If omitted, a Container Database is not created.</td>
</tr>
<tr>
<td>-no-c</td>
<td>--no-cdb</td>
<td></td>
</tr>
<tr>
<td>-cs</td>
<td>--characterset</td>
<td>(Optional) Defines the character set for the database. The default is AL32UTF8.</td>
</tr>
<tr>
<td>-cl</td>
<td>--dbclass</td>
<td>Defines the database class. The options are OLTP, DSS, or IMDB. The default is OLTP. For Enterprise Editions, all three classes are supported. For Standard Edition, only OLTP is supported.</td>
</tr>
<tr>
<td>-co</td>
<td>--dbconsole</td>
<td>(Optional) Indicates whether the Database Console is enabled. If omitted, the console is not enabled. This parameter is not available for a version 11.2.0.4 database on a 2-node RAC DB system. For more information, see To enable the console for a version 11.2.0.4 database on a multi-node DB system on page 1432.</td>
</tr>
<tr>
<td>-no-co</td>
<td>--no-dbconsole</td>
<td></td>
</tr>
<tr>
<td>-d</td>
<td>--pdbadmin</td>
<td>Defines the name of the Pluggable Database (PDB) Admin User. The default value is pdbadmin.</td>
</tr>
<tr>
<td>-dn</td>
<td>--dbdomainname</td>
<td>(Optional) Database domain name (indicates the logical location of the database within the network structure).</td>
</tr>
<tr>
<td>-dt</td>
<td>--dbterritory</td>
<td>(Optional) Defines the territory for the database. The default is AMERICA.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-dh</td>
<td>--dbhomeid</td>
<td>Identifies the database home in which to create the database. The database home must be empty because each database home can have only one database. You can use the dbcli list dbhomes command to get the DB home ID. If this parameter is omitted, the database is created with a new Oracle home.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-l</td>
<td>--dblanguage</td>
<td>(Optional) Defines the language for the database. The default is AMERICAN.</td>
</tr>
<tr>
<td>-m</td>
<td>--adminpassword</td>
<td>A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word &quot;oracle&quot; either in forward or reversed order and regardless of casing. Specify -m (with no password) to be prompted for the password.</td>
</tr>
<tr>
<td>-n</td>
<td>--dbname</td>
<td>Defines the name given to the new database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.</td>
</tr>
<tr>
<td>-ns</td>
<td>--nationalscharacterset</td>
<td>(Optional) Defines the national character set for the database. The default is AL16UTF16.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-p</td>
<td>--pdbname</td>
<td>(Optional) Defines a unique name for the PDB. The PDB name must begin with an alphabetic character and can contain a maximum of 30 alphanumeric characters. The only special character permitted is the underscore (_). The default value is pdb1. PDB names must be unique within a CDB and within the listener to which they are registered. Make sure the PDB name is unique on the system. To ensure uniqueness, do not use the default name value (pdb1).</td>
</tr>
<tr>
<td>-r</td>
<td>--dbstorage</td>
<td>Defines the database storage, either ACFS or ASM. The default value is ASM. See Usage Notes on page 1510 for more information.</td>
</tr>
<tr>
<td>-s</td>
<td>--dbshape</td>
<td>Identifies the database sizing template to use for the database. For example, odb1, odb2, or odb3. The default is odb1. For more information, see Database Sizing Templates on page 1552.</td>
</tr>
<tr>
<td>-u</td>
<td>--databaseUniqueName</td>
<td>Defines a unique name for the database to ensure uniqueness within an Oracle Data Guard group (a primary database and its standby databases). The unique name can contain only alphanumeric and underscore (_) characters. The unique name cannot be changed. The unique name defaults to the name specified in the --dbname parameter.</td>
</tr>
</tbody>
</table>
| -v        | --version | Defines the database version as one of the following:  
  - 18.1.0.0  
  - 12.2.0.1  
  - 12.1.0.2 (the default)  
  - 11.2.0.4 |
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-y</td>
<td>--dbtype</td>
<td>Defines the database type. Specify SI for a 1-node instance, RAC for a 2-node cluster, or RACOne for 1-node instance with a second node in cold standby mode. The default value is RAC. These values are not case sensitive.</td>
</tr>
</tbody>
</table>

#### Usage Notes

- You cannot mix Oracle Database Standard Edition and Enterprise Edition databases on the same DB system. (You can mix supported database versions on the DB system, but not editions.)
- When `--dbhomeid` is not provided, the `dbcli create-database` command will create a new Oracle Database home.

**Note:**

Bare metal DB systems allow only one database per database home.

- When `--dbhomeid` is provided, the `dbcli create-database` command creates the database using the Oracle home specified. Use the `dbcli list-dbhomes` command to get the `dbhomeid`. The database home you specify must be empty.
- Oracle Database 12.1 or later databases are supported on both Oracle Automatic Storage Management (ASM) and Oracle ASM Cluster file system (ACFS). The default is Oracle ACFS.
- Oracle Database 11.2 is supported on Oracle ACFS.
- Each database is configured with its own Oracle ACFS file system for the datafiles and uses the following naming convention: `/u02/app/db user/oradata/db name`. The default size of this mount point is 100G.
- Online logs are stored in the `/u03/app/db user/redo/` directory.
- The Oracle Fast Recovery Area (FRA) is located in the `/u03/app/db user/fast_recovery_area` directory.

#### Examples

To create a database and be prompted for the password interactively:

```
[root@dbsys ~]# dbcli create-database -n hrdb -c -m -cl OLTP -s odb2 -p pdb1
Password for SYS, SYSTEM and PDB Admin:
```

```
{
   "jobId" : "f12485f2-dcbe-4ddf-ae01-de24d37037b6",
   "status" : "Created",
   "message" : null,
   "reports" : [ ],
   "createTimestamp" : "August 08, 2016 03:54:03 AM EDT",
   "description" : "Database service creation with db name: hrdb",
   "updatedTime" : "August 08, 2016 03:54:03 AM EDT"
}
```

To create a database non-interactively, providing the password on the command line:

```
[root@dbsys ~]# dbcli create-database -n crmdb -hm <password> -cl OLTP -s odb2
```

```
{
   "jobId" : "30b5e2a6-493b-4461-98b8-78e9a5f8cdd",
   "status" : "Created",
   "message" : null,
```
dbcli delete-database

Use the `dbcli delete-database` command to delete a database.

**Note:**
The `dbcli create-database` command is available on bare metal DB systems only.

**Syntax**

```
dbcli delete-database -i <db_id> -in <db_name> [-fd] [-j] [-h]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-fd</td>
<td>--force</td>
<td>(Optional) Forces the delete operation.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>The ID of the database to delete. Use the <code>dbcli list-databases</code> command to get the database ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>The name of the database to delete. Use the <code>dbcli list-databases</code> command to get the database name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**
The following command deletes the database named 625d9b8a-baea-4994-94e7-4c4a857a17f9:

```
[root@dbsys ~]# dbcli delete-database -i 625d9b8a-baea-4994-94e7-4c4a857a17f9
```

**dbcli describe-database**

Use the `dbcli describe-database` command to display database details.

**Syntax**

```
dbcli describe-database -i <db_id> -in <db_name> [-h] [-j]
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>The ID of the database to display. Use the <code>dbcli list-databases</code> command to get the database ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>The name of the database to display. Use the <code>dbcli list-databases</code> command to get the database name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

### Example

The following command displays information for a database named b727bf80-c99e-4846-ac1f-28a81a725df6:

```
[root@dbsys ~]# dbcli describe-dbhome -i b727bf80-c99e-4846-ac1f-28a81a725df6
```

DB Home details

```
ID: b727bf80-c99e-4846-ac1f-28a81a725df6
Name: OraDB12102_home1
Version: 12.1.0.2
Home Location: /u01/app/orauser/product/12.1.0.2/dbhome_1
Created: Jun 2, 2016 10:19:23 AM
```

### dbcli list-databases

Use the `dbcli list-databases` command to list all databases on the DB system.

**Syntax**

```
dbcli list-databases [-h] [-j]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

### Example

The following command displays a list of databases:

```
[root@dbsys ~]# dbcli list-databases
```

```
ID            DB Name    DB Version           CDB
Class Shape   Storage     Status
------ ------ -------- ---------  -------
```
Database

The following command displays the JSON output for a database:

```
[root@dbsys ~]# dbcli list-databases -j
{
  "id" : "80ad855a-5145-4f8f-a08f-406c5e4684ff",
  "name" : "dbtst",
  "dbName" : "dbtat",
  "databaseUniqueName" : "dbtst_phx1cs",
  "dbVersion" : "12.1.0.2",
  "dbHomeId" : "2efe7af7-0b70-4e9b-ba8b-71f11c6fe287",
  "instanceOnly" : false,
  "registerOnly" : false,
  "dbId" : "167525515",
  "isCdb" : true,
  "pdbBName" : "pdb1",
  "pdbAdminUserName" : "pdbuser",
  "enableTDE" : true,
  "dbType" : "SI",
  "dbTargetNodeNumber" : "0",
  "dbClass" : "OLTP",
  "dbShape" : "odb2",
  "dbStorage" : "ACFS",
  "dbCharacterSet" : {
    "characterSet" : "US7ASCII",
    "nlsCharacterset" : "AL16UTF16",
    "dbTerritory" : "AMERICA",
    "dbLanguage" : "AMERICAN"
  },
  "dbConsoleEnable" : false,
  "backupConfigId" : null,
  "backupDestination" : "NONE",
  "cloudStorageContainer" : null,
  "state" : {
    "status" : "CONFIGURED"
  },
  "createTime" : "November 09, 2016 17:23:05 PM UTC",
  "updatedTime" : "November 09, 2016 18:00:47 PM UTC"
}
```

dbcli modify-database

Use the `dbcli modify-database` command to modify a database.

**Syntax**

```
dbcli modify-database -i <db_id> -dh <destination_db_home_id> [-h] [-j]
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-dh</td>
<td>--destdbhomeid</td>
<td>Destination database home ID.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--databaseid</td>
<td>Database ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**(dbcli recover-database)**

Use the `dbcli recover-database` command to recover a database.

**Syntax**

```
bdcli recover-database [-br <json>] [-in <db_name>] [-i <db_id>] [-r <time>]
[-t {Latest|PITR|SCN}] [-s] [-l <location>] [-tp <tde_password>] [-h] [-j]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-br</td>
<td>--backupReport</td>
<td>(Optional) JSON input for backup report.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>(Optional) Database resource ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>(Optional) Database name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-l</td>
<td>--tdeWalletLocation</td>
<td>(Optional) TDE wallet backup location. TDE wallet should be backed up in tar.gz format.</td>
</tr>
<tr>
<td>-r</td>
<td>--recoveryTimeStamp</td>
<td>(Required when recovery type is PITR) Recovery timestamp in the format mm/dd/yyyy hh:mm:ss. Default: [ ]</td>
</tr>
<tr>
<td>-s</td>
<td>--scn</td>
<td>(Required when recovery type is SCN) SCN.</td>
</tr>
<tr>
<td>-t</td>
<td>--recoverytype</td>
<td>(Required when backup report is provided) Recovery type. Possible values are Latest, PITR, and SCN.</td>
</tr>
<tr>
<td>-tp</td>
<td>--tdeWalletPassword</td>
<td>(Optional) TDE wallet password.</td>
</tr>
</tbody>
</table>

**(dbcli register-database)**

Use the `dbcli register-database` command to register a database that has been migrated to Oracle Cloud Infrastructure. The command registers the database to the dcs-agent so it can be managed by the dcs-agent stack.
**Note:**

The dbcli register-database command is not available on 2-node RAC DB systems.

**Syntax**

```bash
dbcli register-database -bi <bkup_config_id> -c {OLTP|DSS|IMDB} [-co|-no-co] -s (odb1|odb2|...) -t SI [-o <db_host_name>] [-tp <password>] -sn <service_name> -p [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-bi</td>
<td>--backupconfigid</td>
<td>Defines the backup configuration ID. Use the dbcli list-backupconfigs command to get the ID.</td>
</tr>
<tr>
<td>-c</td>
<td>--dbcclass</td>
<td>Defines the database class. The options are OLTP, DSS, or IMDB. The default is OLTP. For Enterprise Editions, all three classes are supported. For Standard Edition, only OLTP is supported.</td>
</tr>
<tr>
<td>-co</td>
<td>--dbconsole</td>
<td>(Optional) Indicates whether the Database Console is enabled or not. If omitted, the console is not enabled.</td>
</tr>
<tr>
<td>-no-co</td>
<td>--no-dbconsole</td>
<td></td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-o</td>
<td>--hostname</td>
<td>(Optional) Defines the database host name. The default is Local host name.</td>
</tr>
<tr>
<td>-p</td>
<td>--syspassword</td>
<td>Defines a strong password for SYS. Specify -p with no password. You will be prompted for the password. If you must provide the password in the command, for example in a script, use -hp &lt;password&gt; instead of -p.</td>
</tr>
<tr>
<td>-s</td>
<td>--dbshape</td>
<td>Defines the database sizing template to use for the database. For example, odb1, odb2, and odb3. For more information, see Database Sizing Templates on page 1552.</td>
</tr>
</tbody>
</table>
### Parameter
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-sn</td>
<td>--servicename</td>
<td>Defines the database service name used to build the EZCONNECT string for connecting to the database. The connect string format is hostname:port/servicename.</td>
</tr>
<tr>
<td>-t</td>
<td>--dbtype</td>
<td>(Optional) Defines the Database Type as single node (SI). The default value is SI.</td>
</tr>
<tr>
<td>-tp</td>
<td>--tdeWalletPassword</td>
<td>(Optional) Password for TDE wallet. Required if TDE is enabled on the migrated database.</td>
</tr>
</tbody>
</table>

### Example
The following command registers the database with the specified database class, service name, and database sizing template.

```
[root@dbsys ~]# dbcli register-database -c OLTP -s odb1 -sn crmdb.example.com -p
```

Password for SYS:
```
{
   "jobId": "317b430f-ad5f-42ae-bb07-13f053d266e2",
   "status": "Created",
   "message": null,
   "reports": [
   ],
   "createTimestamp": "August 08, 2016 05:55:49 AM EDT",
   "description": "Database service registration with db service name: crmdb.example.com",
   "updatedTime": "August 08, 2016 05:55:49 AM EDT"
}
```

### dbcli update-database
Use the `dbcli update-database` command to associate a backup configuration with a database.

### Syntax
```
dbcli update-database -i <db_id> -bi <bkup_config_id> -b <bkup_config_name> [-id <id>] [-in <name>] [-no-ab] [-h] [-j]
```

### Parameters
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-bi</td>
<td>--backupconfigid</td>
<td>Defines the backup configuration ID. Use the <code>dbcli list-backupconfigs</code> command to get the ID.</td>
</tr>
<tr>
<td>-bin</td>
<td>--backupconfigname</td>
<td>Defines the backup configuration name for future use. Use the <code>dbcli list-backupconfigs</code> command to get the name.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-id</td>
<td>--databaseid</td>
<td>(Optional.) Specifies the DBID, which is a unique 32-bit identification number computed when the database is created. RMAN displays the DBID upon connection to the target database. You can obtain the DBID by querying the V$DATABASE view or the RC_DATABASE and RC_DATABASE_INCARNATION recovery catalog views.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>Defines the database name to be updated. Use the <code>dbcli list-databases</code> command to get the database name.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>Defines the database ID to be updated. Use the <code>dbcli list-databases</code> command to get the database ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-no-ab</td>
<td>--noautobackup</td>
<td>(Optional) Disables automatic backups for the specified database.</td>
</tr>
</tbody>
</table>

**Note:**
Once disabled, automatic backup cannot be re-enabled using the CLI. To re-enable automatic backup, use the Console.

**Example**
The following command associates a backup configuration file with a database:

```
[root@dbsys ~]# dbcli update-database -bi 78a2a5f0-72b1-448f-bd86-cf41b30b64ee -i 71ec8335-113a-46e3-b81f-235f4d1b6fde
{
    "jobId" : "2b104028-a0a4-4855-b32a-b97a37f5f9c5",
    "status" : "Created",
    "message" : null,
    "reports" : [ ],
    "createTimestamp" : 1467775842977,
    "description" : "update database id:71ec8335-113a-46e3-b81f-235f4d1b6fde",
    "updatedTime" : 1467775842978
}
```
Dbhome Commands

The following commands are available to manage database homes:

- `dbcli create-dbhome`
- `dbcli describe-dbhome`
- `dbcli delete-dbhome`
- `dbcli list-dbhomes`
- `dbcli update-dbhome`

`dbcli create-dbhome`

Use the `dbcli create-dbhome` command to create an Oracle Database Home.

**Syntax**

```
dbcli create-dbhome -v <version> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
| -v        | --version | Defines the Database Home version. Specify one of the supported versions:  
            - 18.1.0.0  
            - 12.2.0.1  
            - 12.1.0.2  
            - 11.2.0.4 |

**Example**

The following command creates an Oracle Database Home version 12.1.0.2:

```
[root@dbsys ~]# dbcli create-dbhome -v 12.1.0.2
```

`dbcli describe-dbhome`

Use the `dbcli describe-dbhome` command to display Oracle Database Home details.

**Syntax**

```
dbcli describe-dbhome -i <db_home_id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>
Database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>--dbhomeid</td>
<td>Identifies the database home ID. Use the <code>dbcli list-dbhomes</code> command to get the ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following output is an example of using the display Oracle Database Home details command.

```
[root@dbsys ~]# dbcli describe-dbhome -i 52850389-228d-4397-bbe6-102fda65922b
DB Home details
----------------------------------------------------------------
ID: 52850389-228d-4397-bbe6-102fda65922b
Name: OraDB12102_home1
Version: 12.1.0.2
Home Location: /u01/app/oracle/product/12.1.0.2/dbhome_1
Created: June 29, 2016 4:36:31 AM UTC
```

**dbcli delete-dbhome**

Use the `dbcli delete-dbhome` command to delete a database home from the DB system.

**Syntax**

```
dbcli delete-dbhome -i <db_home_id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbhomeid</td>
<td>Identifies the database home ID to be deleted. Use the <code>dbcli list-dbhomes</code> command to get the ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**dbcli list-dbhomes**

Use the `dbcli list-dbhomes` command to display a list of Oracle Home directories.

**Syntax**

```
dbcli list-dbhomes [-h] [-j]
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>
Database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays a list of Oracle Home directories.

```
[root@dbsys ~]# dbcli list-dbhomes
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>DB Version</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>b727bf80-c99e-4846-ac1f-28a81a725df6 OraDB12102_home1</td>
<td>12.1.0.2 /u01/app/orauser/product/12.1.0.2/dbhome_1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dbcli update-dbhome**

**Tip:**

Your DB system might not include this newer command. If you have trouble running the command, use the CLI Update Command on page 1483 command to update the database CLI and then retry the command.

Use the `dbcli update-dbhome` command to apply the DBBP bundle patch to a database home. For more information about applying patches, see Patching a DB System on page 1407.

**Syntax**

```
dbcli update-dbhome -i <db_home_id> -n <node> [--local] [--precheck] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbhomeid</td>
<td>The ID of the database home. Use the <code>dbcli list-dbhomes</code> command to get the ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--node</td>
<td>(Optional) Node number to be updated. Use the <code>dbcli list-nodes</code> command to get the node number.</td>
</tr>
<tr>
<td></td>
<td>--local</td>
<td>(Optional) Performs the operation on the local node of a multi-node high availability (HA) system. This parameter is not needed to perform the operation on a single-node system.</td>
</tr>
</tbody>
</table>
Example

The following commands update the database home and show the output from the update job:

```bash
[root@dbsys ~]# dbcli update-dbhome -i e1877dac-a69a-40a1-b65a-d5e190e671e6 
{  
    "jobId" : "493e703b-46ef-4a3f-909d-bbd123469bea",  
    "status" : "Created",  
    "message" : null,  
    "reports" : [ ],  
    "createTimestamp" : "January 19, 2017 10:03:21 AM PST",  
    "resourceList" : [ ],  
    "description" : "DB Home Patching: Home Id is e1877dac-a69a-40a1-b65a-d5e190e671e6",  
    "updatedTime" : "January 19, 2017 10:03:21 AM PST"
}

# dbcli describe-job -i 493e703b-46ef-4a3f-909d-bbd123469bea

Job details

ID: 493e703b-46ef-4a3f-909d-bbd123469bea
Description: DB Home Patching: Home Id is e1877dac-a69a-40a1-b65a-d5e190e671e6
Status: Running
Created: January 19, 2017 10:03:21 AM PST
Message:

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start Time</th>
<th>End Time</th>
<th>Status</th>
</tr>
</thead>
</table>

DbstORAGE Commands

The following commands are available to manage database storage:

- dbcli list-dbstorages
- dbcli describe-dbstorage
- dbcli create-dbstorage
- dbcli delete-dbstorage
**dbcli list-dbstorages**

Use the `dbcli list-dbstorages` command to list the database storage in the DB system.

**Syntax**

```
dbcli list-dbstorages [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays details about database storage:

```
[root@dbsys ~]# dbcli list-dbstorages
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>DBUnique Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>_________________________</td>
<td></td>
<td>____________________</td>
<td>______</td>
</tr>
<tr>
<td>afb4a1ce-d54d-4993-a149-0f28c9fb33a4</td>
<td>Acfs</td>
<td>db1_2e56b3a9b815</td>
<td>Configured</td>
</tr>
<tr>
<td>d81e8013-4551-4d10-880b-d1a796bca1bc</td>
<td>Acfs</td>
<td>db11xp</td>
<td>Configured</td>
</tr>
</tbody>
</table>

**dbcli describe-dbstorage**

Use the `dbcli describe-dbstorage` command to show detailed information about a specific database storage resource.

**Syntax**

```
dbcli describe-dbstorage -i <db_storage_id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--id</td>
<td>Defines the database storage ID. Use the <code>dbcli list-dbstorages</code> command to get the database storage ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
Example

The following command displays the database storage details for 105a2db2-625a-45ba-8bdd-ee46da0fd83a:

[root@dbsys ~]# dbcli describe-dbstorage -i 105a2db2-625a-45ba-8bdd-ee46da0fd83a

DBStorage details
----------------------------------------------------------------
ID: 105a2db2-625a-45ba-8bdd-ee46da0fd83a
DB Name: db1
DBUnique Name: db1
DB Resource ID: 439e7bd7-f717-447a-8046-08b5f6493df0
Storage Type: DATA Location: /u02/app/oracle/oradata/db1
RECO Location: /u03/app/oracle/fast_recovery_area/
REDO Location: /u03/app/oracle/redo/
State: ResourceState(status=Configured)
Created: July 3, 2016 4:19:21 AM UTC
UpdatedTime: July 3, 2016 4:41:29 AM UTC

dbcli create-dbstorage

Use the dbcli create-dbstorage command to create the database storage layout without creating the complete database. This is useful for database migration and standby database creation.

Syntax

dbcli create-dbstorage -n <db_name> [-u <db_unique_name>] [-r {ACFS|ASM}] [-s <datasize>] [-h] [-j]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--dbname</td>
<td>Defines the database name. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.</td>
</tr>
<tr>
<td>-r</td>
<td>--dbstorage</td>
<td>(Optional) Defines the type of database storage as ACFS or ASM. The default value is ASM.</td>
</tr>
<tr>
<td>-s</td>
<td>--dataSize</td>
<td>(Optional) Defines the data size in GBs. The minimum size is 10GB. The default size is 100GB.</td>
</tr>
<tr>
<td>-u</td>
<td>--databaseUniqueName</td>
<td>(Optional) Defines the unique name for the database. The default is the database name specified in --dbname.</td>
</tr>
</tbody>
</table>
Example
The following command creates database storage with a storage type of ACFS:

```
[root@dbsys ~]# dbcli create-dbstorage -r ACFS -n testdb -u testdbname
{
   "jobId" : "5884a77a-0577-414f-8c36-1e9d8ae9cee",
   "status" : "Created",
   "message" : null,
   "reports" : [ ],
   "createTimestamp" : 1467952215102,
   "description" : "Database storage service creation with db name: testdb",
   "updatedTime" : 1467952215103
}
```

dbcli delete-dbstorage

Use the `dbcli delete-dbstorage` command to delete database storage that is not being used by the database. A error occurs if the resource is in use.

Syntax

```
dbcli delete-dbstorage -i <dbstorageID> [-h] [-j]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
</tr>
<tr>
<td>-i</td>
<td>--id</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
</tr>
</tbody>
</table>

Example

The following command deletes the specified database storage:

```
[root@dbsys ~]# dbcli delete-dbstorage -i f444dd87-86c9-4969-a72c-fb2026e7384b
{
   "jobId" : "467c9388-18c6-4e1a-8655-2fd3603856ef",
   "status" : "Running",
   "message" : null,
   "reports" : [ ],
   "createTimestamp" : 1467952336843,
   "description" : "Database storage service deletion with id: f444dd87-86c9-4969-a72c-fb2026e7384b",
   "updatedTime" : 1467952336856
}
```
Dgconfig Commands

**dbcli list-dgconfigs**

Use the `dbcli list-dgconfigs` command to list DG configurations.

**Syntax**

```
dbcli list-dgconfigs [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

Featuretracking Commands

**dbcli list-featuretracking**

Use the `dbcli list-featuretracking` command to list tracked features.

**Syntax**

```
dbcli list-featuretracking [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

Job Commands

The following commands are available to manage jobs:

- `dbcli describe-job`
- `dbcli list-jobs`

**dbcli describe-job**

Use the `dbcli describe-job` command to display details about a specific job.

**Syntax**

```
dbcli describe-job -i <job_id> [-h] [-j]
```
**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--jobid</td>
<td>Identifies the job. Use the <code>dbcli list-jobs</code> command to get the jobid.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays details about the specified job ID:

```
[root@dbsys ~]# dbcli describe-job -i 74731897-fb6b-4379-9a37-246912025c17
```

Job details

```
<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Validations</td>
<td>November 18, 2016 8:33:04 PM UTC</td>
</tr>
<tr>
<td>validate recovery window</td>
<td>November 18, 2016 8:33:13 PM UTC</td>
</tr>
<tr>
<td>Db cross check</td>
<td>November 18, 2016 8:33:17 PM UTC</td>
</tr>
<tr>
<td>Database Backup</td>
<td>November 18, 2016 8:33:23 PM UTC</td>
</tr>
<tr>
<td>Backup metadata</td>
<td>November 18, 2016 8:34:22 PM UTC</td>
</tr>
</tbody>
</table>
```

**dbcli list-jobs**

Use the `dbcli list-jobs` command to display a list of jobs, including the job IDs, status, and the job created date and time stamp.

**Syntax**

```
dbcli list-jobs [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
Example

The following command displays a list of jobs:

```
[root@dbsys ~]# dbcli list-jobs
ID                                       Description                                              Status
Created
----------------------------------------
---------------------------------------------------------------------------
----------------------------------- ----------
0a362dac-0339-41b5-9c9c-4d229e363eaa     Database service creation with db name: db11 November 10, 2016 11:37:54 AM UTC Success
9157cc78-b487-4ee9-9f46-0159f10236e4     Database service creation with db name: jhfpdb November 17, 2016 7:19:59 PM UTC Success
013c408d-37ca-4f58-a053-02d4efdc42d0     create backup config:myBackupConfig November 18, 2016 8:28:14 PM UTC Success
921a54e3-c359-4aea-9efc-6ae7346cb0c2     update database id:80ad855a-5145-4f8f-a08f-406c5e4684ff November 18, 2016 8:32:16 PM UTC Success
74731897-fb6b-4379-9a37-246912025c17     Backup service creation with db name: dbtst November 18, 2016 8:33:04 PM UTC Success
40a227b1-8c47-46b9-a116-48cc1476fc12     Creating a report for database 80ad855a-5145-4f8f-a08f-406c5e4684ff November 18, 2016 8:41:39 PM UTC Success
```

Latestpatch Command

dbcli describe-latestpatch

Tip:
Your DB system might not include this newer command. If you have trouble running the command, use the CLI Update Command on page 1483 command to update the database CLI and then retry the command.

Note:
The dbcli describe-latestpatch command is not available on 2-node RAC DB systems. Patching 2-node systems from Object Storage is not supported.

Use the dbcli describe-latestpatch command show the latest patches applicable to the DB system and available in Oracle Cloud Infrastructure Object Storage.

This command requires a valid Object Storage credentials configuration. Use the Bmccredential Commands on page 1498 command to create the configuration if you haven't already done so. If the configuration is missing or invalid, the command fails with the error: Failed to connect to the object store. Please provide valid details.

For more information about updating the CLI, creating the credentials configuration, and applying patches, see Patching a DB System on page 1407.

Syntax

dbcli describe-latestpatch [-h] [-j]
**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays patches available in the object store:

```
[root@dbsys ~]# dbcli describe-latestpatch
```

<table>
<thead>
<tr>
<th>componentType</th>
<th>availableVersion</th>
</tr>
</thead>
<tbody>
<tr>
<td>gi</td>
<td>12.1.0.2.161018</td>
</tr>
<tr>
<td>db</td>
<td>11.2.0.4.161018</td>
</tr>
<tr>
<td>db</td>
<td>12.1.0.2.161018</td>
</tr>
<tr>
<td>oak</td>
<td>12.1.2.10.0</td>
</tr>
</tbody>
</table>

**LogcleanJob Commands**

The following commands are available to manage log cleaning jobs:

- `dbcli create-logCleanJob`
- `dbcli describe-logCleanJob`
- `dbcli list-logCleanJobs`

**dbcli create-logCleanJob**

Use the `dbcli create-logCleanJob` command to create a log cleaning job.

**Syntax**

```
dbcli create-logCleanJob [-c {gi|database|dcs}] [-o <number>] [u {Day|Hour|Minute}] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--components</td>
<td>(Optional) Components. Possible values are gi, database, and dcs. Separate multiple values by commas.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-o</td>
<td>--olderThan</td>
<td>(Optional) Quantity portion of time interval. Default: 30. Cleans logs older than the specified time interval (−o and −u).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-u</td>
<td>--unit</td>
<td>(Optional) Unit portion of time interval. Possible values: Day, Hour, or Minute. Default: Day. Cleans logs older than the specified time interval (-c and -u).</td>
</tr>
</tbody>
</table>

**dbcli describe-logCleanJob**

Use the `dbcli describe-logCleanJob` command to display the summary for a log cleaning job.

**Syntax**

```
dbcli describe-logCleanJob -i <job_id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--jobid</td>
<td>ID of log cleaning job for which to display the summary.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**dbcli list-logCleanJobs**

Use the `dbcli list-logCleanJobs` command to list log cleaning jobs.

**Syntax**

```
dbcli list-logCleanJobs [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Logspaceusage Command**

**dbcli list-logSpaceUsage**

Use the `dbcli list-logSpaceUsage` command to list log space usage.

**Syntax**

```
dbcli list-logSpaceUsage [-c {gi|database|dcs}] [-h] [-j]
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--components</td>
<td>(Optional) Components. Possible values: gi, database, and dcs. Separate multiple values by commas.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

### Netsecurity Commands

The following commands are available to manage network encryption on the DB system:

- `dbcli describe-netsecurity`
- `dbcli update-netsecurity`

**dbcli describe-netsecurity**

Use the `dbcli describe-netsecurity` command to display the current network encryption setting for a database home.

**Syntax**

```
dbcli describe-netsecurity -H <db_home_id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-H</td>
<td>--dbHomeId</td>
<td>Defines the database home ID. Use the <code>dbcli list-dbhomes</code> command to get the dbhomeid.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays the encryption setting for specified database home:

```
[root@dbsys ~]# dbcli describe-netsecurity -H 16c96a9c-f579-4a4c-a645-8d4d22d6889d
```

**NetSecurity Rules**

```
DatabaseHomeID: 16c96a9c-f579-4a4c-a645-8d4d22d6889d

Role: Server
  EncryptionAlgorithms: AES256 AES192 AES128
  IntegrityAlgorithms: SHA1
  ConnectionType: Required

Role: Client
  EncryptionAlgorithms: AES256 AES192 AES128
  IntegrityAlgorithms: SHA1
```
Use the `dbcli update-netsecurity` command to update the Oracle Net security configuration on the DB system.

**Syntax**

```
dbcli update-netsecurity { -c | -s } -t {REJECTED | ACCEPTED | REQUESTED | REQUIRED } -H db_home_id > -e {AES256 | AES192 | AES128 } -i {SHA1 | SHA512 | SHA384 | SHA256 } [-h ] [-j ]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>--client</td>
<td>Indicates that the specified data encryption or data integrity configuration is for the client. (--client and --server are mutually exclusive.)</td>
</tr>
<tr>
<td>-e</td>
<td>--encryptionAlgorithms</td>
<td>Defines the algorithm to be used for encryption. Specify either AES256, AES192, or AES128.</td>
</tr>
<tr>
<td>-H</td>
<td>--dbHomeId</td>
<td>Defines the database home ID. Use the <code>dbcli list-dbhomes</code> command to get the dbHomeId.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--integrityAlgorithms</td>
<td>Defines the algorithm to be used for integrity. Specify either SHA1, SHA512, SHA384, or SHA256. For Oracle Database 11g, the only accepted value is SHA1.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-s</td>
<td>--server</td>
<td>Indicates that the specified data encryption or data integrity configuration is for the server. (--client and --server are mutually exclusive.)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -t        | --connectionType | Specifies how Oracle Net Services data encryption or data integrity is negotiated with clients. The following values are listed in the order of increasing security:  
REJECTED - Do not enable data encryption or data integrity, even if required by the client.  
ACCEPTED - Enable data encryption or data integrity if required or requested by the client.  
REQUESTED - Enable data encryption or data integrity if the client permits it.  
REQUIRED - Enable data encryption or data integrity or preclude the connection.  
For detailed information about network data encryption and integrity, see https://docs.oracle.com/database/121/DBSEG/asoconfg.htm#DBSEG1047. |

**Example**

The following command updates the connection type to ACCEPTED:

```
[root@dbsys ~]# dbcli update-netsecurity -H a2ffbb07-c9c0-4467-a458-bce4d3b76cd5 -t ACCEPTED
```

**Node Command**

**dbcli list-nodes**

Use the `dbcli list-nodes` command to display a list of nodes, including the node numbers.

**Syntax**

```
dbcli list-nodes [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>
Example

The following command displays a list of nodes:

```
[root@dbsys ~]# dbcli list-nodes
node Number node Name          ilom Name            IP Address       Subnet Mask Gateway
---------- ---------------------------------------- -------------------- ------------------ ------------------
0      rac21          N/A     N/A        N/A  N/A        N/A
1      rac22          N/A     N/A        N/A   N/A
```

Objectstoreswift Commands

You can back up a database to an existing bucket in the Oracle Cloud Infrastructure Object Storage service by using the `dbcli create-backup` on page 1488 command, but first you'll need to:

1. Create an object store on the DB system, which contains the endpoint and credentials to access Object Storage, by using the `dbcli create-objectstoreswift` command.
2. Create a backup configuration that refers to the object store ID and the bucket name by using the `dbcli create-backupconfig` on page 1492 command.
3. Associate the backup configuration with the database by using the `dbcli update-database` on page 1516 command.

The following commands are available to manage object stores.

- `dbcli create-objectstoreswift`
- `dbcli describe-objectstoreswift`
- `dbcli list-objectstoreswifts`

**dbcli create-objectstoreswift**

Use the `dbcli create-objectstoreswift` command to create an object store.

**Syntax**

```
dbcli create-objectstoreswift -n <object_store_name>
  -t <object_storage_namespace> -u <user_name> --endpointurl
  https://swiftobjectstorage.<region_name>.oraclecloud.com/v1 -p [-h] [-j]
```

where `<object_storage_namespace>` is your tenancy's Object Storage namespace.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-e</td>
<td>--endpointurl</td>
<td>The following endpoint URL. <a href="https://swiftobjectstorage">https://swiftobjectstorage</a>.&lt;region_name&gt;.oraclecloud.com/v1. See Regions and Availability Domains for region name strings.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--name</td>
<td>The name for the object store to be created.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Full Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-p</td>
<td>--swiftpassword</td>
<td>The auth token that you generated by using the Console or IAM API. For information about generating an auth token for use with Swift, see Managing User Credentials on page 2456. This is not the password for the Oracle Cloud Infrastructure user. Specify <code>-p</code> (with no password) to be prompted. Specify <code>-hp &quot;&lt;password&gt;&quot;</code> in quotes to provide the password (auth token) in the command.</td>
</tr>
<tr>
<td>-t</td>
<td>--tenantname</td>
<td>The Object Storage namespace. of your tenancy.</td>
</tr>
<tr>
<td>-u</td>
<td>--username</td>
<td>The user name for the Oracle Cloud Infrastructure user account, for example: <code>-u djones@example.com</code> This is the user name you use to sign in to the Console. The user name must have tenancy-level access to the Object Storage. An easy way to do this is to add the user name to the Administrators group. However, that allows access to all of the cloud services. Instead, an administrator can create a policy that allows tenancy-level access to just Object Storage. The following is an example of such a policy. Allow group DBAdmins to manage buckets in tenancy Allow group DBAdmins to manage objects in tenancy For more information about adding a user to a group, see Managing Groups on page 2419. For more information about policies, see Getting Started with Policies on page 2135.</td>
</tr>
</tbody>
</table>
**Example**

The following command creates an object store and prompts for the Swift password:

```
[root@dbsys ~]# dbcli create-objectstoreswift -n r2swift
   -t MyObjectStorageNamespace -u djones@example.com -
   e https://swiftobjectstorage.<region_name>.oraclecloud.com/v1
Password for Swift:

{
   "jobId" : "c565bb71-f67b-4fab-9d6f-a34ee36feb7",
   "status" : "Created",
   "message" : "Create object store swift",
   "reports" : [ ],
   "createTimestamp" : "January 19, 2017 11:11:33 AM PST",
   "resourceList" : [ { 
      "resourceId" : "8a0fe039-f5d4-426a-8707-256c612b3a30",
      "resourceType" : "ObjectStoreSwift",
      "jobId" : "c565bb71-f67b-4fab-9d6f-a34ee36feb7",
      "updatedTime" : "January 19, 2017 11:11:33 AM PST"
   } ],
   "description" : "create object store:biyanr2swift",
   "updatedTime" : "January 19, 2017 11:11:33 AM PST"
}
```

**dbcli describe-objectstoreswift**

Use the `dbcli describe-objectstoreswift` command to display details about an object store.

**Syntax**

```
dbcli describe-objectstoreswift -i <object_store_swift_id> -
in <object_store_swift_name> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--objectstoreswiftid</td>
<td>The object store ID. Use the <code>dbcli list-objectstoreswifts</code> command to get the ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--objectstoreswiftName</td>
<td>The object store name. Use the <code>dbcli list-objectstoreswifts</code> command to get the name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays details about an object store:

```
[root@dbsys ~]# dbcli describe-objectstoreswift -i 910e9e2d-25b4-49b4-b88e-
   ff0332f7df87
Object Store details
----------------------------------------------------------------
ID: 910e9e2d-25b4-49b4-b88e-ff0332f7df87
```
dbcli list-objectstoreswifts

Use the `dbcli list-objectstoreswifts` command to list the object stores on a DB system.

**Syntax**

```
dbcli list-objectstoreswifts [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command lists the object stores on the DB system:

```
[root@dbsys ~]# dbcli list-objectstoreswifts
```

<table>
<thead>
<tr>
<th>ID</th>
<th>TenantName</th>
<th>Name</th>
<th>UserName</th>
<th>Url</th>
<th>createTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>2915bc6a-6866-436a-a38c-32302c7c4d8b</td>
<td>LargeComputers</td>
<td>swiftobjstr1</td>
<td><a href="mailto:djones@example.com">djones@example.com</a></td>
<td><a href="https://swiftobjectstorage">https://swiftobjectstorage</a>.&lt;region_name&gt;.oraclecloud.com/v1</td>
<td>November 10, 2016 8:42:18 PM UTC</td>
</tr>
<tr>
<td>910e9e2d-25b4-49b4-b88e-ff0332f7df87</td>
<td>LargeComputers</td>
<td>objstrswift15</td>
<td><a href="mailto:djones@example.com">djones@example.com</a></td>
<td><a href="https://swiftobjectstorage">https://swiftobjectstorage</a>.&lt;region_name&gt;.oraclecloud.com/v1</td>
<td>November 16, 2016 11:25:34 PM UTC</td>
</tr>
</tbody>
</table>

**Pendingjob Command**

**dbcli list-pendingjobs**

Use the `dbcli list-pendingjobs` command to display a list of pending jobs.

**Syntax**

```
dbcli list-pendingjobs [-h] [-j]
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Rmanbackupreport Commands**

The following commands are available to manage RMAN backup reports:

- `dbcli create-rmanbackupreport`
- `dbcli delete-rmanbackupreport`
- `dbcli describe-rmanbackupreport`
- `dbcli list-rmanbackupreports`

**dbcli create-rmanbackupreport**

Use the `dbcli create-rmanbackupreport` command to create an RMAN backup report.

**Syntax**

```
dbcli create-rmanbackupreport -w {summary|detailed} -rn <name> [-i <db_id>] [-in <db_name>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>(Optional) Database resource ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbname</td>
<td>(Optional) Database resource name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-rn</td>
<td>--rptname</td>
<td>RMAN backup report name. Maximum number of characters: 30. Wrap name in single quotes when special characters are used.</td>
</tr>
<tr>
<td>-w</td>
<td>--reporttype</td>
<td>RMAN backup report type. Possible values: summary or detailed.</td>
</tr>
</tbody>
</table>

**dbcli delete-rmanbackupreport**

Use the `dbcli delete-rmanbackupreport` command to delete an RMAN backup report.

**Syntax**

```
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>--dbid</td>
<td>(Optional) Database resource ID.</td>
</tr>
<tr>
<td>-dn</td>
<td>--dbname</td>
<td>(Optional) Database resource name.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--reportid</td>
<td>(Optional) RMAN backup report ID</td>
</tr>
<tr>
<td>-in</td>
<td>--rptname</td>
<td>(Optional) RMAN backup report name</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-n</td>
<td>--numofday</td>
<td>(Optional) Number of days since created (provided with Database ID/Database Name)</td>
</tr>
</tbody>
</table>

**dbcli describe-rmanbackupreport**

Use the `dbcli describe-rmanbackupreport` command to

**Syntax**

```
dbcli describe-rmanbackupreport [-i <rpt_id>] [-in <rpt_name>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--id</td>
<td>(Optional) RMAN backup report ID</td>
</tr>
<tr>
<td>-in</td>
<td>--name</td>
<td>(Optional) RMAN backup report name</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**dbcli list-rmanbackupreports**

Use the `dbcli list-rmanbackupreports` command to

**Syntax**

```
dbcli list-rmanbackupreports [-i <db_id>] [-in <db_name>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbid</td>
<td>(Optional) Database resource ID.</td>
</tr>
</tbody>
</table>
Schedule Commands

The following commands are available to manage schedules:

- `dbcli describe-schedule`
- `dbcli list-schedules`
- `dbcli update-schedule`

**dbcli describe-schedule**

Use the `dbcli describe-schedule` command to describe a schedule.

**Syntax**

```
  dbcli describe-schedule -i <id> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--scheduleid</td>
<td>Schedule ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**dbcli list-schedules**

Use the `dbcli list-schedules` command to list schedules.

**Syntax**

```
  dbcli list-schedules [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**dbcli update-schedule**

Use the `dbcli update-schedule` command to update a schedule.

**Syntax**

```
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>--disable</td>
<td>(Optional) Disables the schedule.</td>
</tr>
<tr>
<td>-e</td>
<td>--enable</td>
<td>(Optional) Enables the schedule.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--scheduleid</td>
<td>Schedule ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-t</td>
<td>--description</td>
<td>(Optional) Description</td>
</tr>
<tr>
<td>-x</td>
<td>--cronExpression</td>
<td>(Optional) Cron expression. Use cronmaker.com to generate a valid cron expression.</td>
</tr>
</tbody>
</table>

### Scheduled execution Command

**dbcli list-scheduledExecutions**

Use the `dbcli list-scheduledExecutions` command to list scheduled executions.

**Syntax**

```
dbcli list-scheduledExecutions [-e <execution_id>] [-i <schedule_id>] [-h] [-j]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-e</td>
<td>--executionid</td>
<td>(Optional) Execution ID.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--scheduleid</td>
<td>(Optional) Schedule ID.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

### Server Command

**dbcli update-server**

**Tip:**

Your DB system might not include this newer command. If you have trouble running the command, use the CLI Update Command on page 1483 command to update the database CLI and then retry the command.

Use the `dbcli update-server` command to apply patches to the server components in the DB system. For more information about applying patches, see Patching a DB System on page 1407.

**Syntax**

```
dbcli update-server [-n <number>] [--local] [--precheck] [-h] [-j]
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-l</td>
<td>--local</td>
<td>(Optional) Performs the operation on the local node of a multi-node high availability (HA) system. This parameter is not needed to perform the operation on a single-node system.</td>
</tr>
<tr>
<td>-n</td>
<td>--node</td>
<td>(Optional) Node number to be updated. Use the <code>dbcli list-nodes</code> command to get the node number.</td>
</tr>
<tr>
<td>-p</td>
<td>--precheck</td>
<td>(Optional) Runs precheck operations to check prerequisites.</td>
</tr>
</tbody>
</table>

### Examples

The following commands update the server and show the output from the update job:

```bash
[root@dbsys ~]# dbcli update-server
{
  "jobId" : "9a02d111-e902-4e94-bc6b-9b820ddf6ed8",
  "status" : "Created",
  "reports" : [ ],
  "createTimestamp" : "January 19, 2017 09:37:11 AM PST",
  "resourceList" : [ ],
  "description" : "Server Patching",
  "updatedTime" : "January 19, 2017 09:37:11 AM PST"
}
```

```bash
# dbcli describe-job -i 9a02d111-e902-4e94-bc6b-9b820ddf6ed8
```

Job details

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start Time</th>
<th>End Time</th>
<th>Status</th>
</tr>
</thead>
</table>
The following command updates node 0 of the server only, with precheck:

```
# dbcli update-server -n 0 -p
{
   "jobId" : "3e2a1e3c-83d3-4101-86b8-4d525f3f8c18",
   "status" : "Created",
   "message" : null,
   "reports" : [ ],
   "createTimestamp" : "April 26, 2019 06:07:27 AM UTC",
   "resourceList" : [ ],
   "description" : "Server Patching Prechecks",
   "updatedTime" : "April 26, 2019 06:07:27 AM UTC"
}
```

**System Command**

**dbcli describe-system**

Use the `dbcli describe-system` command to display details about the system. On a 2-node RAC DB system, the command provides information about the local node.

**Syntax**

```
dbcli describe-system [-b] [-d] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-b</td>
<td>--bom</td>
<td>(Optional) Displays BOM information.</td>
</tr>
<tr>
<td>-d</td>
<td>--details</td>
<td>(Optional) Displays additional information about the DB system, including dcs CLI and agent version information.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**TDE Commands**

The following commands are available to manage TDE-related items (backup reports, keys, and wallets):

- `dbcli list-tdebackupreports`
- `dbcli update-tdekey`
- `dbcli recover-tdewallet`
**dbcli list-tdebackupreports**

Use the `dbcli list-tdebackupreports` command to list backup reports for TDE wallets.

**Syntax**

```
$ dbcli list-tdebackupreports [-i <db_id>] [-in <db_name>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-i</td>
<td>--dbResid</td>
<td>(Optional) Displays the TDE Wallet backup reports for the specified database resource ID. Use the <code>dbcli list-databases</code> command to get the database resource ID.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbResname</td>
<td>(Optional) Displays the TDE Wallet backup reports for the specified database resource name. Use the <code>dbcli list-databases</code> command to get the database resource name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command lists the backup reports for TDE wallets:

```
[root@dbsys ~]# dbcli list-tdebackupreports
DbResID     OraDbId   BackupLocation
--------------------------------------- ------------------------
538ca5b1-654d-4418-8ce1-f49b6c987a60  1257156075   https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/dbaasimage/backuptest/host724007/tdewallet/Testdb5/1257156075/2017-08-17/TDEWALLET_BMC60_2017-08-17_10-58-17.0990.tar.gz
538ca5b1-9fb2-4245-b157-6e25d7c988c5  704287483   https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/dbaasimage/backuptest/host724007/tdewallet/Testdb1/704287483/2017-08-17/TDEWALLET_AUTO_2017-08-17_11-03-25.0953.tar.gz
538ca5b1-9fb2-4245-b157-6e25d7c988c5  704287483   https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/dbaasimage/backuptest/host724007/tdewallet/Testdb1/704287483/2017-08-17/TDEWALLET_AUTO_2017-08-17_11-04-41.0264.tar.gz
19714ffa-de1b-4433-9188-c0592887e609  1157116855   https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/dbaasimage/backuptest/host724007/tdewallet/Testdb7/1157116855/2017-08-17/TDEWALLET_AUTO_2017-08-17_11-57-47.0605.tar.gz
```
**dbcli update-tdekey**

Use the `dbcli update-tdekey` command to update the TDE encryption key inside the TDE wallet. You can update the encryption key for Pluggable Databases (if -pdbNames are specified), and/or the Container Database (if -rootDatabase is specified).

**Syntax**

```
dbcli update-tdekey -i <db_id> -p [-all] -n <pdbname1,pdbname2> [-r|-no-r] -t <tag_name> [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-all</td>
<td>--allPdbNames</td>
<td>(Optional) Flag to rotate (update) all PDB names. To update all instead of specified PDB names, use this parameter instead of -n. Default: false.</td>
</tr>
<tr>
<td>-i</td>
<td>--databaseId</td>
<td>Defines the database ID for which to update the key.</td>
</tr>
<tr>
<td>-p</td>
<td>--password</td>
<td>Defines the TDE Admin wallet password. Specify -p with no password. You will be prompted for the password. If you must provide the password in the command, for example in a script, use -hp &lt;password&gt; instead of -p.</td>
</tr>
<tr>
<td>-n</td>
<td>--pdbNames</td>
<td>Defines the PDB names to be rotated (updated).</td>
</tr>
<tr>
<td>-r</td>
<td>--rootDatabase</td>
<td>Indicates whether to rotate the key for the root database if it is a container database.</td>
</tr>
<tr>
<td>-no-r</td>
<td>--no-rootDatabase</td>
<td></td>
</tr>
<tr>
<td>-t</td>
<td>-tagName</td>
<td>Defines the TagName used to backup the wallet. The default is OdaRotateKey.</td>
</tr>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
</tbody>
</table>

**Example**

The following command updates the key for pdb1 and pdb2 only:

```
[root@dbsys ~]# dbcli update-tdekey -dbid ee3eaab6-a45b-4e61-a218-c4ba665503d9 -p -n pdb1,pdb2

TDE Admin wallet password: {}
```
The following command updates pdb1, pdb2, and the container database:

```bash
[root@dbsys ~]# dbcli update-tdekey -dbid ee3eaab6-a45b-4e61-a218-c4ba665503d9 -p -n pdb1,pdb2 -r
```

TDE Admin wallet password:

```json
{
  "jobId" : "c72385f0-cd81-42df-a8e8-3a1e7cab1278",
  "status" : "Created",
  "message" : null,
  "reports" : [ ],
  "createTimestamp" : 1467876433783,
  "description" : "TDE update",
  "updatedTime" : 1467876433783
}
```

dbcli recover-tdewallet

Use the `dbcli recover-tdewallet` command to recover a TDE wallet.

**Syntax**

```
dbcli recover-tdewallet -in <db_name> -tp <password> [-l <location>] [-h] [-j]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>--help</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-in</td>
<td>--dbName</td>
<td>Database name.</td>
</tr>
<tr>
<td>-j</td>
<td>--json</td>
<td>(Optional) Displays JSON output.</td>
</tr>
<tr>
<td>-l</td>
<td>--tdeWalletBackupLocation</td>
<td>(Optional) TDE wallet backup location. TDE wallet should be backed up in tar.gz format.</td>
</tr>
<tr>
<td>-tp</td>
<td>--tdeWalletPassword</td>
<td>Defines the TDE Admin wallet password.</td>
</tr>
</tbody>
</table>

**Admin Commands**

The following commands are to perform administrative actions on the DB system:

- `dbadmcli manage diagcollect`
- `dbadmcli power`
- `dbadmcli power disk status`
- `dbadmcli show controller`
• `dbadmcli show disk`
• `dbadmcli show diskgroup`
• `dbadmcli show env.hw` (environment type and hardware version)
• `dbadmcli show env.hw` (environment type and hardware version)
• `dbadmcli show fs` (file system details)
• `dbadmcli show storage`
• `dbadmcli stordiag`

**dbadmcli manage diagcollect**

Use the `dbadmcli manage diagcollect` command to collect diagnostic information about a DB system for troubleshooting purposes, and for working with Oracle Support Services.

**Syntax**

```
  dbadmcli manage diagcollect --storage [-h]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>--storage</td>
<td>Collects all of the logs for any storage issues.</td>
</tr>
</tbody>
</table>

**Example**

```
[root@dbsys ~]# dbadmcli manage diagcollect --storage
Collecting storage log data. It will take a while, please wait...
Collecting oak data. It will take a while, please wait...
tar: Removing leading `/` from member names
tar: /opt/oracle/oak/onecmd/tmp/OakCli-Command-Output.log: file changed as we read it
Logs are collected to: /opt/oracle/oak/log/dbsys/oakdiag/oakStorage-dbsys-20161118_2101.tar.gz
```

**dbadmcli power**

Use the `dbadmcli power` command to power a disk on or off.

**Note:**

The `dbadmcli power` command is not available on 2-node RAC DB systems.

**Syntax**

```
  dbadmcli power {-on|-off} <name> [-h]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>name</td>
<td>Defines the disk resource name. The resource name format is pd_[0..3]. Use the <code>dbadmcli show disk</code> command to get the disk resource name.</td>
</tr>
<tr>
<td>-off</td>
<td>Powers off the disk.</td>
</tr>
<tr>
<td>-on</td>
<td>Powers on the disk.</td>
</tr>
</tbody>
</table>

**dbadmcli power disk status**

Use the `dbadmcli power disk status` command to display the current power status of a disk.

**Syntax**

```
dbamcli power disk status <name> [-h]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>name</td>
<td>Identifies a specific disk resource name. The resource name format is pd_[0..3]. For example, pd_01.</td>
</tr>
</tbody>
</table>

**Example**

```
[root@dbsys ~]# dbadmcli power disk status pd_00
The disk is powered ON
```

**dbadmcli show controller**

Use the `dbadmcli show controller` command to display details of the controller.

**Syntax**

```
dbamcli show controller <controller_id> [-h]
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_id</td>
<td>The ID number of the controller. Use the <code>dbadmcli show storage</code> command to get the ID.</td>
</tr>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>

**dbadmcli show disk**

Use the `dbadmcli show disk` command to display the status of a single disk or all disks on the DB system.
Database

Syntax

```
dbadmcli show disk [<name>] [-shared] [-all] [-getlog] [-h]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-all</td>
<td>(Optional) Displays detailed information for the named disk.</td>
</tr>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>-getlog</td>
<td>(Optional) Displays all the SMART log entries for an NVMe disk.</td>
</tr>
<tr>
<td>name</td>
<td>(Optional) Identifies a specific disk resource name. The resource name format is pd_[0..3]. If omitted, the command displays information about all disks on the system.</td>
</tr>
<tr>
<td>-shared</td>
<td>(Optional) Displays all the shared disks.</td>
</tr>
</tbody>
</table>

Examples

To display the status of all the disks on the system:

```
[root@dbsys ~]# dbadmcli show disk
NAME    PATH            TYPE            STATE            STATE_DETAILS
pd_00   /dev/nvme2n1    NVD             ONLINE          Good
pd_01   /dev/nvme3n1    NVD             ONLINE          Good
pd_02   /dev/nvme1n1    NVD             ONLINE          Good
pd_03   /dev/nvme0n1    NVD             ONLINE          Good
```

To display the status of a disk named pd_00:

```
[root@dbsys ~]# dbadmcli show disk pd_00
The Resource is : pd_00
ActionTimeout : 1500
ActivePath     : /dev/nvme2n1
AsmDiskList    : [data_00] [reco_00]
AutoDiscovery  : 1
AutoDiscoveryHi: [data:70:NVD] [reco:30:NVD]
CheckInterval  : 300
ColNum          : 0
CriticalWarning : 0
DependListOpr   : add
Dependency      : [0]
DiskId          : 360025380144d5332
DiskType        : NVD
Enable          : 1
ExpNum          : 29
HbaPortNum      : 10
IState          : 0
Initialized     : 0
IsConfigDepende : false
ModelNum        : MS1PC2DD3ORA3.2T
MonitorFlag     : 1
MultiPathList   : [/dev/nvme2n1]
**Database**

**Name** : pd_00
**NewPartAddr** : 0
**OSUserType** : |userType:Multiuser|
**PlatformName** : X5_2_LITE_IAAS
**PrevState** : Invalid
**PrevUsrDevName** :
**SectorSize** : 512
**SerialNum** : S2LHNAAH502855
**Size** : 3200631791616
**SlotNum** : 0
**SmartDiskWarnin** : 0
**SmartTemperatur** : 32
**State** : Online
**StateChangeTs** : 1467176081
**StateDetails** : Good
**TotalSectors** : 6251233968
**TypeName** : 0
**UsrDevName** : NVD_S00_S2LHNAAH502855
**VendorName** : Samsung
**gid** : 0
**mode** : 660
**uid** : 0

To display the SMART logs for an NVMe disk:

```bash
[root@dbsys ~]# dbadmcli show disk pd_00 -getlog
SMART / Health Information :
---------------------------
Critical Warning : Available Spare below Threshold : FALSE
Critical Warning : Temperature above Threshold : FALSE
Critical Warning : Reliability Degraded : FALSE
Critical Warning : Read-Only Mode : FALSE
Critical Warning : Volatile Memory Backup Device Failure : FALSE
Temperature : 32 degree Celsius
Available Spare : 100%
Available Spare Threshold : 10%
Device Life Used : 0%
Data Units Read (in 512k byte data unit) : 89493
Data Units Written (in 512k byte data unit) : 270387
Number of Host Read Commands : 4588381
Number of Host Write Commands : 6237344
Controller Busy Time : 3 minutes
Number of Power Cycles : 227
Number of Power On Hours : 1115
Number of Unsafe Shutdowns : 218
Number of Media Errors : 0
Number of Error Info Log Entries : 0
```

**dbadmcli show diskgroup**

Use the `dbadmcli show diskgroup` command to list configured diskgroups or display a specific diskgroup configuration.

**Syntax**

To list configured diskgroups:

```bash
dbamcli show diskgroup [-h]
```
To display DATA configurations:

```
dbadmcli show diskgroup [DATA] [-h]
```

To display RECO configurations:

```
dbadmcli show diskgroup [RECO] [-h]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA</td>
<td>(Optional) Displays the DATA diskgroup configurations.</td>
</tr>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
<tr>
<td>RECO</td>
<td>(Optional) Displays the RECO diskgroup configurations.</td>
</tr>
</tbody>
</table>

### Examples

To list all diskgroups:

```
[root@dbsys ~]# dbadmcli show diskgroup
DiskGroups
---------
DATA
RECO
```

To display DATA configurations:

```
[root@dbsys ~]# dbadmcli show diskgroup DATA
ASM_DISK  PATH            DISK  STATE  STATE_DETAILS
data_00  /dev/NVD_S00_S2LHNAAH101026p1  pd_00  ONLINE  Good
data_01  /dev/NVD_S01_S2LHNAAH101008p1  pd_01  ONLINE  Good
```

### dbadmcli show env_hw

Use the `dbadmcli show env_hw` command to display the environment type and hardware version of the current DB system.

**Syntax**

```
dbadmcli show env_hw [-h]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>

### dbadmcli show fs

Use the `dbadmcli show fs` command to display file system details.
**Syntax**

dbadmcli show fs [-h]

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>

**dbadmcli show storage**

Use the `dbadmcli show storage` command to show the storage controllers, expanders, and disks.

**Syntax**

dbadmcli show storage [-h]

To show storage errors:

`dbadmcli show storage -errors [-h]`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-errors</td>
<td>(Optional) Shows storage errors.</td>
</tr>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>

**Example**

To display storage devices:

```
[root@dbsys ~]# dbadmcli show storage
==== BEGIN STORAGE DUMP ========
Host Description: Oracle Corporation:ORACLE SERVER X5-2
Total number of controllers: 5
   Id          = 4
   Pci Slot    = -1
   Serial Num  =
   Vendor      =
   Model       =
   FwVers      =
   strId       = iscsi_tcp:00:00.0
   Pci Address = 00:00.0

   Id          = 0
   Pci Slot    = 13
   Serial Num  = S2LHNAAH504431
   Vendor      = Samsung
   Model       = MS1PC2DD3ORA3.2T
   FwVers      = KFYA8R3Q
   strId       = nvme:25:00.00
   Pci Address = 25:00.00

   Id          = 1
   Pci Slot    = 12
   Serial Num  = S2LHNAAH505449
```
Vendor = Samsung
Model = MS1PC2DD3ORA3.2T
FwVers = KPYA8R3Q
strId = nvme:27:00.00
Pci Address = 27:00.0

Id = 2
Pci Slot = 10
Serial Num = S2LHNAAH503573
Vendor = Samsung
Model = MS1PC2DD3ORA3.2T
FwVers = KPYA8R3Q
strId = nvme:29:00.00
Pci Address = 29:00.0

Id = 3
Pci Slot = 11
Serial Num = S2LHNAAH503538
Vendor = Samsung
Model = MS1PC2DD3ORA3.2T
FwVers = KPYA8R3Q
strId = nvme:2b:00.00
Pci Address = 2b:00.0

Total number of expanders: 0
Total number of PDs: 4
/dev/nvme2n1    Samsung           NVD 3200gb slot:  0  pci : 29
/dev/nvme3n1    Samsung           NVD 3200gb slot:  1  pci :  2
/dev/nvme1n1    Samsung           NVD 3200gb slot:  2  pci : 27
/dev/nvme0n1    Samsung           NVD 3200gb slot:  3  pci : 25

==== END STORAGE DUMP ========

dbadmcli stordiag

Use the dbadmcli stordiag command to collect detailed information for each disk or NVM Express (NVMe).

Syntax

dbadmcli stordiag <name> [-h]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Defines the disk resource name. The resource name format is pd_[0..3].</td>
</tr>
<tr>
<td>-h</td>
<td>(Optional) Displays help for using the command.</td>
</tr>
</tbody>
</table>

Example

To display detailed information for NVMe pd_00:

[root@dbsys ~]# dbadmcli stordiag pd_0

Database Sizing Templates

When you create a database using the dbcli create-database command, you can specify a database sizing template with the --dbshape parameter. The sizing templates are configured for different types of database workloads. Choose the template that best matches the most common workload your database performs:
- Use the OLTP templates if your database workload is primarily online transaction processing (OLTP).
- Use the DSS templates if your database workload is primarily decision support (DSS) or data warehousing.
- Use the in-memory (IMDB) templates if your database workload can fit in memory, and can benefit from in-memory performance capabilities.

The following tables describe the templates for each type of workload.

### OLTP Database Sizing Templates

<table>
<thead>
<tr>
<th>Template</th>
<th>CPU Cores</th>
<th>SGA (GB)</th>
<th>PGA (GB)</th>
<th>Flash (GB)</th>
<th>Processes</th>
<th>Redo Log File Size (GB)</th>
<th>Log Buffer (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>odb1s</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>200</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb1</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>12</td>
<td>200</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb2</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>24</td>
<td>400</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb4</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>48</td>
<td>800</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td>odb6</td>
<td>6</td>
<td>24</td>
<td>12</td>
<td>72</td>
<td>1200</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb8</td>
<td>8</td>
<td>32</td>
<td>16</td>
<td>n/a</td>
<td>1600</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb10</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>n/a</td>
<td>2000</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb12</td>
<td>12</td>
<td>48</td>
<td>24</td>
<td>144</td>
<td>2400</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb16</td>
<td>16</td>
<td>64</td>
<td>32</td>
<td>192</td>
<td>3200</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb20</td>
<td>20</td>
<td>80</td>
<td>40</td>
<td>n/a</td>
<td>4000</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb24</td>
<td>24</td>
<td>96</td>
<td>48</td>
<td>192</td>
<td>4800</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb32</td>
<td>32</td>
<td>128</td>
<td>64</td>
<td>256</td>
<td>6400</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb36</td>
<td>36</td>
<td>128</td>
<td>64</td>
<td>256</td>
<td>7200</td>
<td>4</td>
<td>64</td>
</tr>
</tbody>
</table>

### DSS Database Sizing Templates

<table>
<thead>
<tr>
<th>Template</th>
<th>CPU Cores</th>
<th>SGA (GB)</th>
<th>PGA (GB)</th>
<th>Processes</th>
<th>Redo Log File Size (GB)</th>
<th>Log Buffer (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>odb1s</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>200</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>200</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>400</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb4</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>800</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td>odb6</td>
<td>6</td>
<td>12</td>
<td>24</td>
<td>1200</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>Template</td>
<td>CPU Cores</td>
<td>SGA (GB)</td>
<td>PGA (GB)</td>
<td>Processes</td>
<td>Redo Log File Size (GB)</td>
<td>Log Buffer (MB)</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>----------</td>
<td>----------</td>
<td>-----------</td>
<td>-------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>odb8</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>1600</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb10</td>
<td>10</td>
<td>20</td>
<td>40</td>
<td>2000</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb12</td>
<td>12</td>
<td>24</td>
<td>48</td>
<td>2400</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb16</td>
<td>16</td>
<td>32</td>
<td>64</td>
<td>3200</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb20</td>
<td>20</td>
<td>40</td>
<td>80</td>
<td>4000</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb24</td>
<td>24</td>
<td>48</td>
<td>96</td>
<td>4800</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb32</td>
<td>32</td>
<td>64</td>
<td>128</td>
<td>6400</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb36</td>
<td>36</td>
<td>64</td>
<td>128</td>
<td>7200</td>
<td>4</td>
<td>64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Template</th>
<th>CPU Cores</th>
<th>SGA (GB)</th>
<th>PGA (GB)</th>
<th>In-Memory (GB)</th>
<th>Processes</th>
<th>Redo Log File Size (GB)</th>
<th>Log Buffer (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>odb1s</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>200</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb1</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>200</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb2</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>400</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>odb4</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>800</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td>odb6</td>
<td>6</td>
<td>24</td>
<td>12</td>
<td>12</td>
<td>1200</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb8</td>
<td>8</td>
<td>32</td>
<td>16</td>
<td>16</td>
<td>1600</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb10</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>20</td>
<td>2000</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>odb12</td>
<td>12</td>
<td>48</td>
<td>24</td>
<td>24</td>
<td>2400</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb16</td>
<td>16</td>
<td>64</td>
<td>32</td>
<td>32</td>
<td>3200</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb20</td>
<td>20</td>
<td>80</td>
<td>40</td>
<td>40</td>
<td>4000</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb24</td>
<td>24</td>
<td>96</td>
<td>48</td>
<td>48</td>
<td>4800</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb32</td>
<td>32</td>
<td>128</td>
<td>64</td>
<td>64</td>
<td>6400</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>odb36</td>
<td>36</td>
<td>128</td>
<td>64</td>
<td>64</td>
<td>7200</td>
<td>4</td>
<td>64</td>
</tr>
</tbody>
</table>
Storage Scaling Considerations for Virtual Machine Databases Using Fast Provisioning

**Note:**
This topic applies only to 1-node virtual machine DB systems.

When you provision a virtual machine DB system using the fast provisioning option, the **Available storage** (GB) value you specify during provisioning determines the maximum total storage available through scaling.

The following table details the maximum storage value available through scaling for each setting offered in the provisioning workflow:

<table>
<thead>
<tr>
<th>Initial storage specified during provisioning (GB)</th>
<th>Maximum storage available through scaling (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>2560</td>
</tr>
<tr>
<td>512</td>
<td>2560</td>
</tr>
<tr>
<td>1024</td>
<td>5120</td>
</tr>
<tr>
<td>2048</td>
<td>10240</td>
</tr>
<tr>
<td>4096</td>
<td>20480</td>
</tr>
<tr>
<td>8192</td>
<td>40960</td>
</tr>
</tbody>
</table>

For more information on creating a virtual machine DB system, see [Creating Bare Metal and Virtual Machine DB Systems](#) on page 1370.

**Security Technical Implementation Guide (STIG) Tool for Virtual Machine DB systems**

This topic describes a python script, referred to as the STIG tool, for Oracle Cloud Infrastructure virtual machine DB systems provisioned using Oracle Linux 7. The STIG tool is used to ensure security compliance with DISA's Oracle Linux 7 STIG. The script does the following:

- Makes the base image of the virtual machine DB system compliant with the Oracle Linux 7 STIG
- Embeds certain STIG rules into the system that can be activated after provisioning when required to meet security compliance standards
- Categorizes the embedded rules, allowing you to view and monitor the rules in the following categories:
  - **Static**: Rules included in the base image
  - **DoD**: Rules optionally activated after provisioning when needed to meet U.S. Department of Defense compliance standards
  - **Runtime**: Rules activated after provisioning when needed. Intended for use by all users needing to harden security for virtual machine DB systems (including users outside of the U.S. Department of Defense).
- Provides a rollback capability, allowing you to roll back a DB system to a state with no configuration modifications made by the script
- Provides a compliance check capability, allowing you to see how many of the scripts rules are successfully passed by the DB system

**Acquiring the STIG Tool**

The STIG tool is provided for all newly-provisioned virtual machine DB systems. The STIG tool is provided in the following OS directory location on virtual machine DB system nodes:

```
/opt/oracle/dcs/bin/dbcsstig
```

Updated versions of the STIG tool will be available for download from the [Oracle Technology Network (OTN)](http://www.oracle.com/technology). Updated versions of the STIG tool are also provided as available when you update the DB system agent.
Using the STIG Tool

Use the following syntax for the STIG tool:

```
dbcsstig --<operation> <category>
```

For example:

```
dbcsstig --fix dod
```

Command Reference

Operations

<table>
<thead>
<tr>
<th>Operation Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>--check, -c</td>
<td>Checks for compliance with rules included in specified category</td>
</tr>
<tr>
<td>--fix, -f</td>
<td>Applies fixes for rules included in specified category</td>
</tr>
<tr>
<td>--rollback, -rb</td>
<td>Rolls back system configuration changes implemented by the STIG tool</td>
</tr>
<tr>
<td>--version, -v</td>
<td>Provides version information for the STIG tool script</td>
</tr>
<tr>
<td>--help, -h</td>
<td>Provides command line help information</td>
</tr>
</tbody>
</table>

Rule Categories

<table>
<thead>
<tr>
<th>Category Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>Used to specify rules included in the base image of the virtual machine DB system</td>
</tr>
<tr>
<td>dod</td>
<td>Used to specify rules required for compliance with DISA’s Oracle Linux 7 STIG</td>
</tr>
<tr>
<td>runtime</td>
<td>Used to specify rules activated after provisioning for general security hardening</td>
</tr>
<tr>
<td>all</td>
<td>Used to specify all rule</td>
</tr>
</tbody>
</table>

Enabling FIPS, SE Linux, and STIG on Bare Metal or Virtual Machine DB System Components

This topic describes how to add FIPS security enhancements to a bare metal or virtual machine DB system in Oracle Cloud Infrastructure (OCI). The procedure is performed on each system node, and enables the following:

- Federal Information Processing Standards (FIPS)
- Security Enhanced (SE) Linux
- Security Technical Implementation Guide (STIG) standards

To enable FIPS, SE Linux, and STIG

1. Open an SSH session to the DB system node and switch to the root user, then navigate to `/opt/oracle/dcs/bin`:

```
# sudo -s
# cd /opt/oracle/dcs/bin
```
2. Run the following command to enable FIPS:

```
# dbcli secure-dbsystem -se -sd -fo -fd
```

The system provide details on the enable job:

```
Job details
ID: <job_ID_number>
Description: Secure DB System
Status: Created
Created: November 8, 2020 4:12:29 PM UTC
Progress: 0%
Message:

Task Name Start Time End Time Status
```

3. Verify the job details as follows:

```
# dbcli describe-job -i <job_ID_number>
```

The system provides information on the progress, status, and details of the enable job. For example:

```
Job details
ID: <job_ID_number>
Description: Secure DB System
Status: Success
Created: November 8, 2020 4:12:29 PM UTC
Progress: 100%
Message:

Task Name Start Time End Time Status
```

4. Once the Job details output shows the Status "Success", you must restart your DB system node using the OCI Console. This is required because enabling FIPS and SE Linux updates OS kernel. See To start, stop, or reboot a database system on page 1383 for instructions.

To check a DB system node for FIPS and SE Linux configurations

To confirm that FIPS and SE Linux are enabled on your DB system node, use the following dbcli command:

```
# dbcli get-dbsystemsecurestatus
```
The system returns details as shown in the following example:

```json
{
    "isSELinuxEnabledForOS" : true,
    "isFipsEnabledForOS" : true,
    "fipsStatusForDBs" : [ {
        "databaseResId" : "<DB_ID_number>",
        "status" : true
    } ]
}
```

### External Database Service

You can manage and monitor Oracle Databases that are located outside of Oracle Cloud Infrastructure (OCI) using OCI's External Database service. External Database allows you use cloud-based tools such as Database Management with your external databases.

### About the Database Management Service

As a Database Administrator, you can use the Oracle Cloud Infrastructure Database Management service to monitor and manage your Oracle Databases. Database Management supports Oracle Database versions 11.2.0.4 and later. Using Database Management you can:

- Monitor the key performance and configuration metrics of your fleet of Oracle Databases. You can also compare and analyze database metrics over a selected period of time.
- Group your critical Oracle Databases, which reside across compartments into a Database Group, and monitor them.
- Create SQL jobs to perform administrative operations on a single Oracle Database or a Database Group.

For complete documentation on the Database Management service, see Database Management. The rest of the External Database section of the documentation covers only the creation and management of external database "handles" and the OCI external database connection resource that allows you connect your external database to a handle in OCI.

### How the External Database Service Works

To manage an external database using OCI's External Database service, you create an OCI resource known as a "handle" that represents the external database within your tenancy. After creating a handle for your database, you create a second resource called a database connection. The connection stores the information required for your OCI tenancy to connect to the external database. After creating the connection resource and connecting the OCI handle to your external database instance, you can enable the Database Management service to monitor the health and performance of your database.

### The OCI External Database Handle

You can create an OCI external database handle for the following types of external databases:

- External container databases
- External pluggable databases
- External non-container databases

The handle stores a few pieces of metadata that allow you to manage your database instance within OCI. This metadata includes the following information related to managing the handle in OCI:

- An OCID, which allows the external database instance to be identified and managed within OCI.
- An OCI display name
- Compartments assignment information (optional)
- Tags (optional)
In addition to the OCI-related metadata, the handle stores metadata derived from the database instance. This includes the database unique name, the Oracle Database software edition and version, and other details. All of this information stored by the handle can be viewed in the OCI Console or retrieved using the API. Metadata derived from the external database instance (such as database unique name) is only populated in the handle after a database connection is established between the handle and the instance.

**Scanning an External Container Database to Discover Pluggable Databases**

After you create and connect an external container database handle, you can use the handle to scan the external container database and discover pluggable databases that have not been connected to OCI. If any pluggable databases are discovered that are not connected to Oracle Cloud Infrastructure, the connection details for these databases are listed in the work request generated by the scan operation. See To scan an external container database for pluggable databases on page 1562 for more information.

**The OCI Database Connection Resource**

The OCI database connection resource stores details about how a specific handle connects to an external Oracle Database instance. These details include the following:

- Connection strings details (DNS hostname, port, service name, network protocol)
- Connection type and OCI agent ID
- User credentials and role

**Prerequisites**

To use the External Database service, you will need the following:

- An Oracle Cloud Infrastructure (OCI) tenancy. See Setting Up Your Tenancy on page 122 for information if you do not currently use OCI.
- One or more external databases located outside of OCI. The External Database service supports container databases, pluggable databases, and non-container databases that use the following Oracle Database software versions: 11gR2, 12cR1, 12cR2, 18c, and 19c. You can use the External Database service with database clones and with high-availability / disaster recovery databases standby databases.
- A Management Agent Cloud Service agent with source credentials. See the Management Agent documentation for details on creating this resource in OCI.

**Creating External Database Handles**

This topic provides information on creating OCI external database handles using the OCI Console and API. See External Database Service on page 1558 for an overview of the External Database service.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud external database resources on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more information about writing policies for databases, see Details for the Database Service on page 2240.

**Using the Console**
To create an OCI external pluggable database resource

This procedure describes the steps you take to create an OCI external pluggable database resource, also called a "handle". The handle functions as a representation within OCI of an Oracle Database instance located outside of the Oracle's cloud. **Note:** This procedure is not used to create an Oracle Database instance outside of Oracle's Cloud.

1. Open the . Under , click .
2. Choose your Compartment.
4. Click Create External Pluggable Database.

The Create an external pluggable database dialog opens.

5. Choose a compartment for the external pluggable database.
6. Enter a database display name. The display name is a user-friendly name to help you easily identify the resource.
7. Select an external container database to house the pluggable database.
8. Click Show Advanced Options to specify the following options for the database:

   **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

9. Click Create External Pluggable Database.

WHAT NEXT?

- After creating the OCI external pluggable database resource (the handle), you can configure the handle's connection to the external pluggable database instance. See To create a connection for an OCI external pluggable database resource on page 1564 for more information.
- After connecting the handle to an external pluggable database instance, you can enable Database Management for your external pluggable database. See the Database Management documentation for more information.

To create an OCI external container database

This procedure describes the steps you take to create an OCI external container database resource, also called a "handle". The handle functions as a representation within OCI of an Oracle Database instance located outside of the Oracle's cloud. **Note:** This procedure is not used to create an Oracle Database instance outside of Oracle's Cloud.

1. Open the . Under , click .
2. Choose your Compartment.
4. Click Create External Container Database.

The Create an external container database dialog opens.

5. Choose a compartment for the external pluggable database.
6. Enter a container database display name. The display name is a user-friendly name to help you easily identify the resource.
7. Click Show Advanced Options to specify the following options for the database:

   **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

8. Click Create External Container Database.

WHAT NEXT?

- After creating the OCI external container database resource (the handle), you can configure the resource's connection to a container database located outside of OCI. See To create a connection for an OCI external pluggable database resource on page 1564 for more information.
After connecting the handle to an external container database, you can perform a scan of the external container database to discover pluggable databases. See To scan an external container database for pluggable databases on page 1562 for more information.

After connecting the handle to an external container database, you can enable Database Management for your external container database. See the Database Management documentation for more information.

To create an OCI external non-pluggable database

This procedure describes the steps you take to create an OCI external non-container database resource, also called a "handle". The handle functions as a representation within OCI of an Oracle Database instance located outside of the Oracle's cloud. Note: This procedure is not used to create an Oracle Database instance outside of Oracle's Cloud.

1. Open the . Under , click .
2. Choose your Compartment.
4. Click Create External Non-Container Database.
   The Create an external non-container database dialog opens.
5. Choose a compartment for the external non-container database.
6. Enter a non-container database display name. The display name is a user-friendly name to help you easily identify the resource.
7. Click Show Advanced Options to specify the following options for the database:
   Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
8. Click Create External Non-Container Database.

WHAT NEXT?

After creating the OCI external non-container database resource (the handle), you can configure the handle’s connection to the external database instance. See To create a connection for an OCI external non-container database resource on page 1565 for more information.

After connecting the handle to an external database instance, you can enable Database Management for the external database. See the Database Management documentation for more information.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to create OCI external database handles:

- CreateExternalContainerDatabase
- CreateExternalPluggableDatabase
- CreateExternalNonContainerDatabase

Managing External Database Handles

This topic provides information on managing Oracle Cloud Infrastructure (OCI) external database handles using the OCI Console and API. See External Database Service on page 1558 for an overview of the External Database service.

Note:

See the Database Management documentation for instructions on enabling Database Management for an external database handle in the OCI Console.
**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

For administrators: The policy in *Let database admins manage Oracle Cloud external database resources* on page 2150 lets the specified group do everything with databases and related Database resources.

If you’re new to policies, see *Getting Started with Policies* on page 2135 and *Common Policies* on page 2142. For more information about writing policies for databases, see *Details for the Database Service* on page 2240.

**Using the Console**

*To move an OCI external database handle to another compartment*

1. Open the . Under , click .
2. Choose your *Compartment*.
3. Under *External Databases*, click either *Pluggable Database*, *Container Databases*, or *Non-Container Databases*, depending on the type of external database handle you are managing.
4. In the list of external database handles, click on the name of the handle you want to move.
5. On the external database details page, click the *Move Resource* button.
6. In the *Move Resource to a Different Compartment* dialog, choose a new compartment using the drop-down selector.
7. Click *Move Resource*.

*To delete an OCI external database handle*

This topic describes how to delete the following OCI resources:

- External pluggable database handle
- External container database handle
- External non-container database handle

1. Open the . Under , click .
2. Choose your *Compartment*.
3. Under *External Databases*, click either *Pluggable Database*, *Container Databases*, or *Non-Container Databases*, depending on the type of external database handle you are deleting.
4. In the list of external database handles, click on the name of the handle you want to delete.
5. On the external database details page, click the *Delete* button.

*To scan an external container database for pluggable databases*

1. Open the . Under , click .
2. Choose your *Compartment*.
3. Under *External Databases*, click *Container Databases*.
4. In the list of external container database handles, click on the name of the handle that is connected to the container database you want to scan.

5. On the external container database details page, click **Scan for Pluggable Databases**.

   If any pluggable databases are discovered that are not connected to Oracle Cloud Infrastructure, the connection details for these databases are listed in the **work request** generated by the scan operation.

Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use these API operations to manage external container database resources:

- ListExternalContainerDatabases
- GetExternalContainerDatabase
- ChangeExternalContainerDatabaseCompartment
- ScanExternalContainerDatabasePluggableDatabases
- EnableExternalContainerDatabaseDatabaseManagement
- DisableExternalContainerDatabaseDatabaseManagement
- UpdateExternalContainerDatabase
- DeleteExternalContainerDatabase

Use these API operations to manage external pluggable database resources:

- ListExternalPluggableDatabases
- GetExternalPluggableDatabase
- ChangeExternalPluggableDatabaseCompartment
- EnableExternalPluggableDatabaseDatabaseManagement
- DisableExternalPluggableDatabaseDatabaseManagement
- UpdateExternalPluggableDatabase
- DeleteExternalPluggableDatabase

Use these API operations to manage external non-container database resources:

- ListExternalNonContainerDatabases
- GetExternalNonContainerDatabase
- ChangeExternalNonContainerDatabaseCompartment
- EnableExternalNonContainerDatabaseDatabaseManagement
- DisableExternalNonContainerDatabaseDatabaseManagement
- UpdateExternalNonContainerDatabase
- DeleteExternalNonContainerDatabase

Creating and Managing an External Database Connection

This topic provides information on managing Oracle Cloud Infrastructure (OCI) external database connections using the OCI Console and API. The external database connection resource allows you to connect an OCI external database handle to an Oracle Database instance located outside of OCI. See [External Database Service](#) on page 1558 for more information about the External Database service and the database connection resource.

**Note:**

Currently the External Database service supports only Management Agent Cloud Service (MACS) agents for creating a connection to your external databases. Enterprise Manager Cloud Control Agents are not supported at this time.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let database admins manage Oracle Cloud external database resources on page 2150 lets the specified group do everything with databases and related Database resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more information about writing policies for databases, see Details for the Database Service on page 2240.

Using the Console

To create a connection for an OCI external pluggable database resource

1. Open the . Under , click .
2. Choose your Compartment.
4. In the list of OCI external pluggable database resources (also called "handles"), click the display name of the handle you want to create a connection for.
5. Click Connect to External Pluggable Database.

   The Connect to an external pluggable database dialog opens.
6. Enter a connection display name. This is a user-friendly name to help you easily identify the resource.
7. Enter the DNS hostname for the database on your premises that you are connecting to Oracle Cloud.
8. Enter the port being used by the database outside of Oracle Cloud Infrastructure for database connections.
9. Enter the service name for the database outside of Oracle Cloud Infrastructure that will be used by the connection.
10. Enter the connection agent ID. See Management Agent for more information about this Oracle Cloud Infrastructure feature.
11. Enter the Username for the database credentials that will be used by this connection.
12. Enter the Password for the database credentials that will be used by this connection.
13. Enter a Credential name prefix. This string is the first part of the full credential name. Your prefix is prepended to a system-generated Credential name prefix to create the full credential name.
14. Enter the Role for the database credentials that will be used by this connection.
15. Click Show Advanced Options to specify the following options for the database:

   Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
16. Click Connect to External Pluggable Database.

To create a connection for an OCI external container database resource

1. Open the . Under , click .
2. Choose your Compartment.
4. In the list of OCI external container database resources (also called "handles"), click the display name of the handle you want to create a connection for.
5. Click Connect to External Pluggable Database.

   The Connect to an external pluggable database dialog opens.
6. Enter a connection display name. This is a user-friendly name to help you easily identify the resource.
7. Enter the DNS hostname for the database on your premises that you are connecting to Oracle Cloud Infrastructure.
8. Enter the port being used by the database outside of Oracle Cloud Infrastructure for database connections.
9. Enter the service name for the database outside of Oracle Cloud Infrastructure that will be used by the connection.
10. Enter the connection agent ID. See Management Agent for more information about this Oracle Cloud Infrastructure feature.
11. Enter the Username for the database credentials that will be used by this connection.
12. Enter the Password for the database credentials that will be used by this connection.
13. Enter a Credential name prefix. This string is the first part of the full credential name. Your prefix is prepended to a system-generated Credential name prefix to create the full credential name.
14. Enter the Role for the database credentials that will be used by this connection.
15. Click Show Advanced Options to specify the following options for the database:

   Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

16. Click Connect to External Pluggable Database.

To create a connection for an OCI external non-container database resource

1. Open the . Under , click .
2. Choose your Compartment.
4. In the list of OCI external non-container database resources (also called "handles"), click the display name of the handle you want to create a connection for.
5. Click Connect to External Non-Container Database.

   The Connect to an Connect to an external non-container database dialog opens.

6. Enter a connection display name. This is a user-friendly name to help you easily identify the resource.
7. Enter the DNS hostname for the database on your premises that you are connecting to Oracle Cloud.
8. Enter the port being used by the database outside of Oracle Cloud Infrastructure for database connections.
9. Enter the service name for the database outside of Oracle Cloud Infrastructure that will be used by the connection.
10. Enter the connection agent ID. See Management Agent for more information about this Oracle Cloud Infrastructure feature.
11. Enter the Username for the database credentials that will be used by this connection.
12. Enter the Password for the database credentials that will be used by this connection.
13. Enter a Credential name prefix. This string is the first part of the full credential name. Your prefix is prepended to a system-generated Credential name prefix to create the full credential name.
14. Enter the Role for the database credentials that will be used by this connection.
15. Click Show Advanced Options to specify the following options for the database:

   Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

16. Click Connect to External Non-Container Database.

To check the connection status of an external database connection

1. Open the . Under , click .
2. Choose your Compartment.
3. Under External Databases, click either Pluggable Database, Container Databases, or Non-Container Databases, depending on the type of external database you are using.
4. In the list of external database handles, click the name of the handle you want to check the connection status of.
5. On the Database Details page, under Resources, click Connections.
6. In the list of database connections, click the name of the connection you want to check the status of.
7. Click Check Connection Status. A "Check Connection Status" work request is created. Click on the work request name to see details of the connection status.
To update the connection credentials of an external database handle

1. Open the . Under , click .
2. Choose your **Compartment**.
3. Under **External Databases**, click either **Pluggable Database**, **Container Databases**, or **Non-Container Databases**, depending on the type of external database handle connection you are updating.
4. In the list of external database handles, click on the name of the handle associated with the connection you want to update.
5. On the external database details page, under **Resources**, click **Connections**.
6. In the list of connections, click the name of the connection you want to update.
7. On the External Connection Details page, click **Update Connection Credentials**.
8. In the **Update credentials** dialog, enter the following information:
   - Username
   - Password
   - Role
9. Click **Update Credentials**.

To update the connection strings of an external database handle

1. Open the . Under , click .
2. Choose your **Compartment**.
3. Under **External Databases**, click either **Pluggable Database**, **Container Databases**, or **Non-Container Databases**, depending on the type of external database handle connection you are updating.
4. In the list of external database handles, click on the name of the handle associated with the connection you want to update.
5. On the external database details page, under **Resources**, click **Connections**.
6. In the list of connections, click the name of the connection you want to update.
7. On the External Connection Details page, click **Update Connection Strings**.
8. In the **Update connection strings** dialog, enter the following information:
   - DNS hostname
   - Port
   - Service
9. Click **Update Connection Strings**.

To delete an external database connection

1. Open the . Under , click .
2. Choose your **Compartment**.
3. Under **External Databases**, click either **Pluggable Database**, **Container Databases**, or **Non-Container Databases**, depending on the type of external database handle you are deleting.
4. In the list of external database handles, click on the name of the handle associated with the connection you want to delete.
5. On the external database details page, under **Resources**, click **Connections**.
6. In the list of connections, click the name of the connection you want to delete.
7. On the External Connection Details page, click **Delete**.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to create and manage external database connections:

- CreateExternalDatabaseConnector
- ListExternalDatabaseConnectors
- GetExternalDatabaseConnector
Oracle Database Software Images

This topic provides an overview of the database software image resource type, which you can use to create databases and Oracle Database Homes, and to patch databases. Database software images give you the ability to create a customized Oracle Database software configuration that includes your chosen updates (PSU, RU or RUR), and optionally, a list of one-off (or interim) patches or an Oracle Home inventory file. This reduces the time required to provision and configure your databases, and makes it easy for your organization to create an approved "gold image" for developers and database administrators.

Using Database Software Images in Oracle Cloud Infrastructure

Creation and Storage of Database Software Images

Database software images are resources within your tenancy that you create prior to provisioning or patching a DB system, Exadata Cloud Service instance, Database Home, or database. There is no limit on the number of database software images you can create in your tenancy, and you can create your images with any Oracle Database software version and update supported in Oracle Cloud Infrastructure.

Database software images are automatically stored in Oracle-managed Object Storage and can be viewed and managed in the Oracle Cloud Infrastructure Console. Note that database software images incur Object Storage usage costs. Database software image are regional-level resources and can be accessed from any availability domain within their region.

See To create a database software image on page 1568 for information on creating an image.

Using a Database Software Image with a Bare Metal or Virtual Machine DB System

Provisioning: After you create a database software image, you can use it to provision the initial database in a new bare metal or virtual machine DB system, or to provision a new database in an existing bare metal DB system. For more information, see the following topics:

• To create a DB system on page 1372
• To create a new database in an existing DB system on page 1415

Patching: You can use a database software image to update the database software of an existing virtual machine or bare metal database in Oracle Cloud Infrastructure. This is sometimes referred to as in-place patching. See To patch a database on page 1422 for information on using a custom database software image to patch a database in a bare metal or virtual machine DB system. To determine if a database has been patched with a particular database software image, follow the instructions in To view the patch history of a database on page 1422. For Oracle Data Guard associations, you can use a custom database software image for in-place patching on both the primary and standby database instances to ensure that both databases have the same patches.

Using a Database Software Image with an Exadata Cloud Service Instance

Provisioning: After you create a database software image, you can use it to create an Oracle Database Home in an Exadata Cloud Service instance. For more information, see To create a new Database Home in an existing Exadata Cloud Service instance on page 1330.

Patching: To patch a database in an Exadata Cloud Service instance using a custom database software image, create the Database Home using the image, and then move the database to that Database Home. For more information, see Patching Individual Oracle Databases in an Exadata Cloud Service Instance on page 1287.

Setting up Data Guard: When creating an Oracle Data Guard association, you can use a custom database software image to create a new Database Home for the new standby database. For more information, see To enable Oracle Data Guard on an Exadata Cloud Service instance on page 1342.
Using the Console

To create a database software image

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
3. Click Create Database Software Image.
4. In the Display name field, provide a display name for your image. Avoid entering confidential information.
5. Choose your Compartment.
6. Choose a Shape family. A custom database software images is compatible with only one shape family. Available shape families are the following:
   - Bare metal and virtual machine DB systems
   - Exadata Cloud Service instances
7. Choose the Database version for your image.
8. Choose the patch set update, proactive bundle patch, or release update. For information on Oracle Database patching models, see Release Update Introduction and FAQ (Doc ID 2285040.1).
9. Optionally, you can enter a comma-separated list of one-off (interim) patch numbers.
10. Optionally, you can upload an Oracle Home inventory file from an existing Oracle Database.
11. Click Show Advanced Options to add tags to your database software image. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
12. Click Create Database Software Image.

To view the patch information of a database software image

To view the Oracle Database version, update information (PSU/BP/RU level) and included one-off (interim) patches of a database software image, use the following instructions:

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
3. In the list of database software images, find the image you want to view and click on the display name of the image.
4. On Database Software Image Details page for your selected image, details about the image are displayed:
   - The Oracle Database version is displayed in the General Information section. For example: 19.0.0.0
   - The PSU/BP/RU field of the Patch Information section displays update level for the image. For example: 19.5.0.0
   - The One-Off Patches field displays the number of one-off patches included in the image, if any. The count includes all patches specified when creating the image (excluding patches listed in Isinventory). To view the included patches (if any are included), click the Copy All link and paste the list of included patches into a text editor. The copied list of patch numbers is comma-separated and can be used to create additional database software images.

To delete a database software image

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
3. In the list of database software images, find the image you want to delete and click the action icon (three dots) at the end of the row.
4. Click Delete.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage database software images:
• CreateDatabaseSoftwareImage
• ListDatabaseSoftwareImages
• GetDatabaseSoftwareImage
• DeleteDatabaseSoftwareImage
• ChangeDatabaseSoftwareImageCompartment

Oracle Maximum Availability Architecture in Oracle Cloud Infrastructure

Oracle Maximum Availability Architecture is a set of best practices developed by Oracle engineers over many years for the integrated use of Oracle High Availability technologies.

Oracle Maximum Availability Architecture and Autonomous Database Cloud

High availability is suitable for all development, test, and production databases that have high uptime requirements and low data loss tolerance. By default, Autonomous Databases are highly available, incorporating a multi-node configuration to protect against localized hardware failures that do not require fast disaster recovery. Each Autonomous Database application service resides in at least one Oracle Real Application Clusters (Oracle RAC) instance with the option to fail over to another available Oracle RAC instance using Autonomous Data Guard for unplanned outages or planned maintenance activities, resulting in zero or near-zero downtime. Autonomous Database's automatic backups are stored in Oracle Cloud Infrastructure Object Storage and replicated to another availability domain, and can be restored in the event of a disaster. Major database upgrades, however, require downtime.

The uptime service-level objective per month is 99.95% (a maximum of 22 minutes of downtime per month), but when you use Maximum Availability Architecture best practices for continuous service, most months would effectively have zero downtime. The uptime service-level objective does not include downtime due to customer-initiated high availability tests, disaster recovery (such as an availability domain or regional outage), database corruptions, or downtime due to planned maintenance that cannot be done online or through an Oracle RAC rolling update solution, such as major database upgrades from one release to another.

The following table describes the recovery-time objectives and recovery-point objectives (data loss tolerance) for service-level objectives.

<table>
<thead>
<tr>
<th>Failure and Maintenance Events</th>
<th>Database Downtime</th>
<th>Service-Level Downtime (RTO)</th>
<th>Potential Service-Level Data Loss (RPO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localized events, including:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Exadata cluster network topology failures</td>
<td>Zero</td>
<td>Near-zero</td>
<td>Zero</td>
</tr>
<tr>
<td>• Storage (disk and flash) failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Database instance failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Database server failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Periodic software and hardware maintenance updates</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Database Downtime (RTO)

- **Database Downtime (RTO)**: Minutes to hours
- **Service-Level Downtime (RTO)**: Minutes to hours
- **Potential Service-Level Data Loss (RPO)**: 15 minutes

<table>
<thead>
<tr>
<th>Failure and Maintenance Events</th>
<th>Database Downtime</th>
<th>Service-Level Downtime (RTO)</th>
<th>Potential Service-Level Data Loss (RPO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events requiring restoring from backup because standby database does not exist:</td>
<td>Minutes to hours</td>
<td>Minutes to hours</td>
<td>15 minutes</td>
</tr>
<tr>
<td>• Data corruptions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Full database failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Complete storage failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability domain or region failures</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the preceding table, the amount of downtime for events requiring restoring from a backup varies due to the nature of the failure. In the most optimistic case, a physical block corruption is detected and the block is repaired with block media recovery in minutes. In this case, only a small portion of the database is affected with zero data loss.

In a more pessimistic case, an availability domain or data region fails, and a new cluster must be provisioned and restored with the latest database backup, including all archives, and a complete database recovery must be run. Data loss is limited by the last successful archive log backup, the frequency of which is every 15 minutes, by default, and includes a log switch and subsequent archive log backup of any redo that has not been backed up to Oracle Cloud Infrastructure Object Storage. Data loss can be seconds or, at worst, around 15 minutes.

**Autonomous Data Guard for Autonomous Databases on Dedicated Exadata Infrastructure**

Enable Autonomous Data Guard for mission-critical production databases that have more strict uptime requirements than databases with the default high-availability configuration and limited data-loss tolerance considering a wider range of potential problems, such as data corruption and database and regional site failures. Enabling Autonomous Data Guard adds one symmetric standby database with Oracle Data Guard to an Exadata rack that is located in another availability domain or in another region.

The primary and standby database systems are configured symmetrically to ensure that performance service levels are maintained after Data Guard role transitions. Oracle Data Guard features asynchronous redo transport (maximum performance mode) within the same region across availability domains, or across regions, by default. If zero data loss is required, then you can change to synchronous redo transport (maximum availability mode).

As with databases that are not Data Guard-enabled, each Autonomous Database application service resides in at least one Oracle RAC instance and will automatically fail over to another available Oracle RAC instance, as previously described. The standby database provides expanded application services to offload reporting, queries, and some updates. The Database Backup Cloud Service schedules automated backups, which are stored in Oracle Cloud Infrastructure Object Storage and replicated to another availability domain. Those backups can be used to restore databases in the event of a double disaster where both primary and standby databases are lost.

Local and remote virtual cloud network peering provides a secure, high-bandwidth network across availability domains and regions for any traffic between primary and standby servers.

The uptime service-level objective per month is 99.995% (maximum 132 seconds of downtime per month) and recovery-time objectives (downtime) and recovery-point objectives (data loss) are low, as described in the subsequent table, when a manual failover is initiated. When you use Maximum Availability Architecture best practices for continuous service, most months would have an effective downtime of zero. The uptime service-level objective does not include downtime as a result of user-initiated high availability tests, user-initiated Data Guard switchover tests, or the time it takes to initiate a manual Data Guard failover.

Users can choose whether their database failover site is located in a different availability domain within the same region or in a different region, contingent upon application or business requirements, and data center availability.
**Autonomous Data Guard Recovery Time (RTO) and Recovery Point (RPO) Service-level Objectives**

<table>
<thead>
<tr>
<th>Failure and Maintenance Events</th>
<th>Service-Level Downtime (RTO)</th>
<th>Potential Service-Level Data Loss (RPO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localized events, including:</td>
<td>Near zero</td>
<td>Zero</td>
</tr>
<tr>
<td>• Exadata cluster network fabric failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Storage (disk and flash) failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Database instance failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Database server failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Periodic software and hardware maintenance updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events requiring failover to the standby database using Autonomous Data Guard-enabled dedicated Autonomous Databases, including:</td>
<td>Few seconds to two minutes</td>
<td>• Zero for maximum availability protection mode (uses synchronous redo transport). Most commonly used for intra-region standby databases.</td>
</tr>
<tr>
<td>• Data corruptions (because Data Guard has automatic block repair for physical corruptions, a failover operation is required only for logical corruptions or extensive data corruptions)</td>
<td></td>
<td>• Near zero for maximum performance protection mode (uses asynchronous redo transport). Most commonly used for cross-region standby databases.</td>
</tr>
<tr>
<td>• Full database failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Complete storage failures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Availability domain or region failures</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Maintaining Application Uptime**

Ensure that network connectivity to Oracle Cloud Infrastructure is reliable so that you can access your tenancy's Autonomous Database resources.

Follow the guidelines in the [Continuous Availability: Best Practices for Applications Using Autonomous Database - Dedicated](#) and [Application Continuity: MAA Checklist for Preparation](#) white papers to experience application-level service uptime similar to that of the database uptime.

**Oracle Maximum Availability Architecture in Exadata DB Systems**

Oracle Maximum Availability Architecture in Oracle Cloud Infrastructure provides inherent high availability, data protection, and disaster recovery protection integrated with both cloud automation and lifecycle operations, enabling Oracle Cloud Infrastructure to be the best cloud solution for enterprise databases and applications.

**Oracle Maximum Availability Architecture Benefits in Oracle Cloud**

- **Deployment**: Oracle deploys Exadata in Oracle Cloud Infrastructure using Oracle Maximum Availability Architecture best practices, including configuration best practices for storage, network, operating system, Oracle Grid Infrastructure, and Oracle Database. Exadata is optimized to run enterprise Oracle Databases with extreme scalability and availability.

- **Oracle Maximum Availability Architecture database templates**: All cloud databases created with Oracle Cloud automation use Oracle Maximum Availability Architecture settings optimized for the Exadata in Oracle Cloud. Oracle does not recommend that you use custom scripts to create cloud databases.

- **Backup and restore automation**: When you configure automatic backup to Oracle Cloud Infrastructure Object Storage, backup copies exist across multiple availability domains for additional protection, and RMAN validates
cloud database backups for any physical corruptions. Database backups occur daily with a full backup occurring once per week and incremental backups occurring on all other days. Archive log backups occur frequently to reduce potential data loss in case of disaster.

- **Exadata inherent benefits**: Exadata is the best Oracle Maximum Availability Architecture platform that Oracle offers, engineered with hardware, software, database, and availability innovations to support the most mission-critical enterprise applications. Specifically, Exadata provides unique high availability, data protection, and quality-of-service capabilities that set Oracle apart from any other platforms or cloud vendor.

For a comprehensive list of Oracle Maximum Availability Architecture benefits for Exadata DB systems, see [Exadata Database Machine: Maximum Availability Architecture Best Practices](http://example.com) and [Deploying Oracle Maximum Availability Architecture with Exadata Database Machine](http://example.com). Examples of these benefits include:

- **High availability and low brownout**: Fully-redundant, fault-tolerant hardware exists in the storage, network, and database servers. Resilient, highly-available software, such as Oracle Real Application Clusters (Oracle RAC), Oracle Clusterware, Oracle Database, Oracle Automatic Storage Management, Oracle Linux, and Oracle Exadata Storage Server enable applications to maintain application service levels through unplanned outages and planned maintenance events. For example, Exadata has instant failure detection that can detect and repair database node, storage server, and network failures in less than two seconds, and resume application and database service uptime and performance. Other platforms can experience 30 seconds, or even minutes, of blackout and extended application brownouts for the same type of failures. Only the Exadata platform offers a wide range of unplanned outage and planned maintenance tests to evaluate end-to-end application and database brownouts and blackouts.

- **Data protection**: Exadata provides Oracle Database physical and logical block corruption prevention, detection, and, in some cases, automatic remediation. The Exadata Hardware Assisted Resilient Data (HARD) checks include support for server parameter files, control files, log files, Oracle data files, and Oracle Data Guard broker files when those files are stored in Exadata storage. This intelligent Exadata storage validation stops corrupted data from being written to disk when a HARD check fails, which eliminates a large class of failures that the database industry had previously been unable to prevent. Examples of the Exadata HARD checks include:

  - Redo and block checksum
  - Correct log sequence
  - Block type validation
  - Block number validation
  - Oracle data structures, such as block magic number, block size, sequence number, and block header and tail data structures

Exadata HARD checks initiate from Exadata storage software (cell services) and work transparently after enabling a database `DB_BLOCK_CHECKSUM` parameter, which is enabled by default in the cloud. Exadata is the only platform that currently supports the HARD initiative. Furthermore, Oracle Exadata Storage Server provides non-intrusive, automatic hard disk scrub and repair. This feature periodically inspects and repairs hard disks during idle time. If bad sectors are detected on a hard disk, then Oracle Exadata Storage Server automatically sends a request to Oracle Automatic Storage Management to repair the bad sectors by reading the data from another mirror copy. Finally, Exadata and Oracle Automatic Storage Management can detect corruptions as data blocks are read into the buffer cache and automatically repair data corruption with a good copy of the data block on a subsequent database write. This inherent intelligent data protection makes Exadata and Exadata Cloud the best data protection storage platform for Oracle Databases. For comprehensive data protection, a Maximum Availability Architecture best practice is to use a standby database on a separate Exadata to detect, prevent, and automatically repair corruptions that cannot be addressed by Exadata, alone. The standby database also minimizes downtime and data loss for disasters that result from site, cluster, and database failures.

- **Response time quality of service**: Only Exadata has end-to-end quality-of-service capabilities to ensure that response time remains low and optimum. Database server I/O capping and Exadata storage I/O latency capping ensures that read or write I/O can be redirected to partnered cells when response time exceeds a certain threshold. If storage becomes unreliable (but not failed) because of poor and unpredictable performance, then the disk or flash cache can be quarantined, offline, and later brought back online if heuristics show that I/O performance is back to acceptable levels. Resource management can help prioritize...
key database network or I/O functionality, so that your application and database perform at an optimized level. For example, database log writes get priority over backup requests on the Exadata network and storage. Furthermore, rapid response time is maintained during storage software updates by ensuring that partner flash cache is warmed so flash misses are minimized.

- **End-to-end testing and holistic health checks**: Because Oracle owns the entire Exadata Cloud infrastructure, end-to-end testing and optimizations benefit every Exadata customer around the world, whether hosted on premise or in the cloud. Validated optimizations and fixes required to run any mission-critical system are uniformly applied after rigorous testing. Health checks are designed to evaluate the entire stack. The Exadata health check utility **EXACHK** is Exadata cloud-aware and highlights any configuration and software alerts that may have occurred because of customer changes. No other cloud platform currently has this kind of end-to-end health check available. For Oracle Autonomous Database, **EXACHK** runs automatically to evaluate Maximum Availability Architecture compliance. For non-autonomous databases, Oracle recommends running **EXACHK** at least once a month, and before and after any software updates, to evaluate any new best practices and alerts.

- **Oracle Maximum Availability Architecture best practices paper**: Oracle Maximum Availability Architecture engineering collaborates with Oracle Cloud teams to integrate Oracle Maximum Availability Architecture practices that are optimized for Oracle Cloud Infrastructure and security. See **MAA Best Practices for the Oracle Cloud** for additional information about continuous availability, Oracle Data Guard, Hybrid Data Guard, Oracle GoldenGate, and other Maximum Availability Architecture-related topics.

The following table lists various software updates and the impacts associated with those updates on databases and applications.

<table>
<thead>
<tr>
<th>Software Update</th>
<th>Database Impact</th>
<th>Application Impact</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Zero downtime</td>
<td>Zero to single-digit seconds</td>
<td>Performed by Oracle Cloud</td>
</tr>
<tr>
<td>Storage cells</td>
<td>Zero downtime</td>
<td>Zero to single-digit seconds</td>
<td>Performed by Oracle Cloud</td>
</tr>
<tr>
<td>Exadata Dom0</td>
<td>Zero downtime with Oracle RAC rolling updates</td>
<td>Zero downtime</td>
<td>Performed by Oracle Cloud</td>
</tr>
<tr>
<td>Exadata DomU</td>
<td>Zero downtime with Oracle RAC rolling updates</td>
<td>Zero downtime</td>
<td>Performed by Oracle Cloud for Autonomous Database</td>
</tr>
<tr>
<td>Oracle Database quarterly update or patch</td>
<td>Zero downtime with Oracle RAC rolling updates</td>
<td>Zero downtime</td>
<td>Performed by Oracle Cloud for Autonomous Database</td>
</tr>
<tr>
<td>Oracle Grid Infrastructure quarterly update, patch, or upgrade</td>
<td>Zero downtime with Oracle RAC rolling updates</td>
<td>Zero downtime</td>
<td>Performed by Oracle Cloud for Autonomous Database</td>
</tr>
</tbody>
</table>
### Achieving Continuous Availability for your Applications

As part of Exadata Cloud, all software updates (except for non-rolling database upgrades) can be done online or with Oracle RAC rolling updates to achieve continuous database uptime. Furthermore, any local failures of the storage, Exadata network, or Exadata database server are managed, automatically, and database uptime is maintained.

To achieve continuous application uptime during Oracle RAC switchover or failover events, follow these application-configuration best practices:

- Use non-default Oracle Clusterware-managed services to connect your application.
- Use recommended connection string with built-in timeouts, retries, and delays, so that incoming connections do not see errors during outages.
- Configure your connections with Fast Application Notification.
- Drain and relocate services prior to any planned maintenance outage on Exadata that requires restarting any of the Oracle RAC instances. Software updates to Exadata Dom0 or DomU are automatic. For Oracle Database and Oracle Grid Infrastructure software updates, Exadata Cloud-assisted tools and Autonomous Database drain and relocate services automatically.
- Leverage Application Continuity or Transparent Application Continuity to replay in-flight uncommitted transactions transparently after failures.

For more information, see [Continuous Availability: Best Practices for Applications Using Autonomous Database - Dedicated](#) and [Application Continuity: MAA Checklist for Preparation](#) white papers to experience application-level service uptime similar to that of the database uptime.

### Oracle Maximum Availability Architecture Reference Architectures in the Exadata Cloud

Exadata Cloud supports all four Oracle Maximum Availability Architecture reference architectures, providing support for all Oracle Databases, regardless of their specific high availability, data protection, and disaster recovery service-level agreements. See [MAA Best Practices for the Oracle Cloud](#) for more information about Oracle Maximum Availability Architecture in the Exadata Cloud.

### Security Zone Integration

This topic describes the Database service's support of security zones. Security zones are compartments in your tenancy created with a set of security policies called a security recipe. This topic concentrates on the Oracle-managed Maximum Security Recipe, which provides the highest level of protection for your Database resources. The policies of a particular security recipe are applied to any resource that is provisioned or moved into a security zone compartment that uses the recipe. Thus, the only way to apply security zone policies is to control the compartment assignments of your Oracle Cloud Infrastructure resources.

For a complete overview of security zones, see the Security Zone section of the Oracle Cloud Infrastructure user guide.

### Restrictions on Database Service Resources Located in Maximum Security Recipe Compartments

The Maximum Security Recipe includes all available security zone policies. For example, restrictions placed on a databases in a Maximum Security Recipe compartments include:
• The database cannot allow public network access
• The database must have automatic backups enabled
• The database cannot have Data Guard associations that aren’t located in security zone compartments

For a complete list of the Database restrictions implemented by the Maximum Security Recipe, see the Security Zone Policies topic.

Supported Database Service Resources

The following Database service resources can be provisioned and managed in security zones that use the Maximum Security Recipe:

• Autonomous Database: Databases using dedicated Exadata infrastructure and using shared Exadata infrastructure with private endpoint access
• Bare metal and virtual machine DB systems
• Exadata Cloud DB systems

Always Free Autonomous Databases, Autonomous Database configured with public endpoints, and the Exadata Cloud@Customer service are not compatible with Maximum Security Recipe compartments.

DB System Time Zone

The Time Zone field in the Console and in the API allows you to launch a bare metal, virtual machine, or Exadata DB system with a time zone other than UTC (the default). Although UTC is the recommended time zone to use, having a common time zone for your database clients and application hosts can simplify management and troubleshooting for the database administrator.

The time zone that you specify when you create the DB system applies to the host and to the Oracle Grid Infrastructure (if the system has Grid Infrastructure), and controls the time zone of the database log files. The time zone of the database itself is not affected, however, the database’s time zone affects only the timestamp datatype. You can change the database time zone manually but Oracle recommends that you keep it as UTC (the default) to avoid data conversion and improve performance when data is transferred among databases. This configuration is especially important for distributed databases, replication, and export and import operations.

Time Zone Options

Whether you use the Console or the API, the time zone options you can select from are represented in the named region format, for example, America/Los_Angeles. The Console allows you to select UTC, the time zone detected in your browser (if your browser supports time zone detection), or an alternate time zone.

To specify an alternate time zone (the Select another time zone option), you first select a value in the Region or country field to narrow the list of time zones to select from in the Time zone field. In the America/Los_Angeles example, America is the time region and Los_Angeles is the time zone. The options you see in these two fields roughly correlate with the time zones supported in both the Java.util.TimeZone class and on the Linux operating system. If you do not see the time zone you are looking for, try selecting "Miscellaneous" in the Region and country field.

Tip:

If you are using the API and would like to see a list of supported time zones, you can examine the time zone options in the Console. These options appear on the Create DB System page when you show advanced options after you select a DB system shape.

Changing Time Zones After Provisioning

Follow these steps if you need to change the time zone of the DB system host, Oracle Grid Infrastructure, or database, after you launch the DB system:
To change the time zone of the host on DB systems that use Grid Infrastructure

1. Log on to the host system as root.
2. Stop the CRS stack on all of the compute nodes.

   #Grid_Home/bin/crsct1 stop crs

3. Run the following commands to check the current time zone and to change it to the time zone you choose:

   $ cat /etc/sysconfig/clock
   ZONE="America/New_York"
   $ cp -p /etc/sysconfig/clock /etc/sysconfig/clock.20160629
   $ vi /etc/sysconfig/clock
   ZONE="Europe/Berlin"
   $ date
   Wed Jun 29 10:35:17 EDT 2016
   $ ln -sf /usr/share/zoneinfo/Europe/Berlin /etc/localtime
   $ date
   Wed Jun 29 16:35:27 CEST 2016

   In this example, the time zone was changed from America/New_York to Europe/Berlin.

   Tip:
   To see a list of valid time zones on the host, you can run the ls -l /usr/share/zoneinfo command.

4. (Optional) On an Exadata DB system, you can verify that /opt/oracle.cellos/cell.conf indicates the correct time zone. Using our example, the time zone entry in this file would be <Timezone>Europe/Berlin</Timezone>.
5. Restart the CRS stack on all of the compute nodes.

   #Grid_Home/bin/crsct1 start crs

To change the time zone of the host on DB systems that use Logical Volume Manager

Use this procedure for Fast Provisioned virtual machine DB systems, which use Logical Volume Manager instead of Grid Infrastructure for storage management.

1. Log on to the host system as root.
2. Stop the database and the listener on all of the compute nodes.

   #sqlplus / as sysdba
   SQL> shutdown immediate
   #lsnrctl stop

3. Stop all other running processes from the Oracle Database Home.
4. Run the following commands to check the current time zone and to change it to the time zone you choose:

   $ cat /etc/sysconfig/clock
   ZONE="America/New_York"
   $ cp -p /etc/sysconfig/clock /etc/sysconfig/clock.20160629
   $ vi /etc/sysconfig/clock
   ZONE="Europe/Berlin"
   $ date
   Wed Jun 29 10:35:17 EDT 2016
   $ ln -sf /usr/share/zoneinfo/Europe/Berlin /etc/localtime
In this example, the time zone was changed from *America/New_York* to *Europe/Berlin*.

Tip:

To see a list of valid time zones on the host, you can run the `ls -l /usr/share/zoneinfo` command.

5. As Oracle, restart the listener and the database on all of the compute nodes.

```
lsnrctl start
sqlplus / as sysdba
startup
```

**To change the time zone of the Oracle Grid Infrastructure**

The time zone of the Oracle Grid Infrastructure determines the time zone of the database log files.
You can change this time zone by updating the `TZ` property in the `GRID_HOME/crs/install/s_crsconfig_<node_name>_env.txt` configuration file.

Note:

This procedure does not apply to Fast Provisioned virtual machine DB systems, which use Logical Volume Manager instead of Grid Infrastructure for storage management.

1. Ensure that you are logged onto the host as `root` and that the CRS stack is stopped on all of the compute nodes. See To change the time zone of the host on DB systems that use Grid Infrastructure on page 1576.
2. Inspect the current time zone value in the `GRID_HOME/crs/install/s_crsconfig_<node_name>_env.txt` file.

```
$ cat /u01/app/19.0.0.0/grid/crs/install/s_crsconfig_node1_env.txt
#########################################################################
#This file can be used to set values for the NLS_LANG and TZ environment variables and to set resource limits for Oracle Clusterware and Database processes.
#1. The NLS_LANG environment variable determines the language and characterset used for messages. For example, a new value can be configured by setting NLS_LANG=JAPANESE_JAPAN.UTF8
#2. The Time zone setting can be changed by setting the TZ entry to the appropriate time zone name. For example, TZ=America/New_York
#3. Resource limits for stack size, open files and number of processes can be specified by modifying the appropriate entries.
#
#Do not modify this file except as documented above or under the direction of Oracle Support Services.
#########################################################################
TZ=UTC
NLS_LANG=AMERICAN_AMERICA.WE8ISO8859P1
CRS_LIMIT_STACK=2048
CRS_LIMIT_OPENFILE=65536
CRS_LIMIT_NPROC=16384
TNS_ADMIN=
```

In this example, the time zone is set to UTC.

3. Modify the time zone value, as applicable. Perform this task for all nodes in the cluster.
4. Restart the CRS stack on all of the compute nodes.

```
#Grid_Home/bin/crsctl start crs
```
For more information about changing the time zone of the Grid Infrastructure, see How To Change Timezone for Grid Infrastructure (Doc ID 1209444.1).

To change the time zone of a database

Use the `ALTER DATABASE SET TIME_ZONE` command to change the time zone of a database. This command takes either a named region such as America/Los_Angeles or an absolute offset from UTC.

This example sets the time zone to UTC:

```
ALTER DATABASE SET TIME_ZONE = '+00:00';
```

You must restart the database for the change to take effect. For more information, see Setting the Database Time Zone.

Database Metrics

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure Database service resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

The Database service metrics help you measure useful quantitative data, such as CPU and storage utilization, the number of successful and failed database logon and connection attempts, database operations, SQL queries, and transactions, and so on. You can use metrics data to diagnose and troubleshoot problems with your Database Service resources.

See the following topics for information about currently available database metrics:

- Autonomous Database Metrics on page 1578
- External Database Metrics on page 1589

Prerequisites

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Autonomous Database Metrics

This topic describes the metrics emitted by the Database service in the oci_autonomous_database namespace.

Resources: Autonomous Databases.

For a complete list of available metrics for Autonomous Databases, see Available Metrics: oci_autonomous_database on page 1579.

To view a default set of metrics charts in the Console, navigate to the Autonomous Database that you're interested in, and then click Metrics. You also can use the Monitoring service to create custom queries.
Database

**Available Metrics: oci_autonomous_database**

The metrics listed in the following table are automatically available for any Autonomous Database that you create. You do not need to enable monitoring on the resource to get these metrics.

<table>
<thead>
<tr>
<th>Note:</th>
<th>Valid alarm intervals are 5 minutes or greater due to the frequency at which these metrics are emitted. See To create an alarm for details on creating alarms.</th>
</tr>
</thead>
</table>

Database service metrics for Autonomous Databases include the following *dimensions*:

**AUTONOMOUSDBTYPE**

The type of Autonomous Database, Autonomous Data Warehouse (ADW) or Autonomous Transaction Processing (ATP).

**deploymentType**

The Exadata infrastructure type, shared or dedicated. When using the Console to view default metric charts for multiple Autonomous Databases, you must specify this dimension.

**DISPLAYNAME**

The friendly name of the Autonomous Database.

**REGION**

The region in which the Autonomous Database resides.

**RESOURCEID**

The OCID of the Autonomous Database.

**RESOURCENAME**

The name of the Autonomous Database.

In the following table, metrics that are marked with an asterisk (*) can be viewed only on the Service Metrics page of the Oracle Cloud Infrastructure Console. All metrics can be filtered by the dimensions described in this topic. Note that some metrics are only available for Autonomous Databases using either shared Exadata infrastructure or dedicated Exadata infrastructure. This is indicated in the Applicable Exadata Infrastructure Type column.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Applicable Exadata Infrastructure Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApplyLag</td>
<td>Apply Lag</td>
<td>seconds</td>
<td>This metric displays (in seconds) how far the standby database is behind the primary database as of the time sampled.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>BlockChanges</td>
<td>DB Block Changes</td>
<td>changes per second</td>
<td>The average number of blocks changed per second.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>ConnectionLatency</td>
<td>Connection Latency</td>
<td>millisecond</td>
<td>The time taken to connect to a Autonomous Database that uses shared Exadata infrastructure in each region from a Compute service virtual machine in the same region.</td>
<td>Shared only</td>
</tr>
<tr>
<td>CpuTime*</td>
<td>CPU Time</td>
<td>seconds per second</td>
<td>Average rate of accumulation of CPU time by foreground sessions in the database over the time interval. The CPU time component of Average Active Sessions.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>CpuUtilization</td>
<td>CPU Utilization</td>
<td>percent</td>
<td>The CPU usage expressed as a percentage, aggregated across all consumer groups. The utilization percentage is reported with respect to the number of CPUs the database is allowed to use, which is two times the number of OCPUs.</td>
<td>Both</td>
</tr>
<tr>
<td>CurrentLogons*</td>
<td>Current Logons</td>
<td>count</td>
<td>The number of successful logons during the selected interval.</td>
<td>Both</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>DBTime*</td>
<td>DB Time</td>
<td>seconds per second</td>
<td>The amount of time database user sessions spend executing database code (CPU Time + WaitTime). DB Time is used to infer database call latency, because DB Time increases in direct proportion to both database call latency (response time) and call volume. It is calculated as the average rate of accumulation of database time by foreground sessions in the database over the time interval. Also known as Average Active Sessions.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>ExecuteCount</td>
<td>Execute Count</td>
<td>count</td>
<td>The number of user and recursive calls that executed SQL statements during the selected interval.</td>
<td>Both</td>
</tr>
<tr>
<td>FailedConnections</td>
<td>Failed Connections</td>
<td>count</td>
<td>The number of failed database connections.</td>
<td>Shared only</td>
</tr>
<tr>
<td>FailedLogons</td>
<td>Failed Logons</td>
<td>count</td>
<td>The number of log ons that failed because of an invalid user name and/or password, during the selected interval.</td>
<td>Shared only</td>
</tr>
<tr>
<td>IOPS</td>
<td>IOPS</td>
<td>operations per second</td>
<td>The average number of I/O operations per second.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>IOTThroughput</td>
<td>IO Throughput</td>
<td>MB per second</td>
<td>The average throughput in MB per second.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>LogicalBlocksRead</td>
<td>Logical Reads</td>
<td>reads per second</td>
<td>The average number of logical block reads (&quot;db block gets&quot; plus &quot;consistent gets&quot;) per second. Includes buffered and direct I/O.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>OCPUsAllocated</td>
<td>OCPU Allocated</td>
<td>integer</td>
<td>The actual number of OCPUs allocated by the service during the selected interval of time.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>ParsesByType</td>
<td>Parses By Type</td>
<td>parses per second</td>
<td>The number of hard or soft parses per second.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>ParseCount*</td>
<td>Parse Count (Total)</td>
<td>count</td>
<td>The number of hard and soft parses during the selected interval.</td>
<td>Both</td>
</tr>
<tr>
<td>QueryLatency</td>
<td>Query Latency</td>
<td>millisecond</td>
<td>The time taken to display the results of a simple query on the user's screen.</td>
<td>Shared only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>QueuedStatements</td>
<td>Queued Statements</td>
<td>count</td>
<td>The number of queued SQL statements, aggregated across all consumer groups, during the selected interval.</td>
<td>Both</td>
</tr>
<tr>
<td>RedoSize</td>
<td>Redo Generated</td>
<td>MB per second</td>
<td>The Average amount of redo generated in MB per second.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>RunningStatements</td>
<td>Running Statements</td>
<td>count</td>
<td>The number of running SQL statements, aggregated across all consumer groups, during the selected interval.</td>
<td>Both</td>
</tr>
<tr>
<td>Sessions</td>
<td>Sessions</td>
<td>count</td>
<td>The number of sessions in the database.</td>
<td>Both</td>
</tr>
<tr>
<td>StorageAllocated</td>
<td>Storage Space Allocated</td>
<td>GB</td>
<td>Maximum amount of space allocated to the database during the interval.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>------</td>
<td>-------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>StorageAllocatedByTablespace*</td>
<td>Allocated Storage Space By Tablespace</td>
<td>GB</td>
<td>Maximum amount of space allocated for each tablespace during the interval.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>StorageUsed*</td>
<td>Storage Space Used</td>
<td>GB</td>
<td>Maximum amount of space used during the interval.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>StorageUsedByTablespace*</td>
<td>Storage Space Used By Tablespace</td>
<td>GB</td>
<td>Maximum amount of space used by each tablespace during the interval.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>StorageUtilization</td>
<td>Storage Utilization</td>
<td>percent</td>
<td>The percentage of provisioned storage capacity currently in use. Represents the total allocated space for all tablespaces.</td>
<td>Both</td>
</tr>
<tr>
<td>StorageUtilizationByTablespace*</td>
<td>Storage Space Utilization By Tablespace</td>
<td>percent</td>
<td>The percentage of space utilized by each tablespace.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Applicable Exadata Infrastructure Type</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>TransactionsByStatus</td>
<td>Transactions By Status</td>
<td>transactions per second</td>
<td>The number of committed or rolled back transactions per second.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>TransactionCount*</td>
<td>Transaction Count</td>
<td>count</td>
<td>The combined number of user commits and user rollbacks during the selected interval.</td>
<td>Both</td>
</tr>
<tr>
<td>TransportLag</td>
<td>Transport Lag</td>
<td>seconds</td>
<td>The approximate number of seconds of redo not yet available on the standby database as of the time sampled.</td>
<td>Dedicated only</td>
</tr>
<tr>
<td>UserCalls*</td>
<td>User Calls</td>
<td>count</td>
<td>The combined number of logons, parses, and execute calls during the selected interval.</td>
<td>Both</td>
</tr>
</tbody>
</table>
### Metric Display Name

**WaitTime**

**Metric**

**Wait Time**

**Unit**

seconds per second

**Description**

Average rate of accumulation of non-idle wait time by foreground sessions in the database over the time interval. The wait time component of Average Active Sessions.

**Applicable Exadata Infrastructure Type**

Dedicated only

---

**Using the Console**

**To view default metric charts for a single Autonomous Database**

1. Open the navigation menu. Under **Oracle Database**, click **Autonomous Data Warehouse**, **Autonomous JSON Database**, or **Autonomous Transaction Processing**.
2. Choose the **Compartment** that contains the Autonomous Database you want to view, and then click display name of the database to view its details.
3. Under **Resources**, click **Metrics**.

   The **Metrics** page displays a default set of charts for the current Autonomous Database. See **Available Metrics: oci_autonomous_database** on page 1579 for information about the default charts.

   For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**To view default metric charts for multiple Autonomous Databases**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. For **Compartment**, select the compartment that contains the Autonomous Databases that you're interested in.
3. For **Metric Namespace**, select **oci_autonomous_database**.

   The **Service Metrics** page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

4. For **Dimensions**, specify an Exadata infrastructure deployment type (shared or dedicated). **Important**: If you do not specify a deployment type, no service metrics will display on the page.

   Optionally, you can specify other dimensions to filter your displayed metrics. See **To filter results** on page 2673 and **To select different resources** on page 2673 in the Monitoring documentation for more information.

   **Tip:**

   If there are multiple Autonomous Databases in the compartment, the charts default to show a separate line for each master encryption key. You can
instead show a single line aggregated across all Autonomous Databases in the compartment by selecting the Aggregate Metric Streams check box.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

## External Database Metrics

This topic describes the metrics emitted by the Database service in the `oracle_external_database` namespace.

Resources: External Databases.

To view a default set of metrics charts in the Console, navigate to the external database that you're interested in, and then click Metrics. You also can use the Monitoring service to create custom queries.

### Available Metrics: `oracle_external_database`

The metrics listed in the following table are automatically available for external databases.

<table>
<thead>
<tr>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Collection Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AllocatedStorageUtilizationByTablespace</strong></td>
<td>percent</td>
<td>Percentage of space used by tablespace out of allocated. <em>Not applicable to external container databases.</em></td>
<td>30 minutes</td>
</tr>
<tr>
<td><strong>BlockChanges</strong></td>
<td>changes per second</td>
<td>The average number of blocks changed per second.</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

Database service metrics for external databases include the following dimensions:

- **DISPLAYNAME**
  - The friendly name of the external database.

- **REGION**
  - The `region` in which the OCI external database resource resides.

- **RESOURCEID**
  - The `OCID` of the external database.

- **RESOURCENAME**
  - The name of the external database.

In the following table, metrics that are marked with an asterisk (*) can be viewed only on the Service Metrics page of the Oracle Cloud Infrastructure Console. All metrics can be filtered by the dimensions described in this topic.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Collection Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>CpuCount*</td>
<td>CPU Count</td>
<td>CPU</td>
<td>Container and non-container databases: The value of the cpu_count parameter, if set; otherwise, the value of num_cpus for the database host. Pluggable databases: The value of the cpu_count parameter if set. Otherwise the value of the cpu_count parameter of the associated container database (if set), or the num_cpus value of the database host if the cpu_count of the container database is not set.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>CpuTime*</td>
<td>CPU Time</td>
<td>seconds per second</td>
<td>Average rate of accumulation of CPU time by foreground sessions in the database over the time interval. The CPU time component of Average Active Sessions.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>CpuUtilization</td>
<td>CPU Utilization</td>
<td>percent</td>
<td>The CPU usage expressed as a percentage, aggregated across all consumer groups. The utilization percentage is reported with respect to the number of CPUs the database is allowed to use, which is two times the number of OCPUs.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>CurrentLogons</td>
<td>Current Logons</td>
<td>count</td>
<td>The number of successful logons during the selected interval.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Collection Frequency</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>DBTime</td>
<td>DB Time</td>
<td>seconds per second</td>
<td>The amount of time database user sessions spend executing database code (CPU Time + WaitTime). DB Time is used to infer database call latency, because DB Time increases in direct proportion to both database call latency (response time) and call volume. It is calculated as the average rate of accumulation of database time by foreground sessions in the database over the time interval. Also known as Average Active Sessions.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>ExecuteCount</td>
<td>Execute Count</td>
<td>count</td>
<td>The number of user and recursive calls that executed SQL statements during the selected interval.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>IOPS*</td>
<td>IOPS</td>
<td>operations per second</td>
<td>The average number of I/O operations per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>IOThroughput*</td>
<td>IO Throughput</td>
<td>MB per second</td>
<td>The average throughput in MB per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>LogicalBlocksRead</td>
<td>Logical Reads</td>
<td>reads per second</td>
<td>The average number of logical block reads (&quot;db block gets&quot; plus &quot;consistent gets&quot;) per second. Includes buffered and direct I/O.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>MaxTablespaceSize</td>
<td>Max Tablespace Size</td>
<td>GB</td>
<td>Maximum possible tablespace size. Not applicable to external container databases.</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Collection Frequency</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>MemoryUsage*</td>
<td>Memory Usage</td>
<td>MB</td>
<td>The total amount of memory used by the database during the collection interval. Not applicable to external pluggable databases.</td>
<td>15 minutes</td>
</tr>
<tr>
<td>MonitoringStatus</td>
<td>Monitoring Status</td>
<td>No unit; failed status is displayed when monitoring is interrupted.</td>
<td>5 minutes</td>
<td></td>
</tr>
<tr>
<td>ParseCount*</td>
<td>Parse Count (Total)</td>
<td>count</td>
<td>The number of hard and soft parses during the selected interval.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>ParsesByType*</td>
<td>Parses By Type</td>
<td>parses per second</td>
<td>The number of hard or soft parses per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RedoSize*</td>
<td>Redo Generated</td>
<td>MB per second</td>
<td>The Average amount of redo generated in MB per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>StorageAllocated*</td>
<td>Storage Space Allocated</td>
<td>GB</td>
<td>Maximum amount of space allocated to the database during the interval.</td>
<td>30 minutes</td>
</tr>
<tr>
<td>StorageAllocatedByTablespace*</td>
<td>Storage Space By Tablespace</td>
<td>GB</td>
<td>Maximum amount of space allocated for each tablespace during the interval.</td>
<td>30 minutes</td>
</tr>
<tr>
<td>StorageUsed*</td>
<td>Storage Space Used</td>
<td>GB</td>
<td>Maximum amount of space used during the interval.</td>
<td>30 minutes</td>
</tr>
<tr>
<td>StorageUsedByTablespace*</td>
<td>Storage Space Used By Tablespace</td>
<td>GB</td>
<td>Maximum amount of space used by each tablespace during the interval.</td>
<td>30 minutes</td>
</tr>
<tr>
<td>StorageUtilization</td>
<td>Storage Utilization</td>
<td>percent</td>
<td>The percentage of provisioned storage capacity currently in use. Represents the total allocated space for all tablespaces.</td>
<td>30 minutes</td>
</tr>
</tbody>
</table>
### Metric Display Name

<table>
<thead>
<tr>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Collection Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>StorageUtilization</td>
<td>percent</td>
<td>The percentage of space utilized by each tablespace. <em>Not applicable to external container databases.</em></td>
<td>30 minutes</td>
</tr>
<tr>
<td>TransactionCount</td>
<td>count</td>
<td>The combined number of user commits and user rollbacks during the selected interval.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TransactionsByStatus</td>
<td>transactions per second</td>
<td>The number of committed or rolled back transactions per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>UserCalls</td>
<td>count</td>
<td>The combined number of logons, parses, and execute calls during the selected interval.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>WaitTime</td>
<td>seconds per second</td>
<td>Average rate of accumulation of non-idle wait time by foreground sessions in the database over the time interval. The wait time component of Average Active Sessions.</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

### Using the Console

**To view default metric charts for a single External Database**

1. Open the . Under , click .
2. Choose the **Compartment** that contains the External Database you want to view, and then click display name of the database to view its details.
3. Under **Resources**, click **Metrics**.

The **Metrics** page displays a default set of charts for the current External Database. See [Available Metrics: oracle_external_database](#) on page 1589 for information about the default charts.

For more information about monitoring metrics and using alarms, see [Monitoring Overview](#) on page 2660. For information about notifications for alarms, see [Notifications Overview](#) on page 3350.

**To create metrics queries for all available external database metrics using the Monitoring Service’s Metrics Explorer tool**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Click **Metrics Explorer**. Note: external database metrics are not available in the **Service Metrics** tab. For information on building queries in the Metrics Explorer tab, see [Building Metric Queries](#) on page 2700.
3. Create a metrics query:
   - For **Compartment**, select the compartment that contains the external databases that you're interested in.
   - For **Metric Namespace**, select `oracle_external_database`.
   - Select a **Metric name**. See Available Metrics: `oracle_external_database` on page 1589 for definitions of each metric.
   - Select an **Interval**. See Available Metrics: `oracle_external_database` on page 1589 for information on the collection frequency of each external database metric.
   - Select the **Statistic** type. This is the aggregation function applied for converting a set of data points. Available functions include count, max, mean, rate, min, sum, and percentile.
   - Select a **Metric dimension**. Dimensions are used to filter metric data. For example, by choosing the "resourceID" dimension, you can specific a single external database by selecting the OCID of the OCI external database resource.

4. Click **Update Chart** after configuring your query.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

Using the Oracle Database Service Overview to Manage Resources

This topic describes the **Overview** page in the Oracle Database section of the Oracle Cloud Infrastructure Console. The Overview page gives you a way to view and manage all of your tenancy's Oracle Database resources using a single dashboard tool. The Overview provides information on all of your work request activity, alarms, announcements and more, regardless of whether the databases use Autonomous Database, bare metal, virtual machine, Exadata Cloud, or Exadata Cloud@Customer infrastructure.

**Resource Summary Section**

The resource summary tiles provide you with details on how many Oracle Databases you have currently provisioned in your tenancy. The Autonomous Database tile provides total numbers of databases by workload type and infrastructure type.

![279 Autonomous Databases](image)

The Databases tile provides total numbers of bare metal, or virtual machine databases by database edition type, total numbers of Exadata databases by infrastructure type.
At the bottom of each tile are messages reporting whether or not usage of the resources listed in the column are near or at service limits for the tenancy. For resources that are near or at service limits, you can request a service limit increase.

**Operations Section**

The tiles for alarms, activity, announcements, and service health allow you to quickly assess whether any of your Oracle Database resources need attention, how normal operations are proceeding, and if there are service-related announcements you need to know about to effectively manage your resources.

"The Alarms tile displays the Oracle Cloud Infrastructure Monitoring service alarms for your Database service resources. You can click the alarm icon in the Alarms tile to navigate to detailed information about the alarms. In the list view of your tenancy's alarms, you can limit the list by compartment, alarm status, and alarm severity. For more information on creating and using alarms to manage your Oracle Database resources, see the Monitoring documentation.

The Activity tile displays the number of in-progress work requests for your Database service resources. Click on the tile's activity icon to navigate to a complete list of in-progress work requests in your specified compartment.

The Announcements tile displays the number of unread Oracle Database announcements for your tenancy, if any. Click the tile's announcements icon to navigate to your unread announcements. See Console Announcements on page 260 for more information on Oracle Cloud Infrastructure announcements.

The Service Health tile displays the availability status of all Oracle Database instances in the selected region, and allows you to easily navigate to the Console's Oracle Cloud Infrastructure status page to check the availability status of all Oracle Cloud Infrastructure services, by region.
What's New and Help

The What's New list provides a view of the most recent updates to the Oracle Database service. The Help list provides quick access to information about each type of Oracle Database cloud offering.

<table>
<thead>
<tr>
<th>What's New</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events for ADBS: 19c DB Version Upgrade</td>
<td>Autonomous databases</td>
</tr>
<tr>
<td>May 6, 2020</td>
<td>Bare Metal and VM DB systems</td>
</tr>
<tr>
<td>Exadata Cloud at Customer: Time Zone</td>
<td>Exadata DB Systems</td>
</tr>
<tr>
<td>May 7, 2020</td>
<td>Exadata Cloud at Customer</td>
</tr>
<tr>
<td>Exadata Cloud at Customer: Character Set and Language</td>
<td>Contact Support</td>
</tr>
<tr>
<td>May 7, 2020</td>
<td>View all release notes</td>
</tr>
<tr>
<td>View all release notes</td>
<td>View all documentation</td>
</tr>
</tbody>
</table>

To see a list of alarms for your tenancy's Oracle Database resources
1. Open the navigation menu. Under Database, click Overview.
2. Under Advanced, click Alarms.
3. Optional. Limit the scope of the list using the compartment selector under List Scope.
4. Optional. Limit the list to alarms with a particular status or severity using the available list filters.

To see a list of work requests for your tenancy's Oracle Database resources
1. Open the navigation menu. Under Database, click Overview.
2. Under Advanced, click Activity.
3. Optional. Limit the scope of the list using the compartment selector under List Scope.
4. Optional. Limit the list to work requests with a particular status or operation type using the available list filters.

To see a list of announcements for your tenancy's Oracle Database resources
1. Open the navigation menu. Under Database, click Overview.
2. Under Advanced, click Announcements.
3. Optional. Limit the list by announcement status, Oracle Database service type, announcement action type, and publication time.

To see details about your tenancy's Oracle Database resource categories that are at or near service limits
1. Open the navigation menu. Under Database, click Overview.
2. Under Advanced, click Limits.
3. Optional. Limit the scope of the information using the compartment selector under List Scope.
4. Optional. Limit the list by Oracle Database service type using the Service Type filter. This allows you to view limits information for either Autonomous Databases, co-managed databases, or Exadata infrastructure instances.
5. Optional. Limit the list to information about the Console's currently specified region, or to an availability domain within the current region, using the Scope filter.

Using Performance Hub to Analyze Database Performance

This topic describes how to use Performance Hub to analyze and tune the performance of a selected Oracle Cloud Infrastructure Autonomous Database. With this tool, you can view real-time and historical performance data. When you view historical data in the Performance Hub, you are viewing statistics collected as part of the hourly snapshots of your database.

Note:
Performance Hub supports only Autonomous Databases.

Note:
Using Identity and Access Management (IAM), you can create a policy that grants users access to Performance Hub while limiting actions they can take on an Autonomous Database. For more information, about policies and how to use them, see How Policies Work. The following example shows a policy that grants access only to performance data without allowing general use access on Autonomous Databases.

Allow group <groupname> to inspect autonomous-database-family in compartment <name>
Allow group <groupname> to use autonomous-database-family in compartment <name> where request.operation = 'RetrieveAutonomousDatabasePerformanceBulkData'

Performance Hub Features

The Performance Hub window consists of a graphical Time Range display that you use to select the time period of all data to be displayed. It includes the following tabs that display performance data:

- ASH Analytics
- SQL Monitoring
- Workload
- Blocking Sessions
- ADDM (available for databases using shared Exadata infrastructure).

These tabs, described in detail in this topic, provide information that you can use to analyze the performance of a selected database, including the following:

- How much of the database is waiting for a resource, such as CPU or disk I/O
- Whether database performance degraded over a given time period and what could be the likely cause
- Which specific modules may be causing a load on the system, and where most of database time is being spent on this module
- Which SQL statements are the key contributors to changes in database performance, and which executions are causing them
- Which user sessions are causing performance bottlenecks
- Which sessions are currently blocking and if there are outstanding requests for a lock

Time Range Selector

The time range selector is displayed at the top of the Performance Hub page. It consists of a graphically displayed time field as shown in the following illustration. The selected time range applies to all charts and graphs in the Performance Hub window.
You can hide the Activity Summary chart to save space and display only the main tab content. To do so, click the **Hide Activity Summary** checkbox that is located directly above the graph.

![Performance Hub Activity Summary](image)

**Figure 1: Performance Hub Activity Summary**

The time range field (#1 in the previous illustration) shows database activity in chart form for the specified **Time Range** period. The time range is the amount of time being monitored.

Use the **Quick Select** selector to set the time range. The menu includes five time choices, **Last Hour, Last 8 Hours, Last 24 Hours, Last Week,** and **Custom.** The default time range is Last Hour. You can also click the **Time Range** field to specify a custom time range. This opens the **Custom Time Range** dialog, allowing you to specify a custom range.

The **Activity Summary** graph displays the average number of active sessions broken down by **CPU, User I/O, and Wait.** Maximum threads are shown as a red line above the time field.

The sliding box (circled at right in the previous illustration) on the time range chart is known as the **time slider.** The time slider selects a section of the time range (#2 in the previous illustration) shown in the time range field. It shows the time being analyzed. In the illustration, the arrows inside the time slider point to the vertical 'handle' elements on the left and right boundaries of the slider box. The time slider works as follows:

- To change the start and end time of the analysis while keeping the same amount of time between them, left click anywhere inside the box. Then slide the box left or right along the time range without changing its size. The selected times are displayed below the time graph.
- To increase or decrease the length of time being analyzed, left click either one of the **handles** and drag it left or right to expand or contract the box.
- To refresh the data in Performance Hub according to the time range chosen, click **Refresh** (upper right corner of the window).

**Note:**

The time slider provides an extra display feature in the Workload tab. See the description in the Workload Tab section of this page.

Use the **Quick Select** menu to set the time duration. The menu includes the following five time choices: **Last Hour, Last 8 Hours, Last 24 Hours, Last Week,** and **Custom.** The default Time Range is Last Hour. The time slider selects the time period of the data displayed in Performance Hub. The time slider has a different default time period based on the selected Time Range.
Time Zone Selector

The Time Zone selector is located above the time range field, beside the Quick Select and Time Range selectors. By default, when you open Performance Hub, the tool displays data in UTC (Coordinated Universal Time) time. You can use the time zone selector to change the time zone to either your local web browser time, or the time zone setting of the database you are working with. When you change the time zone, the Performance Hub reports display data in your specified time zone.

ASH Analytics Tab

Displayed by default, the ASH (Active Session History) Analytics tab shows ASH analytics charts that you can use to explore ASH data. You can use this tab to drill down into database performance across multiple dimensions such as Consumer Group, Wait Class, SQL ID, and User Name. In the ASH Analytics tab, you can select an Average Active Sessions dimension and view the top activity for that dimension for the selected time period.

The Average Active Session chart has a control at the right end of the chart to select the displayed resolution of ASH data (low, medium, high, or maximum). For more information on ASH, see Active Session History (ASH) in Oracle Database Concepts.

ASH Sample Resolution

The ASH Sample Resolution menu gives users the ability to control the sampling of ASH data displayed in the Average Active Sessions chart. Data resolution means displaying more or fewer data points in the sample data in given time period. Lower resolution displays coarser data with better performance and less impact on the database. Higher resolution aggregates more data to display finer detail, but can have a corresponding cost in latency and impact on the database.

The Sample Resolution menu is displayed at the right side of the chart. The data resolution selections are:

- **Low** - the chart displays the fewest data points in the selected data sample.
- **Medium** - the chart displays more data points in the selected data sample.
- **High** - the chart displays more data points in the selected data sample.
- **Maximum** - the chart displays the most data points available in the selected data sample.

To use this feature, see To view the average active sessions data by a selected dimension on page 1602

Activity tables

By default, the two tables located below the Average Active Sessions graph display the top SQLs and user sessions for the time period covered by the Average Activity Sessions graph. Use the menus at the top left of each of the two tables to view activities by other dimensions.

SQL Monitoring Tab

The SQL Monitoring tab is not displayed by default. To view it, click SQL Monitoring on the Performance Hub page.

SQL statements are only monitored if they have been running for at least five seconds or if they are run in parallel. The table in this section displays monitored SQL statement executions by dimensions including Last Active Time, CPU Time, and Database Time. The table displays currently running SQL statements and SQL statements that completed, failed, or were terminated. The columns in the table provide information for monitored SQL statements including Status, Duration, and SQL ID.

The Status column includes the following icons:

- A spinning icon indicates that the SQL statement is executing.
- A green check mark icon indicates that the SQL statement completed its execution during the specified time period.
- A red cross icon indicates that the SQL statement did not complete. The icon displays when an error occurs because the session was terminated.
- A clock icon indicates that the SQL statement is queued.
To terminate a running or queued SQL statement, click **Kill Session**.

You can also click an SQL ID to go to the corresponding **Real-time SQL Monitoring** page. This page provides extra details to help you tune the selected SQL statement.

### Workload Tab

The Workload tab graphically displays four sets of statistics that you can use to monitor the database workload and identify spikes and bottlenecks. Each set of statistics is displayed in a separate region, as described in the following sections.

#### Monitored and analyzed time indications

The time slider has more functionality in the Workload tab than it does in the Active Session History and SQL Monitoring tabs. Note the following about the **Quick Select** time range options:

- **Last Hour**, **Last 8 Hours**, and **Last 24 Hours** - The charts in the Workload tab display data for the entire time period of specified time range. A shadowed area is displayed in each chart that corresponds to the position of the time slider in the time range.
- **Last Week** - The charts in the Workload tab display data for the selected time period of the time slider in the time range. There is no shadowed area displayed in this case.
- **Custom** - The shadowed area display depends on whether the time period is up to and including 24 hours, or greater than 24 hours.

#### Regions

The tab contains four regions: CPU Statistics, Wait Time Statistics, Workload Profile, and Sessions. Each region contains one or more charts that indicate the characteristics of the workload and the distribution of the resources. The data displayed on all the charts is for the same time period, as selected by the Time Range and time slider at the top of the window.

- **The CPU Statistics** region contains two charts:
  - **CPU Time** - This chart shows how much CPU time is being used by the foreground sessions every second. It identifies where the CPU time is mostly spent in the workload and pinpoints any unusual CPU spikes.
  - **CPU Utilization (%)** - This chart indicates the percentage of CPU time aggregated by consumer group as calculated by the resource manager.

- **The Wait Time Statistics** region contains a chart that displays the time used in different wait classes. To see the total average active sessions, select the **DB Time** check box. The activities are broken down by the 13 wait classes.

- **The Workload Profile** region contains a group of charts that indicate patterns of user calls, executions, transactions, and parses, as well as the number of running statements and queued statements. This region includes a menu that you can use to select the data to display. It contains the following options.
  - **User Calls** - This option displays the combined number of logons, parses, and execute calls per second.
  - **Executions** - This option displays the combined number of user and recursive calls that executed SQL statements per second.
  - **Transactions** - This option displays the combined number of user commits and user rollbacks per second.
  - **Parses** - This option displays the combined number of hard and soft parses per second.
  - **Running Statements** - This option displays the number of running SQL statements, aggregated by consumer group.
  - **Queued Statements** - This option displays the number of queued parallel SQL statements, aggregated by consumer group.

- **The Sessions** region contains charts that show the number of current logons and sessions. It contains a menu that includes the following options:
  - **Current Logons** - This option displays the number of current successful logons.
  - **Sessions** - This option displays the number of sessions.
Blocking Sessions Tab

The Performance Hub blocking sessions tab displays the current blocking and waiting sessions in a hierarchical display. You can view detailed information about each blocking session, and can view the sessions blocked by each blocking session. You can also use the tab to inspect or drill down into the SQL involved, to determine the cause of the blocking. You can perform several operations in the tab, including killing one or more of the listed sessions to resolve a waiting session problem. Instructions for the tab functions are located in this topic under Using the Oracle Cloud Infrastructure Console on page 1602.

The hierarchical display nests waiting sessions underneath the session that is blocking them in an easily viewable parent-child relationship. The hierarchy can contain any number of levels to correctly represent the structure of the sessions involved.

The sessions listed include sessions that are waiting for a resource and sessions that hold a resource that is being waited on that creates the blocking condition.

ADDM Tab

The Performance Hub Automatic Database Diagnostic Monitor (ADDM) tab includes controls to access the information stored by ADDM. ADDM analyzes the Automatic Workload Repository (AWR) data on a regular basis, then locates the root causes of performance problems, provides recommendations for correcting any problems, and identifies non-problem areas of the application. Because AWR is a repository of historical performance data, ADDM can be used to analyze performance issues after the event, often saving time and resources that would be needed to reproduce a problem.

ADDM provides the following benefits:

• Time-based quantification of application problem impacts and recommendation benefits
• Recommendations for treating the root causes of problems
• Identification of non-problem areas of the application

In addition to the benefits ADDM provides for production systems, it can be used on development and test systems to provide early warnings of application performance issues.

Instructions to use the ADDM tab are located below in Using the Oracle Cloud Infrastructure Console on page 1602.

Automatic Workload Repository Reports

The Automatic Workload Repository (AWR) collects, processes, and maintains performance statistics for problem detection and self-tuning purposes. This data is both in memory and stored in the database. From the Performance Hub, you can generate and download a report of the gathered data.

An AWR report shows data captured between two points in time (or snapshots). AWR reports are divided into multiple sections. The content of the report contains the workload profile of the system for the selected range of snapshots. The HTML report includes links that you can use to navigate quickly between sections.

The statistics collected and processed by AWR include:

• Object statistics that determine both access and usage statistics of database segments
• Time model statistics based on time usage for activities, displayed in the V$SYS_TIME_MODEL and V$SESS_TIME_MODEL views
• Some of the system and session statistics collected in the V$SYSSTAT and V$SESSTAT views
• SQL statements that are producing the highest load on the system, based on criteria such as elapsed time and CPU time
• ASH statistics, representing the history of recent sessions activity

To generate and download an AWR report, see To download an AWR report on page 1603.
Using the Oracle Cloud Infrastructure Console
To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database

1. Open the navigation menu. Under Database, click Autonomous Transaction Processing or Autonomous Data Warehouse.
2. Choose your Compartment.
3. In the list of Autonomous Databases, click the display name of the database you want to analyze using Performance Hub reports.
4. Click Performance Hub.

To view the average active sessions data by a selected dimension

1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database which you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information.
   • The database name is displayed at the top of the Performance Hub page.
   • The time period for which information is available on the Performance Hub is displayed in the Time Range field.
   • The selected time period is indicated on the time slider graph by the adjustable time slider box.
   • The ASH Analytics tab is displayed with the top activity for a selected dimension in the selected time period.
2. Use the Quick Select selector to set the exact time period for which data is displayed in the ASH Analytics tables and graphs. By default, the last hour is selected. The time range is the total amount of time available for analysis.
3. Use the box on the time slider to further narrow down the time period for which performance data is displayed on the ASH Analytics tab.
4. Select a dimension in the Average Active Sessions drop-down list to display ASH analytics by that dimension. When the Consumer Group dimension is selected, the data is categorized by default to the High, Medium, or Low service name that is associated with the Autonomous Database.
   Optionally, you can:
   • Click the Maximum Threads check box to view the number of Max CPU Threads. The red line on the chart shows this limit.
   • Click the Total Activity check box to view a black border that denotes total activity of all the components of the selected dimension on the chart. This option is selected by default when you use the filtering capabilities to only view the data for a particular component within a dimension. For information on filtering Average Active Sessions data, see Filter Average Active Sessions Data.
5. Use the Sample Resolution menu to select the sampling of ASH data displayed in the Average Active Sessions chart. To select a resolution, click Sample Resolution to display the following menu and click the desired resolution to display the data.
   • Low - the graph displays the fewest data points available in the selected data sample.
   • Medium - the graph displays more data points in the selected data sample.
   • High - the graph displays more data points in the selected data sample.
   • Maximum - the graph displays the most data points available in the selected data sample.
6. For the dimension selected in the Average Active Sessions drop-down list, you can further drill down into session details by selecting dimensions in the two sections at the bottom of the ASH Analytics tab. By default, the following dimensions are selected:
   • SQL ID by Consumer Group, which displays the SQL statements with the top average active sessions activity for consumer groups for the selected time period. You can right-click the bar charts to sort the SQL statements in ascending or descending order or click the SQL ID to go the SQL Details page.
   • User Session by Consumer Group, which displays the user sessions with the top average active sessions activity for consumer groups for the selected time period. You can right-click the bar charts to sort the user sessions in ascending or descending order or click the user session to go to the User Session page.
To filter average active sessions data

1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database that you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information.
   - The database name is displayed at the top of the Performance Hub page.
   - The time period for which information is available on the Performance Hub is displayed in the Time Range field. The selected time period is indicated on the time slider graph by the adjustable time slider block.

   The ASH Analytics tab is displayed with the top activity for a selected dimension in the selected time period.

2. Use the Quick Select selector to set the exact time period for which data is displayed in the ASH Analytics tables and graphs. By default, the last hour is selected. The time range is the total amount of time available for analysis.

3. Use the adjustable time slider box to further narrow down the time period for which performance data is displayed on the ASH Analytics tab.

4. In the ASH Analytics tab, select a dimension in the Average Active Sessions by drop-down list. By default, Consumer Group is selected.

   The chart is displayed. Each color in the chart denotes a component of the selected dimension. For example, the Consumer Group dimension has High, Medium, and Low, which are predefined service names assigned to your Autonomous Database to provide different levels of concurrency and performance.

5. Click a component in the legend. The selected component is displayed in the Applied Filters field and the chart is updated to only display data pertaining to that component. The total activity, which includes all the components of the dimension, is defined by a black outline and is displayed by default when you filter data.

To view the SQL Monitoring report

1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database which you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information.
   - The database name is displayed at the top of the Performance Hub page.
   - The time period for which information is available on the Performance Hub is displayed in the Time Range field. The selected time period is indicated on the time slider graph by the adjustable time slider box.

2. Click SQL Monitoring to display the SQL monitoring tab.

3. Optionally, you can get detailed information on a specific SQL statement by clicking an ID number in the SQL ID column. When you click an ID number, the Real-time SQL Monitoring page is displayed.

4. Click Download Report to download the report data for your selected SQL statement.

To download an AWR report

For databases version 18c and older:

1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database which you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information.
   - The database name is displayed at the top of the Performance Hub page.
   - The time period for which information is available on the Performance Hub is displayed in the Time Range field. The selected time period is indicated on the time slider graph by the adjustable time slider box.

2. Click AWR to display the Generate AWR Report dialog.

3. You can choose to generate a report either from two snapshots closest to the current time and date or from a custom time range of your choice.

4. You can choose to generate a report either from two snapshots closest to the current time and date or from a custom time range of your choice.

5. If you choose to generate a report from a custom time range, then select Custom and select start and end times for your range. Click Download.

6. Oracle Database generates a report named AWRReport_date_range.html that downloads to the default download folder for your browser. View the report after the download completes.
For databases version 19c and newer:

1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database which you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information.
   - The database name is displayed at the top of the Performance Hub page.
   - The time period for which information is available on the Performance Hub is displayed in the Time Range field. The selected time period is indicated on the time slider graph by the adjustable time slider box.

2. In the Quick Select menu, choose a time period for which an AWR report will be generated.

3. In the upper right corner, click Reports > Automatic Workload Repository.
   
   The Generate Automatic Workload Repository dialog box is displayed.

4. Use the Start Snapshot and End Snapshot menus to select the beginning and end of the snapshot time range to generate the report.

5. Click Download. The database generates the report named AWRReport_date_range.html. When the report is complete, the report name is displayed at the top of the screen, and the report is automatically downloaded to the default download folder for your browser.

6. Open the default download folder for your browser on your system and view the report from there.

To view the Workload metrics

1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database that you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information. The database name is displayed at the top of the Performance Hub page.

2. Use the Quick Select selector to set the exact time period for which data is displayed in the ASH Analytics tables and graphs. By default, the last hour is selected. The time range is the total amount of time available for analysis.

3. Use the time slider to further narrow down the time period for which performance data is displayed on the Workload tab. All charts show data for the entire specified time range if within 24 hours.

4. Click Workload to view the Workload tab. The four regions and their associated charts are displayed.
   
   - **CPU Statistics** The CPU Statistics region contains two charts, CPU Time and CPU Utilization (%).
     
     To display how much CPU Time is being consumed by the foreground sessions per second, select CPU Time in the menu in this region. This identifies where the CPU time is mostly spent in the workload and pinpoints any unusual CPU spikes. When CPU time is selected optionally click the Maximum Threads check box to show the maximum CPU time available. This shows the CPU time component of Average Active Sessions.
     
     To display the CPU Utilization (%) chart, select CPU Utilization (%) in the menu. This chart displays the percentage of CPU time aggregated by consumer group, as calculated by the resource manager.
   
   - **Wait Time Statistics** The Wait Time Statistics region contains one chart that displays the time used in different wait classes. To see the total average active sessions, select the DB Time check box. The activities are broken down by the 13 wait classes.
   
   - **Workload Profile** To change the metrics displayed in the Workload Profile, click the menu and select the metric that you want to view.
     
     - Select User Calls to display the combined number of logons, parses, and execute calls per second.
     
     - Select Executions to display the combined number of user and recursive calls that executed SQL statements per second.
     
     - Select Transactions to display the combined number of user commits and user rollbacks per second.
     
     - Select Parses to display the combined number of hard and soft parses per second
     
     - Select Running Statements to display the number of running SQL statements, aggregated by consumer group.
     
     - Select Queued Statements to display the number of queued parallel SQL statements, aggregated by consumer group.
• **Sessions** To change the metrics displayed in the Sessions region, click the menu and select the metric that you want to view:
  
  • Select **Current Logons** to display the number of current successful logons.
  • Select **Sessions** to display the number of sessions.

**To view blocking and waiting sessions**

1. Go to the **Performance Hub** page of the Oracle Cloud Infrastructure Console for the database that you want to manage. See **To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database** on page 1602 for more information.
   
   • The database name is displayed at the top of the Performance Hub page.
   • The time period for which information is available on the Performance Hub is displayed in the **Time Range** field. The selected time period is indicated on the time slider graph by the adjustable time slider box. See the Time Range information in **Performance Hub Features** on page 1597 to learn how to set the duration of the time to be monitored.

2. Click **Blocking Sessions** to display details about current blocking and waiting sessions. Analysis of historical sessions is not supported.

3. Click the link in each column of the table to view the details of the listed blocking and waiting sessions, as shown in the following table.

<table>
<thead>
<tr>
<th>Tab Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>This is the name of the user.</td>
</tr>
<tr>
<td>Status</td>
<td>The status indicates whether the session is active, inactive, or expired.</td>
</tr>
<tr>
<td>Lock</td>
<td>This is the lock type for the session. Click the lock type to display a table with more information about the session lock. It lists the Lock Type, Lock Mode, Lock Request, Object Type, Subobject Type, Time, ID1, ID2, Lock Object Address, and Lock Address of the selected session.</td>
</tr>
<tr>
<td>User Session</td>
<td>The user session lists the Instance, SID, and Serial number.</td>
</tr>
<tr>
<td>SQL ID</td>
<td>This is the ID of the SQL associated with the session.</td>
</tr>
<tr>
<td>Wait Event</td>
<td>This is the wait event for the session. Click the wait event to show additional wait event details.</td>
</tr>
<tr>
<td>Object Name</td>
<td>This is the name of the locked database object.</td>
</tr>
<tr>
<td>Blocking Time</td>
<td>This is the time that a blocking session has been blocking a session.</td>
</tr>
<tr>
<td>Wait Time</td>
<td>This is the time that a session has been waiting.</td>
</tr>
</tbody>
</table>

**Note:**

If you see an error message that says the server failed to get performance details for the selected session at the selected time, try the selection again. If the same error message is displayed, try a different time selection. If that fails, contact Oracle Support.

**Setting the Minimum Wait Time**

The minimum wait time works like a filter for the Blocking Sessions information. It sets the minimum time that a session must wait before it is displayed in the tab. For example, if the minimum wait time is set to three seconds, and a session has waited only two seconds, it is not displayed in the table. But if you change the minimum wait time to one second, the session that waited only two seconds is added to the display.
Killing a Session
1. Click the check box at the left of the session User Name to select a session. The Kill Session button is enabled.
2. Click Kill Session. The Kill Session confirmation dialog box is displayed.
3. Click Kill Session to end the session.

Displaying Lock Details
1. In the session Lock column, click the name of the lock type (Lock or Exclusive Lock) for the session. The Wait Event Details message box is displayed.
2. Note the information in the table and use as needed to determine any action to take.

Displaying Wait Event Information
1. In the session Wait Event column, click the name of the wait event for the selected session. The Session Lock Information table is displayed.
2. Note the information in the message box and use as needed to determine any action to take.

Displaying Session Details
1. In the session User Session column, click the session identifier for the session. The Performance Hub Session Details page is displayed.
2. Optionally move the time slider to display a specific time range of the session.
3. Use the Session Details page to explore additional details about the session.

Displaying SQL Details
1. In the session SQL ID column, click the SQL ID associated with the session. The Performance Hub SQL Details page is displayed.
2. Optionally move the time slider to display a specific time range of the session.
3. Select one or more of the following tabs, note the information in them, and take any action needed.
   • Summary. This tab displays the SQL Overview and Source details.
   • ASH Analytics. This tab displays the SQL average active sessions.
   • Execution Statistics. This tab displays the SQL plans and plan details.
   • SQL Monitoring. This tab displays information about monitored SQL executions.
   • SQL Text. This tab displays the SQL.

To view ADDM data
This procedure explains how to view Automatic Database Diagnostic Monitor (ADDM) information with Performance Hub.
1. Go to the Performance Hub page of the Oracle Cloud Infrastructure Console for the database that you want to manage. See To navigate to Performance Hub in the Oracle Cloud Infrastructure Console interface of an Autonomous Database on page 1602 for more information. The database name is displayed at the top of the Performance Hub page.
2. Click the ADDM tab to open it.
3. Use the menu located below Quick Select to select a time range. The data for that time range is displayed.
4. In the **Activity Summary** area, just below the data, click one of the **gray AWR snapshot icons** to display findings for the associated ADDM task. A white check mark in the gray icon indicates that there are problem findings available. When selected, the gray icon changes to blue.

**Note:**

You can alternatively select an ADDM task from the menu below the ADDM tab or by positioning the time slider above an icon.

**Note:**

When you manually change the ADDM task selection, either by clicking the gray icon for an associated AWR snapshot, or by selecting an option from the ADDM task menu, the time slider position and size are adjusted to cover the analysis period for the ADDM task.

5. Hover over the icon to display a message about the AWR snapshot and ADDM task, including the number of findings for the ADDM task. The findings are displayed in two tables:

- **Findings table.** When there are findings, the Findings table shows the Name of the finding, the Impact, Number of recommendations, and Average Active Sessions for that finding. If there are no findings available, the table displays a message that says no findings are available for the selected analysis period.

- **Warnings and Information table.** The Warnings and Information table is displayed below the Findings table. It lists messages related to the findings.
  - Warning messages identify issues such as missing data in the AWR that may affect the completeness or accuracy of the ADDM analysis.
  - Information messages provide information that is relevant to understanding the performance of the database but does not represent a performance problem. This may include identification of non-problem areas of the database and automatic database maintenance activity.

**Note:**

Both the Findings table and the Warnings and Information table are collapsible to save space when many findings are found. Click the **minus icon** to collapse a table. Click the **plus icon** to expand the table again.

6. If a finding has ADDM recommendations available, the name of the finding is displayed as a link. Click the **name of the finding** to display more information about the finding, including a table of recommendations for corrective actions. Each recommendation includes the problem area, the suggested action to take to solve it, and the estimated benefit that will result when the action is taken.

7. Click the **expand icon** at the end of a row in the recommendations table to view a rationale for the recommendation.

### Migrating Databases to the Cloud

You can migrate your on-premises Oracle Database to an Oracle Cloud Infrastructure Database service database using a number of different methods that use several different tools. The method that applies to a given migration scenario depends on several factors, including the version, character set, and platform endian format of the source and target databases.

**Tip:**

Oracle now offers the **Zero Downtime Migration** service, a quick and easy way to move on-premises Oracle Databases and Oracle Cloud Infrastructure Classic databases to Oracle Cloud Infrastructure. You can migrate databases to the following types of Oracle Cloud Infrastructure systems: Exadata, Exadata Cloud@Customer, bare metal, and virtual machine.

Zero Downtime Migration leverages Oracle Active Data Guard to create a standby instance of your database in an Oracle Cloud Infrastructure system. You switch over only when you are ready, and your source database remains
Choosing a Migration Method

Not all migration methods apply to all migration scenarios. Many of the migration methods apply only if specific characteristics of the source and destination databases match or are compatible. Moreover, additional factors can affect which method you choose for your migration from among the methods that are technically applicable to your migration scenario.

Some of the characteristics and factors to consider when choosing a migration method are:

• On-premises database version
• Database service database version
• On-premises host operating system and version
• On-premises database character set
• Quantity of data, including indexes
• Data types used in the on-premises database
• Storage for data staging
• Acceptable length of system outage
• Network bandwidth

To determine which migration methods are applicable to your migration scenario, gather the following information.

1. Database version of your on-premises database:
   • Oracle Database 12c Release 2 version 12.2.0.1
   • Oracle Database 12c Release 1 version 12.1.0.2 or higher
   • Oracle Database 12c Release 1 version lower than 12.1.0.2
   • Oracle Database 11g Release 2 version 11.2.0.3 or higher
   • Oracle Database 11g Release 2 version lower than 11.2.0.3

2. For on-premises Oracle Database 12c Release 2 and Oracle Database 12c Release 1 databases, the architecture of the database:
   • Multitenant container database (CDB)
   • Non-CDB

3. Endian format (byte ordering) of your on-premises database’s host platform

   Some platforms are little endian and others are big endian. Query V$TRANSPORTABLE_PLATFORM to identify the endian format, and to determine whether cross-platform tablespace transport is supported.

   The Oracle Cloud Infrastructure Database uses the Linux platform, which is little endian.

4. Database character set of your on-premises database and the Oracle Cloud Infrastructure Database database.

   Some migration methods require that the source and target databases use compatible database character sets.

5. Database version of the Oracle Cloud Infrastructure Database database you are migrating to:
   • Oracle Database 12c Release 2
   • Oracle Database 12c Release 1
   • Oracle Database 11g Release 2

   Oracle Database 12c Release 2 and Oracle Database 12c Release 1 databases created on the Database service use CDB architecture. Databases created using the Enterprise Edition software edition are single-tenant, and databases created using the High Performance or Extreme Performance software editions are multitenant.

After gathering this information, use the “source” and “destination” database versions as your guide to see which migration methods apply to your migration scenario:

• Migrating from Oracle Database 11g to Oracle Database 11g in the Cloud on page 1616
Migration Connectivity Options

You have several connectivity options when migrating your on-premises databases to the Oracle Cloud Infrastructure. The options are listed below in order of preference.

1. **FastConnect**: Provides a secure connection between your existing network and your virtual cloud network (VCN) over a private physical network instead of the internet. For more information, see FastConnect on page 3173.

2. **IPSec VPN**: Provides a secure connection between a dynamic routing gateway (DRG) and customer-premise equipment (CPE), consisting of multiple IPSec tunnels. The IPSec connection is one of the components forming a site-to-site VPN between a VCN and your on-premises network. For more information, see VPN Connect on page 2932.

3. **Internet gateway**: Provides a path for network traffic between your VCN and the internet. For more information, see Internet Gateway on page 3243.

Migration Methods

Many methods exist to migrate Oracle databases to the Oracle Cloud Infrastructure Database service. Which of these methods apply to a given migration scenario depends on several factors, including the version, character set, and platform endian format of the source and target databases.

- **Data Pump Conventional Export/Import** on page 1621
- **Data Pump Full Transportable** on page 1622
- **Data Pump Transportable Tablespace** on page 1625
- **Remote Cloning a PDB** on page 1627
- **Remote Cloning Non-CDB** on page 1628
- **RMAN Cross-Platform Transportable PDB** on page 1628
- **RMAN Cross-Platform Transportable Tablespace Backup Sets** on page 1629
- **RMAN Transportable Tablespace with Data Pump** on page 1631
- **RMAN DUPLICATE from an Active Database** on page 1636
- **RMAN CONVERT Transportable Tablespace with Data Pump** on page 1633
- **SQL Developer and INSERT Statements to Migrate Selected Objects** on page 1644
- **SQL Developer and SQL*Loader to Migrate Selected Objects** on page 1644
- **Unplugging/Plugging a PDB** on page 1644
- **Unplugging/Plugging Non-CDB** on page 1645
- **Zero Downtime Migration Service**

Migrating an On-Premises Database to Oracle Cloud Infrastructure by Creating a Backup in the Cloud

**Note:**

This topic is not applicable to Exadata DB systems.

You can migrate an on-premises database to Oracle Cloud Infrastructure by creating a backup of your on-premises database in Oracle Cloud Infrastructure's Database service.

Oracle provides a Python script to create a backup of your database. The script invokes an API call to create the backup and then places the backup in Oracle Cloud Infrastructure. You can then use the Console or the API to create a new database or DB system from that backup. Backups created using the instructions in this topic appear under Standalone Backups in the console.
The Python script is bundled as a part of the Oracle Cloud Infrastructure CLI installation. Oracle provides the migration script and associated files at no cost. Normal Object Storage charges apply for the storage of your backup in Oracle Cloud Infrastructure.

**Compatibility**

The scripted migration process is compatible with the following bare metal and virtual machine DB system configurations:
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Version or Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Version</td>
<td>19.x</td>
<td>• For versions 19c, 18c, 12.2.0.1, and 12.1.0.2:</td>
</tr>
<tr>
<td></td>
<td>18.x</td>
<td>• Only Container Databases (CDBs) are supported. The scripted migration process may work with non-CDB databases for these database</td>
</tr>
<tr>
<td></td>
<td>12.2.0.1</td>
<td>versions, but Oracle does not provide support for the migration of non-CDB databases using the script described in this topic.</td>
</tr>
<tr>
<td></td>
<td>12.1.0.2</td>
<td>For information on creating an on-premises pluggable database (PDB) by cloning a non-CDB in Oracle Database 19c, see About Cloning a</td>
</tr>
<tr>
<td></td>
<td>11.2.0.4</td>
<td>Non-CDB. For an overview of multitenant architecture in Oracle Database 19c, see Introduction to the Multitenant Architecture.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information on creating an on-premises pluggable database (PDB) from a non-CDB database in Oracle Database 12c Release 2 (12.2),</td>
</tr>
<tr>
<td></td>
<td></td>
<td>see Upgrading a Non-CDB Oracle Database To a PDB on a CDB. For an overview of multitenant architecture in 12c Release 2, see</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overview of Managing a Multitenant Environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Oracle Cloud Infrastructure Database service will attempt to run datapatch, which requires read/write mode. If there are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pluggable databases (PDBs), they should also be in read/write mode to ensure that datapatch runs on them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For version 11.2.0.4, depending on the source database patch level, you may need to roll back patches prior to migrating.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Rolling Back Patches on a Version 11.2 Database for more information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If your on-premises database has an interim patch (previous known as a one-off patch), see Applying Interim Patches for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>details on applying the patch in Oracle Cloud Infrastructure.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Version or Type</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source Database Platform</td>
<td>Oracle Enterprise Linux / Red Hat Enterprise Linux 5.x</td>
<td>• The scripted migration described in this topic may work in Microsoft Windows environments, but Oracle currently does not provide support for this script in Windows.</td>
</tr>
<tr>
<td></td>
<td>Oracle Linux / Red Hat Enterprise Linux 6.x</td>
<td>• For Oracle Linux 6.x users, see Configuring Oracle Linux 6 to install Python for details on configuring the operating system to install a compatible version of Python. See Installing the CLI for more information regarding Oracle Linux 6.</td>
</tr>
<tr>
<td></td>
<td>Oracle Linux / Red Hat Enterprise Linux 7.x</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>TDE</td>
<td>• In a non-TDE configuration, the RMAN encryption password is required.</td>
</tr>
<tr>
<td></td>
<td>Non-TDE</td>
<td>• Oracle requires that unencrypted on-premises databases be encrypted after they are restored to Oracle Cloud Infrastructure. The stored RMAN standalone backups are always encrypted.</td>
</tr>
<tr>
<td>Target Database Edition</td>
<td>Standard Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Edition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Edition - High Performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Edition - Extreme Performance</td>
<td></td>
</tr>
<tr>
<td>Cluster</td>
<td>Single</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RAC</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisites**

On the source database host:

• Outbound internet connectivity for installing Python packages, running yum install, and access to the Oracle Cloud Infrastructure API and Object Storage.

• RMAN configuration to autobackup controlfile and spfile:

```
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
```

**Note:**

RMAN configuration changes must be completed prior to running the script. The script may modify RMAN parameters as required to complete the backup and migration tasks.
To Migrate an On-Premises Database Using a Standalone Backup

Perform the following tasks on the source database host:

1. Create a directory named `/home/oracle/migrate`.

   Tip:
   You can name the `migrate` portion of the directory path anything you want. If you use a different name, you must adjust all of the paths that appear in this task accordingly. The following examples assume the name `migrate` for simplicity and clarity.

2. As `root`, run the CLI installer in the directory you created in step 1. (For example, `/home/oracle/migrate`.)
   See Installing the CLI for instructions on running the installer script in either Windows or the Bash environment (for MacOS, Linux, and Unix).

   The installer installs Python 3.6.0 if either Python 2.7 or Python 3.6 does not exist on the machine. The installer also installs the Python script required to create and migrate a standalone backup from an on-premises database.

   On Oracle Linux 6, a newer version of Python (such as Python 3.6.0) is usually required. Use the following instructions to configure Oracle Linux 6 before running the backup script.

3. Copy the following files into the new directory:
   - Oracle Database Backup Module (`opc_install.jar`)
   - Your API *.pem key file.

4. Respond to the prompts as follows:

   (yum install)  
   Is this ok [y/N]: y  

   ==> Missing native dependencies. Continue and install the following dependencies: gcc, libffi-devel, python36u-devel, openssl-devel? (Y/n): Y  

   ==> In what directory would you like to place the install? (leave blank to use '/root/lib/oracle-cli'): /home/oracle/migrate/lib/oracle-cli  

   ==> In what directory would you like to place the 'oci' executable? (leave blank to use '/root/bin'): /home/oracle/migrate/bin  

   ==> In what directory would you like to place the OCI scripts? (leave blank to use '/root/bin/oci-cli-scripts'): /home/oracle/migrate/bin/oci-cli-scripts  

   ==> Currently supported optional packages are: ['db (will install cx_Oracle)'] What optional CLI packages would you like to be installed (comma separated names; press enter if you don't need any optional packages)?: db  

   ==> Modify profile to update your $PATH and enable shell/tab completion now? (Y/n): Y  

   ==> Enter a path to an rc file to update (leave blank to use '/root/.bashrc'): /home/oracle/.bashrc

5. Perform the following file operations:

6. Edit the `/home/oracle/migrate/config.txt` file

```
[DEFAULT]
tenancy=<your_tenancy_OCID>
user=<your_user_OCID>
fingerprint=<fingerprint>
key_file=/home/oracle/migrate/<your_api_key>.pem
region=<region>
```

If you do not know your API signing key's fingerprint, see How to Get the Key's Fingerprint on page 4183.

7. As oracle user (not root), run one of the following sets of commands, depending on the type of database you are migrating.

**For a non-TDE database:**

```
export AD=<destination_availability_domain>
export C=<destination_compartment_OCID>
export ORACLE_SID=<ORACLE_SID>
export ORACLE_HOME=<ORACLE_HOME>
export PATH=$PATH:$ORACLE_HOME/bin
export LC_ALL=en_US.UTF-8
export ORACLE_UNQNAME=<source_DB_unique_name>
rm -rf /home/oracle/migrate/onprem_upload
cd /home/oracle/migrate/bin/oci-cli-scripts/
./create_backup_from_onprem --config-file /home/oracle/migrate/config.txt
--display-name <example_display_name> --availability-domain $AD --edition ENTERPRISE_EDITION_EXTREME_PERFORMANCE --opc-installer-dir /home/oracle/migrate --tmp-dir /home/oracle/migrate/onprem_upload --compartment-id $C
--rman-password <password>
```

**For a TDE-enabled database:**

```
export AD=<destination_availability_domain>
export C=<destination_compartment_OCID>
export ORACLE_SID=<ORACLE_SID>
export ORACLE_HOME=<ORACLE_HOME>
export PATH=$PATH:$ORACLE_HOME/bin
rm -rf /home/oracle/migrate/onprem_upload
cd /home/oracle/migrate/bin/oci-cli-scripts/
./create_backup_from_onprem --config-file /home/oracle/migrate/config.txt
--display-name <example_display_name> --availability-domain $AD --edition ENTERPRISE_EDITION_EXTREME_PERFORMANCE --opc-installer-dir /home/oracle/migrate --tmp-dir /home/oracle/migrate/onprem_upload --compartment-id $C
```

See the following list of parameters used by the script for more details.

8. Create a new database or launch a new DB system using the backup you created in the preceding step. See Creating Databases on page 1414 for information on creating a new database from a backup. See Creating Bare Metal and Virtual Machine DB Systems on page 1370 for information on creating a new DB system from a backup.
Configuring Oracle Linux 6 to install Python

In Oracle Linux 6 use the following /etc/yum.repos.d/ol6.repo file to ensure that a compatible version of Python is installed by the script if a compatible version is not already installed. Include this file before attempting to run the script with the ./install.sh command.

```
[ol6_latest]
name=Oracle Linux $releasever Latest ($basearch)
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1
```

Parameters used by the script

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--config-file</code></td>
<td>The path to the oci-cli config file. The default path is as follows: ~/.oci/config</td>
<td>No</td>
</tr>
<tr>
<td><code>--profile</code></td>
<td>The profile in the config file to load. This profile will also be used to locate any default parameter values which have been specified in the OCI CLI-specific configuration file. The default value is DEFAULT.</td>
<td>No</td>
</tr>
<tr>
<td><code>--compartment-id</code></td>
<td>The compartment OCID of the Oracle Cloud Infrastructure compartment that will contain your standalone backup.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>--display-name</code></td>
<td>The name of the backup, as you want it to be displayed in the OCI Console under Standalone Backups. Avoid entering confidential information.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>--availability-domain</code></td>
<td>The availability domain where the backup is to be stored.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| `--edition`        | The edition of the Oracle Cloud Infrastructure DB system that will contain the database created from the standalone backup. You can choose the same edition as the on-premises database, or any addition above the on-premises database. The choices, listed from lowest to highest, are the following:  
  - STANDARD_EDITION  
  - ENTERPRISE_EDITION  
  - ENTERPRISE_EDITION_HIGH_PERFORMANCE  
  - ENTERPRISE_EDITION_EXTREME_PERFORMANCE | Yes      |
The script will produce a standalone backup of your on-premises database in your Oracle Cloud Infrastructure tenancy. You can check the Console for your backup by viewing the *Standalone Backups* page in the Database service, under *Bare Metal, VM, and Exadata*.

**Tip:**
To access command line help for the backup script, run the following command in the `/home/oracle/migrate/bin/oci-cli-scripts/` directory:

```
create_backup_from_onprem --help
```

### Migrating from Oracle Database 11g to Oracle Database 11g in the Cloud

You can migrate Oracle Database 11g databases from on-premises to Oracle Database 11g databases in the Database service using several different methods.

The applicability of some of the migration methods depends on the on-premises database’s character set and platform endian format.

If you have not already done so, determine the database character set of your on-premises database, and determine the endian format of the platform your on-premises database resides on. Use this information to help you choose an appropriate method.

- **Data Pump Conventional Export/Import**
  
  This method can be used regardless of the endian format and database character set of the on-premises database.

  For the steps this method entails, see *Data Pump Conventional Export/Import* on page 1621.

- **Data Pump Transportable Tablespace**
  
  This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Oracle Cloud Infrastructure Database database are compatible.

  For the steps this method entails, see *Data Pump Transportable Tablespace* on page 1625.

- **RMAN Transportable Tablespace with Data Pump**
  
  This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Oracle Cloud Infrastructure Database database are compatible.

  For the steps this method entails, see *RMAN Transportable Tablespace with Data Pump* on page 1631.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--opc-installer-dir</code></td>
<td>The directory containing the <code>opc_installer.jar</code> file. This is the directory you created in step 1 of this procedure.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>--additional-opc-args</code></td>
<td>Optional additional arguments for the <code>opc installer</code>.</td>
<td>No</td>
</tr>
<tr>
<td><code>--tmp-dir</code></td>
<td>Optional temporary directory for intermediate files.</td>
<td>No</td>
</tr>
<tr>
<td><code>--rman-password</code></td>
<td>The RMAN password to use for the standalone backup. The password must have 8 or more characters.</td>
<td>Required if TDE is not enabled</td>
</tr>
<tr>
<td><code>--rman-channels</code></td>
<td>RMAN channels. The default value is 5.</td>
<td>No</td>
</tr>
<tr>
<td><code>--help</code></td>
<td>Displays in-line help for the script in the OCI-CLI environment.</td>
<td>No</td>
</tr>
</tbody>
</table>
• **RMAN CONVERT Transportable Tablespace with Data Pump**

  This method can be used only if the database character sets of your on-premises database and the Oracle Cloud Infrastructure Database database are compatible.

  This method is similar to the Data Pump Transportable Tablespace method, with the addition of the `RMAN CONVERT` command to enable transport between platforms with different endianness. Query `V$TRANSPORTABLE_PLATFORM` to determine if the on-premises database platform supports cross-platform tablespace transport and to determine the endian format of the platform. The Database service platform is little-endian format.

  For the steps this method entails, see [RMAN CONVERT Transportable Tablespace with Data Pump](#) on page 1633.

**Migrating from Oracle Database 11g to Oracle Database 12c in the Cloud**

You can migrate Oracle Database 11g databases from on-premises to Oracle Database 12c databases in the Database service using several different methods.

The applicability of some of the migration methods depends on the on-premises database’s version, database character set and platform endian format.

If you have not already done so, determine the database version and database character set of your on-premises database, and determine the endian format of the platform your on-premises database resides on. Use this information to help you choose an appropriate method.

• **Data Pump Conventional Export/Import**

  This method can be used regardless of the endian format and database character set of the on-premises database.

  For the steps this method entails, see [Data Pump Conventional Export/Import](#) on page 1621.

• **Data Pump Transportable Tablespace**

  This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database service database are compatible.

  For the steps this method entails, see [Data Pump Transportable Tablespace](#) on page 1625.

• **RMAN Transportable Tablespace with Data Pump**

  This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database service database are compatible.

  For the steps this method entails, see [RMAN Transportable Tablespace with Data Pump](#) on page 1631.

• **RMAN CONVERT Transportable Tablespace with Data Pump**

  This method can be used only if the database character sets of your on-premises database and the Database service database are compatible.

  This method is similar to the Data Pump Transportable Tablespace method, with the addition of the `RMAN CONVERT` command to enable transport between platforms with different endianness. Query `V$TRANSPORTABLE_PLATFORM` to determine if the on-premises database platform supports cross-platform tablespace transport and to determine the endian format of the platform. The Database service platform is little-endian format.

  For the steps this method entails, see [RMAN CONVERT Transportable Tablespace with Data Pump](#) on page 1633.

• **Data Pump Full Transportable**

  This method can be used only if the source database release version is 11.2.0.3 or later, and the database character sets of your on-premises database and the Database service database are compatible.

  For the steps this method entails, see [Data Pump Full Transportable](#) on page 1622.
Migrating from Oracle Database 12c CDB to Oracle Database 12c in the Cloud

You can migrate Oracle Database 12c CDB databases from on-premises to Oracle Database 12c databases in the Oracle Cloud Infrastructure Database service using several different methods.

The applicability of some of the migration methods depends on the on-premises database’s character set and platform endian format.

If you have not already done so, determine the database character set of your on-premises database, and determine the endian format of the platform your on-premises database resides on. Use this information to help you choose an appropriate method.

- **Data Pump Conventional Export/Import**
  This method can be used regardless of the endian format and database character set of the on-premises database.
  For the steps this method entails, see Data Pump Conventional Export/Import on page 1621.

- **Data Pump Transportable Tablespace**
  This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database database are compatible.
  For the steps this method entails, see Data Pump Transportable Tablespace on page 1625.

- **RMAN Transportable Tablespace with Data Pump**
  This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Oracle Cloud Infrastructure Database service database are compatible.
  For the steps this method entails, see RMAN Transportable Tablespace with Data Pump on page 1631.

- **RMAN CONVERT Transportable Tablespace with Data Pump**
  This method can be used only if the database character sets of your on-premises database and the Database database are compatible.
  This method is similar to the Data Pump Transportable Tablespace method, with the addition of the RMAN CONVERT command to enable transport between platforms with different endianness. Query \$TRANSPORTABLE_PLATFORM to determine if the on-premises database platform supports cross-platform tablespace transport and to determine the endian format of the platform. The Database service platform is little-endian format.
  For the steps this method entails, see RMAN CONVERT Transportable Tablespace with Data Pump on page 1633.

- **RMAN Cross-Platform Transportable Tablespace Backup Sets**
  This method can be used only if the database character sets of your on-premises database and the Database service database are compatible.
  For the steps this method entails, see RMAN Cross-Platform Transportable Tablespace Backup Sets on page 1629.

- **Data Pump Full Transportable**
  This method can be used only if the database character sets of your on-premises database and the Database service database are compatible.
  For the steps this method entails, see Data Pump Full Transportable on page 1622.

- **Unplugging/Plugging (CDB)**
  This method can be used only if the on-premises platform is little endian, and the on-premises database and Database database have compatible database character sets and national character sets.
  For the steps this method entails, see Unplugging/Plugging a PDB on page 1644.
• Remote Cloning (CDB)

This method can be used only if the on-premises platform is little endian, the on-premises database release is 12.1.0.2 or higher, and the on-premises database and Database service database have compatible database character sets and national character sets.

For the steps this method entails, see Remote Cloning a PDB on page 1627.

• RMAN Cross-Platform Transportable PDB

This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database service database are compatible.

For the steps this method entails, see RMAN Cross-Platform Transportable PDB on page 1628.

• SQL Developer and SQL*Loader to Migrate Selected Objects

You can use SQL Developer to create a cart into which you add selected objects to be loaded into your Oracle Database 12c database on the cloud. In this method, you use SQL*Loader to load the data into your cloud database.

For the steps this method entails, see SQL Developer and SQL*Loader to Migrate Selected Objects on page 1644.

• SQL Developer and INSERT Statements to Migrate Selected Objects

You can use SQL Developer to create a cart into which you add selected objects to be loaded into your Oracle Database 12c database on the cloud. In this method, you use SQL INSERT statements to load the data into your cloud database.

For the steps this method entails, see SQL Developer and INSERT Statements to Migrate Selected Objects on page 1644.

Migrating from Oracle Database 12c Non-CDB to Oracle Database 12c in the Cloud

You can migrate Oracle Database 12c non-CDB databases from on-premises to Oracle Database 12c databases in Oracle Cloud Infrastructure Database service using several different methods.

The applicability of some of the migration methods depends on the on-premises database’s character set and platform endian format.

If you have not already done so, determine the database character set of your on-premises database, and determine the endian format of the platform your on-premises database resides on. Use this information to help you choose an appropriate method.

• Data Pump Conventional Export/Import

This method can be used regardless of the endian format and database character set of the on-premises database.

For the steps this method entails, see Data Pump Conventional Export/Import on page 1621.

• Data Pump Transportable Tablespace

This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database database are compatible.

For the steps this method entails, see Data Pump Transportable Tablespace on page 1625.

• RMAN Transportable Tablespace with Data Pump

This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database service database are compatible.

For the steps this method entails, see RMAN Transportable Tablespace with Data Pump on page 1631.
• RMAN CONVERT Transportable Tablespace with Data Pump

This method can be used only if the database character sets of your on-premises database and the Database service database are compatible.

This method is similar to the Data Pump Transportable Tablespace method, with the addition of the RMAN CONVERT command to enable transport between platforms with different endianness. Query V$TRANSPORTABLE_PLATFORM to determine if the on-premises database platform supports cross-platform tablespace transport and to determine the endian format of the platform. The Database service platform is little-endian format.

For the steps this method entails, see RMAN CONVERT Transportable Tablespace with Data Pump on page 1633.

• RMAN Cross-Platform Transportable Tablespace Backup Sets

This method can be used only if the database character sets of your on-premises database and the Database database are compatible.

For the steps this method entails, see RMAN Cross-Platform Transportable Tablespace Backup Sets on page 1629.

• Data Pump Full Transportable

This method can be used only if the database character sets of your on-premises database and the Database service database are compatible.

For the steps this method entails, see Data Pump Full Transportable on page 1622.

• Unplugging/Plugging (non-CDB)

This method can be used only if the on-premises platform is little endian, and the on-premises database and Database service database have compatible database character sets and national character sets.

You can use the unplug/plug method to migrate an Oracle Database 12c non-CDB database to Oracle Database 12c in the cloud. This method provides a way to consolidate several non-CDB databases into a single Oracle Database 12c CDB on the cloud.

For the steps this method entails, see Unplugging/Plugging Non-CDB on page 1645.

• Remote Cloning (non-CDB)

This method can be used only if the on-premises platform is little endian, the on-premises database release is 12.1.0.2 or higher, and the on-premises database and Database service database have compatible database character sets and national character sets.

You can use the remote cloning method to copy an Oracle Database 12c non-CDB on-premises database to your Oracle Database 12c database in the cloud.

For the steps this method entails, see Remote Cloning Non-CDB on page 1628.

• SQL Developer and SQL*Loader to Migrate Selected Objects

You can use SQL Developer to create a cart into which you add selected objects to be loaded into your Oracle Database 12c database on the cloud. In this method, you use SQL*Loader to load the data into your cloud database.

For the steps this method entails, see SQL Developer and SQL*Loader to Migrate Selected Objects on page 1644.

• SQL Developer and INSERT Statements to Migrate Selected Objects

You can use SQL Developer to create a cart into which you add selected objects to be loaded into your Oracle Database 12c database on the cloud. In this method, you use SQL INSERT statements to load the data into your cloud database.

For the steps this method entails, see SQL Developer and INSERT Statements to Migrate Selected Objects on page 1644.
Database

**Data Pump Conventional Export/Import**

You can use this method regardless of the endian format and database character set of the on-premises database.

To migrate an on-premises source database, tablespace, schema, or table to the database on a Database service database deployment using Data Pump Export and Import, you perform these tasks:

1. On the on-premises database host, invoke Data Pump Export and export the on-premises database.
2. Use a secure copy utility to transfer the dump file to the Database service compute node.
3. On the Database service compute node, invoke Data Pump Import and import the data into the database.
4. After verifying that the data has been imported successfully, you can delete the dump file.

For information about Data Pump Import and Export, see these topics:

- "Data Pump Export Modes" in *Oracle Database Utilities* for Release 12.2, 12.1 or 11.2.
- "Data Pump Import Modes" in *Oracle Database Utilities* for Release 12.2, 12.1 or 11.2.

**Data Pump Conventional Export/Import: Example**

This example provides a step-by-step demonstration of the tasks required to migrate a schema from an on-premises Oracle database to a Database service database.

This example illustrates a schema mode export and import. The same general procedure applies for a full database, tablespace, or table export and import.

In this example, the on-premises database is on a Linux host.

1. On the on-premises database host, invoke Data Pump Export to export the schemas.
   a. On the on-premises database host, create an operating system directory to use for the on-premises database export files.

   ```
   $ mkdir /u01/app/oracle/admin/orcl/dpdump/for_cloud
   ```

   b. On the on-premises database host, invoke SQL*Plus and log in to the on-premises database as the **SYSTEM** user.

   ```
   $ sqlplus system
   Enter password: <enter the password for the SYSTEM user>
   ```

   c. Create a directory object in the on-premises database to reference the operating system directory.

   ```
   SQL> CREATE DIRECTORY dp_for_cloud AS '/u01/app/oracle/admin/orcl/dpdump/for_cloud';
   ```

   d. Exit from SQL*Plus.

   e. On the on-premises database host, invoke Data Pump Export as the **SYSTEM** user or another user with the `DATAPUMP_EXP_FULL_DATABASE` role and export the on-premises schemas. Provide the password for the user when prompted.

   ```
   $ expdp system SCHEMAS=fsowner DIRECTORY=dp_for_cloud
   ```
2. Use a secure copy utility to transfer the dump file to the Database service compute node.
   In this example the dump file is copied to the /u01 directory. Choose the appropriate location based on the size of the file that will be transferred.
   a. On the Database service compute node, create a directory for the dump file.
      
      ```bash
      $ mkdir /u01/app/oracle/admin/ORCL/dpdump/from_onprem
      ```
   b. Before using the `scp` command to copy the export dump file, make sure the SSH private key that provides access to the Database service compute node is available on your on-premises host.
   c. On the on-premises database host, use the SCP utility to transfer the dump file to the Database service compute node.
      
      ```bash
      $ scp -i private_key_file \\
      /u01/app/oracle/admin/orcl/dpdump/for_cloud/expdat.dmp \\
      oracle@IP_address_DBaaS_VM:/u01/app/oracle/admin/ORCL/dpdump/from_onprem
      ```
3. On the Database service compute node, invoke Data Pump Import and import the data into the database.
   a. On the Database service compute node, invoke SQL*Plus and log in to the database as the `SYSTEM` user.
      
      ```bash
      $ sqlplus system
      Enter password: <enter the password for the SYSTEM user>
      ```
   b. Create a directory object in the Database service database.
      
      ```sql
      SQL> CREATE DIRECTORY dp_from_onprem AS '/u01/app/oracle/admin/ORCL/dpdump/from_onprem';
      ```
   c. If they do not exist, create the tablespace(s) for the objects that will be imported.
   d. Exit from SQL*Plus.
   e. On the Database service compute node, invoke Data Pump Import and connect to the database. Import the data into the database.
      
      ```bash
      impdp system SCHEMAS=fsowner DIRECTORY=dp_from_onprem
      ```
4. After verifying that the data has been imported successfully, you can delete the `expdat.dmp` file.

## Data Pump Full Transportable

You can use this method only if the source database release version is 11.2.0.3 or later, and the database character sets of your on-premises database and the Oracle Cloud Infrastructure Database service database are compatible.

You can use the Data Pump full transportable method to copy an entire database from your on-premises host to the database on a Database service database deployment.

To migrate an Oracle Database 11g on-premises database to the Oracle Database 12c database on a Database service database deployment using the Data Pump full transportable method, you perform these tasks:

1. On the on-premises database host, prepare the database for the Data Pump full transportable export by placing the user-defined tablespaces in `READ ONLY` mode.
2. On the on-premises database host, invoke Data Pump Export to perform the full transportable export.
3. Use a secure copy utility to transfer the Data Pump Export dump file and the datafiles for all of the user-defined tablespaces to the Database service compute node.
4. Set the on-premises tablespaces back to `READ WRITE`.
5. On the Database service compute node, prepare the database for the tablespace import.
6. On the Database service compute node, invoke Data Pump Import and connect to the database.
7. After verifying that the data has been imported successfully, you can delete the dump file.
Data Pump Full Transportable: Example

This example provides a step-by-step demonstration of the tasks required to migrate an Oracle Database 11g database to a Database service 12c database.

In this example, the source database is on a Linux host.

1. On the source database host, prepare the database for the Data Pump full transportable export.
   a. On the source database host, create a directory in the operating system to use for the source export.

      $ mkdir /u01/app/oracle/admin/orcl/dpdump/for_cloud

   b. On the source database host, invoke SQL*Plus and log in to the source database as the SYSTEM user.

      $ sqlplus system
      Enter password: <enter the password for the SYSTEM user>

   c. Create a directory object in the source database to reference the operating system directory.

      SQL> CREATE DIRECTORY dp_for_cloud AS '/u01/app/oracle/admin/orcl/ dpdump/for_cloud';

   d. Determine the name(s) of the tablespaces and data files that belong to the user-defined tablespaces by querying DBA_DATA_FILES. These files will also be listed in the export output.

      SQL> SELECT tablespace_name, file_name FROM dba_data_files;
      +-----------------+--------------------------------------------------+
      | TABLESPACE_NAME | FILE_NAME                                        |
      |-----------------+--------------------------------------------------|
      | USERS           | /u01/app/oracle/oradata/orcl/users01.dbf         |
      | UNDOTBS1        | /u01/app/oracle/oradata/orcl/undotbs01.dbf       |
      | SYSAUX          | /u01/app/oracle/oradata/orcl/sysaux01.dbf        |
      | SYSTEM          | /u01/app/oracle/oradata/orcl/system01.dbf        |
      | EXAMPLE         | /u01/app/oracle/oradata/orcl/example01.dbf       |
      | FSDATA          | /u01/app/oracle/oradata/orcl/fsdata01.dbf        |
      | FSINDEX         | /u01/app/oracle/oradata/orcl/fsindex01.dbf       |
      | SQL>            |                                                 |

   e. On the source database host, set all tablespaces that will be transported (the transportable set) to READ ONLY mode.

      SQL> ALTER TABLESPACE example READ ONLY;
      Tablespace altered.
      SQL> ALTER TABLESPACE fsindex READ ONLY;
      Tablespace altered.
      SQL> ALTER TABLESPACE fsdata READ ONLY;
      Tablespace altered.
      SQL> ALTER TABLESPACE users READ ONLY;
      Tablespace altered.
      SQL>

   f. Exit from SQL*Plus.

2. On the source database host, invoke Data Pump Export to perform the full transportable export. Specify FULL=y and TRANSPORTABLE=always. Because this is an Oracle Database 11g database and full transportable is an Oracle Database 12c feature, specify VERSION=12. Provide the password for the SYSTEM user when prompted.

      $ expdp system FULL=y TRANSPORTABLE=always VERSION=12 DUMPFILE=expdat.dmp
      DIRECTORY=dp_for_cloud
3. Use a secure copy utility to transfer the Data Pump Export dump file and the datafiles for all of the user-defined tablespaces to the Database service compute node.

   In this example the dump file is copied to the /u01 directory. Choose the appropriate location based on the size of the file that will be transferred.

   a. On the Database service compute node, create a directory for the dump file.

      $ mkdir /u01/app/oracle/admin/ORCL/dpdump/from_source

   b. Before using the scp utility to copy files, make sure the SSH private key that provides access to the Database service compute node is available on your source host.

   c. On the source database host, use the scp utility to transfer the dump file and all datafiles of the transportable set to the Database service compute node.

      $ scp -i private_key_file \
          /u01/app/oracle/admin/orcl/dpdump/for_cloud/expdat.dmp  \
          oracle@compute_node_IP_address:/u01/app/oracle/admin/ORCL/dpdump/from_source

      $ scp -i private_key_file \
          /u01/app/oracle/oradata/orcl/example01.dbf  \
          oracle@compute_node_IP_address:/u02/app/oracle/oradata/ORCL/PDB2

      $ scp -i private_key_file \
          /u01/app/oracle/oradata/orcl/fsdata01.dbf  \
          oracle@compute_node_IP_address:/u02/app/oracle/oradata/ORCL/PDB2

      $ scp -i private_key_file \
          /u01/app/oracle/oradata/orcl/fsindex01.dbf  \
          oracle@compute_node_IP_address:/u02/app/oracle/oradata/ORCL/PDB2

      $ scp -i private_key_file \
          /u01/app/oracle/oradata/orcl/users01.dbf  \
          oracle@compute_node_IP_address:/u02/app/oracle/oradata/ORCL/PDB2

4. Set the source tablespaces back to READ WRITE.

   a. Invoke SQL*Plus and log in as the SYSTEM user.

   b. Set the user-defined tablespaces back to READ WRITE mode.

      SQL> ALTER TABLESPACE example READ WRITE;
      Tablespace altered.
      SQL> ALTER TABLESPACE fsdata READ WRITE;
      Tablespace altered.
      SQL> ALTER TABLESPACE fsindex READ WRITE;
      Tablespace altered.
      SQL> ALTER TABLESPACE users READ WRITE;
      Tablespace altered.

   c. Exit from SQL*Plus.

5. On the Database service compute node, prepare the PDB for the tablespace import.

   a. On the Database service compute node, invoke SQL*Plus and log in to the PDB as the SYSTEM user.

   b. Create a directory object in the PDB.

      SQL> CREATE DIRECTORY dp_from_source AS '/u01/app/oracle/admin/ORCL/dpdump/from_source';
6. On the Database service compute node, invoke Data Pump Import and connect to the PDB.

   Import the data into the database using the `TRANSPORT_DATAFILES` option.

   ```shell
   $ impdp system@PDB2 FULL=y DIRECTORY=dp_from_source \
   TRANSPORT_DATAFILES="/u02/app/oracle/oradata/ORCL/PDB2/example01.dbf", "/u02/app/oracle/oradata/ORCL/PDB2/fsdata01.dbf", "/u02/app/oracle/oradata/ORCL/PDB2/fsindex01.dbf", "/u02/app/oracle/oradata/ORCL/PDB2/users01.dbf"
   ```

7. After verifying that the data has been imported successfully, you can delete the `expdat.dmp` dump file.

### Data Pump Transportable Tablespace

You can use this method only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Oracle Cloud Infrastructure Database service database are compatible.

The Transportable Tablespace method is generally much faster than a conventional export/import of the same data because the data files containing all of the actual data are simply copied to the destination location. You use Data Pump to transfer only the metadata of the tablespace objects to the new database.

To migrate an on-premises source database to the database deployment on the Database service using the Data Pump Transportable Tablespace method, you perform these tasks:

1. On the on-premises database host, prepare the database for the Data Pump transportable tablespace export.
2. On the on-premises database host, invoke Data Pump Export to perform the transportable tablespace export.
3. Use a secure copy utility to transfer the Data Pump Export dump file and the tablespace datafiles to the Database service compute node.
4. Set the on-premises tablespaces back to `READ WRITE`.
5. On the Database service compute node, prepare the database for the tablespace import.
6. On the Database service compute node, invoke Data Pump Import and connect to the database.
7. Set the tablespaces on the Database service database to `READ WRITE` mode.
8. After verifying that the data has been imported successfully, you can delete the dump file.

### Data Pump Transportable Tablespace: Example

This example provides a step-by-step demonstration of the tasks required to migrate tablespaces in an on-premises Oracle database to a Database service database.

This example performs a migration of the `FSDATA` and `FSINDEX` tablespaces.

In this example, the on-premises database is on a Linux host.

1. On the on-premises database host, prepare the database for the Data Pump transportable tablespace export.
   a. On the on-premises database host, create a directory in the operating system to use for the on-premises export.
      ```bash
      mkdir /u01/app/oracle/admin/orcl/dpdump/for_cloud
      ```
   b. On the on-premises database host, invoke SQL*Plus and log in to the on-premises database as the `SYSTEM` user.
      ```bash
      sqlplus system
      Enter password: <enter the password for the SYSTEM user>
      ```
   c. Create a directory object in the on-premises database to reference the operating system directory.
      ```sql
      SQL> CREATE DIRECTORY dp_for_cloud AS '/u01/app/oracle/admin/orcl/dpdump/for_cloud';
      ```
   d. Determine the name(s) of the datafiles that belong to the `FSDATA` and `FSINDEX` tablespaces by querying `DBA_DATA_FILES`. These files will also be listed in the export output.
      ```sql
      SQL> SELECT file_name FROM dba_data_files
      ```
2  WHERE tablespace_name = 'FSDATA';

FILE_NAME
-----------------------------------------------
/u01/app/oracle/oradata/orcl/fsdata01.dbf

SQL> SELECT file_name FROM dba_data_files
  2  WHERE tablespace_name = 'FSINDEX';

FILE_NAME
-----------------------------------------------
/u01/app/oracle/oradata/orcl/fsindex01.dbf

e. On the on-premises database host, set all tablespaces that will be transported (the transportable set) to READ ONLY mode.

   SQL> ALTER TABLESPACE fsindex READ ONLY;
   Tablespace altered.
   SQL> ALTER TABLESPACE fsdata READ ONLY;
   Tablespace altered.

f. Exit from SQL*Plus.

2. On the on-premises database host, invoke Data Pump Export to perform the transportable tablespace export.

   On the on-premises database host, invoke Data Pump Export and connect to the on-premises database. Export the on-premises tablespaces using the TRANSPORT_TABLESPACES option. Provide the password for the SYSTEM user when prompted.

   expdp system TRANSPORT_TABLESPACES=fsdata,fsindex TRANSPORT_FULL_CHECK=YES DIRECTORY=dp_for_cloud

3. Use a secure copy utility to transfer the Data Pump Export dump file and the tablespace datafiles to the Database service compute node.

   In this example the dump file is copied to the /u01 directory. Choose the appropriate location based on the size of the file that will be transferred.

   a. On the Database service compute node, create a directory for the dump file.

      mkdir /u01/app/oracle/admin/ORCL/dpdump/from_onprem

   b. Before using the scp utility to copy files, make sure the SSH private key that provides access to the Database service compute node is available on your on-premises host.

   c. On the on-premises database host, use the scp utility to transfer the dump file and all datafiles of the transportable set to the Database service compute node.

      scp -i private_key_file \
      /u01/app/oracle/admin/orcl/dpdump/from_cloud/expdat.dmp \ 
      oracle@IP_address_DBaaS_VM:/u01/app/oracle/admin/ORCL/dpdump/from_onprem

      $ scp -i private_key_file \
      /u01/app/oracle/oradata/orcl/fsdata01.dbf \ 
      oracle@IP_address_DBaaS_VM:/u02/app/oracle/oradata/ORCL

      $ scp -i private_key_file \
      /u01/app/oracle/oradata/orcl/fsindex01.dbf \ 
      oracle@IP_address_DBaaS_VM:/u02/app/oracle/oradata/ORCL

4. Set the on-premises tablespaces back to READ WRITE.

   a. Invoke SQL*Plus and log in as the SYSTEM user.

   b. Set the FSDATA and FSINDEX tablespaces back to READ WRITE mode.

      SQL> ALTER TABLESPACE fsdata READ WRITE;
      Tablespace altered.
SQL> ALTER TABLESPACE fsindex READ WRITE;
Tablespace altered.

c. Exit from SQL*Plus.

5. On the Database service compute node, prepare the database for the tablespace import.
   a. On the Database service compute node, invoke SQL*Plus and log in to the database as the SYSTEM user.
   b. Create a directory object in the Database service database.

      SQL> CREATE DIRECTORY dp_from_onprem AS '/u01/app/oracle/admin/ORCL/dpdump/from_onprem';

   c. If the owners of the objects that will be imported do not exist in the database, create them before performing
      the import. The transportable tablespace mode of import does not create the users.

      SQL> CREATE USER fsowner
          2  PROFILE default
          3  IDENTIFIED BY fspass
          4  TEMPORARY TABLESPACE temp
          5  ACCOUNT UNLOCK;

6. On the Database service compute node, invoke Data Pump Import and connect to the database.

   Import the data into the database using the `TRANSPORT_DATAFILES` option.

      impdp system DIRECTORY=dp_from_onprem \
      TRANSPORT_DATAFILES='/u02/app/oracle/oradata/ORCL/fsdata01.dbf', \
      '/u02/app/oracle/oradata/ORCL/fsindex01.dbf'

7. Set the tablespaces on the Database service database to `READ WRITE` mode.
   a. Invoke SQL*Plus and log in as the SYSTEM user.
   b. Set the `FSDATA` and `FSINDEX` tablespaces to `READ WRITE` mode.

      SQL> ALTER TABLESPACE fsdata READ WRITE;
      Tablespace altered.
      SQL> ALTER TABLESPACE fsindex READ WRITE;
      Tablespace altered.

c. Exit from SQL*Plus.

8. After verifying that the data has been imported successfully, you can delete the `expdat.dmp` dump file.

Remote Cloning a PDB

You can use this method only if the on-premises platform is little endian, the on-premises database release is 12.1.0.2
or higher, and the on-premises database and Database service database have compatible database character sets and
national character sets.

You can use the remote cloning method to copy a PDB from your on-premises Oracle Database 12c database to a
PDB in an Oracle Database 12c database on the Database service.

Migration Tasks

To migrate an Oracle Database 12c PDB to a PDB in a Database service database deployment using the remote
cloning method, you perform these tasks:

1. On the on-premises database host, invoke SQL*Plus and close the on-premises PDB and then reopen it in `READ
   ONLY` mode.
2. On the Database service compute node, invoke SQL*Plus and create a database link that enables a connection to
   the on-premises database.
3. On the Database service compute node, execute the `CREATE PLUGGABLE DATABASE` command to clone the
   on-premises PDB.
4. On the Database compute node, open the new PDB by executing the `ALTER PLUGGABLE DATABASE OPEN` command.

5. Optionally, on the on-premises database host invoke SQL*Plus and set the on-premises PDB back to READ WRITE mode.

For more information, see "Cloning a Remote PDB or Non-CDB" in Oracle Database Administrator's Guide for Release 12.2 or 12.1.

**Remote Cloning Non-CDB**

You can use this method only if the on-premises platform is little endian, the on-premises database release is 12.1.0.2 or higher, and the on-premises database and Database service database have compatible database character sets and national character sets.

You can use the remote cloning method to copy an Oracle Database 12c non-CDB on-premises database to a PDB in an Oracle Database 12c database on the Databaseservice.

**Migration Tasks**

To migrate an Oracle Database 12c non-CDB database to a Database service database deployment using the remote cloning method, you perform these tasks:

1. On the on-premises database host, invoke SQL*Plus and set the on-premises database to READ ONLY mode.
2. On the Database service compute node, invoke SQL*Plus and create a database link that enables a connection to the on-premises database.
3. On the Database service compute node, execute the `CREATE PLUGGABLE DATABASE` command to clone the on-premises non-CDB database.
4. On the Database service compute node, execute the `$ORACLE_HOME/rdbms/admin/noncdb_to_pdb.sql` script.
5. On the Database service compute node, open the new PDB by executing the `ALTER PLUGGABLE DATABASE OPEN` command.
6. Optionally, on the on-premises database host invoke SQL*Plus and set the on-premises database back to READ WRITE mode.

For more information, see "Cloning a Remote PDB or Non-CDB" in Oracle Database Administrator's Guide for Release 12.2 or 12.1.

**RMAN Cross-Platform Transportable PDB**

This method can be used only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database service database are compatible.

To migrate an Oracle Database 12c PDB to a PDB in an Oracle Database 12c database on a Database service deployment using the RMAN cross-platform transportable PDB method, you perform these tasks:

1. On the on-premises database host, invoke SQL*Plus and close the on-premises PDB.
2. On the on-premises database host, execute the `ALTER PLUGGABLE DATABASE UNPLUG` command to generate an XML file containing the list of datafiles that will be plugged in on the cloud database.
3. On the on-premises database host, invoke RMAN and connect to the root. Execute the `BACKUP FOR TRANSPORT PLUGGABLE DATABASE` command.
4. Use a secure copy utility to transfer the XML file and the backup set to the Database service compute node.
5. On the Database service compute node, invoke RMAN and connect to the root. Execute the `RESTORE ALL FOREIGN DATAFILES` command.
6. the Database service compute node, invoke SQL*Plus and connect to the root. Execute the `CREATE PLUGGABLE DATABASE` command.
7. the Database service compute node, execute the `ALTER PLUGGABLE DATABASE OPEN` command.

For more information, see "Performing Cross-Platform Data Transport in CDBs and PDBs" in Oracle Database Backup and Recovery User's Guide for Release 12.2 or 12.1.
**RMAN Cross-Platform Transportable Tablespace Backup Sets**

You can use this method only if the database character sets of your on-premises database and the Database service database are compatible.

**Note:**

For detailed information on a similar method that enables you to perform a cross-platform transport of an entire database, see the Oracle Database 12c Backup and Recovery User's Guide for Release 12.2 or 12.1. When you transport an entire database to a different platform, the source platform and the destination platform must use the same endian format.

To migrate Oracle Database 12c on-premises tablespaces to an Oracle Database 12c database on a Database service deployment using the RMAN cross-platform transportable backup sets method, you perform these tasks:

1. On the on-premises database host, prepare the database by placing the user-defined tablespaces that you intend to transport in **READ ONLY** mode.
2. On the on-premises database host, invoke RMAN and use the `BACKUP` command with the **TO PLATFORM** or **FOR TRANSPORT** clause and the `DATAPUMP` clause to create a backup set for cross-platform transport. See in "BACKUP" in Oracle Database Backup and Recovery Reference for Release 12.2 or 12.1 for more information on the BACKUP command.
3. Use a secure copy utility to transfer the backup sets, including the Data Pump export dump file, to the Database service compute node.
4. Set the on-premises tablespaces back to **READ WRITE**.
5. On the Database service compute node, prepare the database by creating the required schemas.
6. On the Database service compute node, invoke RMAN and use the `RESTORE` command with the `foreignFileSpec` subclause to restore the cross-platform backup.
7. On the Database service compute node, set the tablespaces on the database to **READ WRITE** mode.

For more information, see "Overview of Cross-Platform Data Transport Using Backup Sets" in Oracle Database Backup and Recovery User's Guide for Release 12.2 or 12.1.

**RMAN Cross-Platform Transportable Tablespace Backup Sets: Example**

This example provides a step-by-step demonstration of the tasks required to migrate tablespaces in an Oracle Database PDB to a Database service database.

This example performs a migration of the FSDATA and FSINDEX tablespaces.

In this example, the on-premises database is on a Linux host.

1. On the on-premises database host, prepare the database by creating a directory for the export dump file and placing the user-defined tablespaces that you intend to transport in **READ ONLY** mode..
   a. On the on-premises database host, create a directory in the operating system to use for the export dump.
      ```bash
      mkdir /u01/app/oracle/admin/orcl/dpdump/for_cloud
      ```
   b. On the on-premises data host, invoke SQL*Plus and log in to the PDB as the **SYSTEM** user.
      ```sql
      sqlplus system@pdb_servicename
      Enter password: enter the password for the SYSTEM user
      ```
   c. Create a directory object in the on-premises database to reference the operating system directory.
      ```sql
      SQL> CREATE DIRECTORY dp_for_cloud AS '/u01/app/oracle/admin/orcl/dpdump/for_cloud';
      ```
   d. On the on-premises database host, set all tablespaces that will be transported (the transportable set) to **READ ONLY** mode.
      ```sql
      SQL> ALTER TABLESPACE fsindex READ ONLY;
      ```
Database

SQL> ALTER TABLESPACE fsdata READ ONLY;

e. Exit from SQL*Plus.

2. On the on-premises database host, invoke RMAN and use the BACKUP command with the TO PLATFORM or FOR TRANSPORT clause and the DATAPUMP clause to create a backup set for cross-platform transport.

a. On the on-premises database host, create an operating system directory for the datafiles.

```bash
mkdir /u01/app/oracle/admin/orcl/rman_transdest
```

b. Invoke RMAN and log in as a user that has been granted the SYSDBA or SYSBACKUP privilege.

```bash
rman target username@pdb_servicename
```

c. Execute the BACKUP command.

```sql
RMAN> BACKUP FOR TRANSPORT
2> FORMAT '/u01/app/oracle/admin/orcl/rman_transdest/fs_tbs.bck'
3> TABLESPACE fsdata,fsindex
4> DATAPUMP FORMAT '/u01/app/oracle/admin/orcl/rman_transdest/fs_tbs.dmp';
```

d. Log out of RMAN.

e. Optionally, navigate to the directory you specified in the BACKUP command to view the files that were created.

```bash
cd /u01/app/oracle/admin/orcl/rman_transdest
$ ls
fs_tbs.bck  fs_tbs.dmp
```

3. Use a secure copy utility to transfer the backup set, including the Data Pump export dump file, to the Database service compute node.

a. On the Database service compute node, create a directory for the backup set and dump file.

```bash
mkdir /tmp/from_onprem
```

b. Before using the scp command to copy files, make sure the SSH private key that provides access to the Database service compute node is available on your on-premises host.

c. On the on-premises database host, use the SCP utility to transfer the backup set and the dump file to the Database service compute node.

```bash
scp -i private_key_file 
/u01/app/oracle/admin/orcl/rman_transdest/fs_tbs.bck 
oracle@$IP_address_DBaaS_VM:/tmp/from_onprem

$ scp -i private_key_file 
/u01/app/oracle/admin/orcl/rman_transdest/fs_tbs.dmp 
oracle@$IP_address_DBaaS_VM:/tmp/from_onprem
```

4. Set the on-premises tablespaces back to READ WRITE.

a. Invoke SQL*Plus and log in to the PDB as the SYSTEM user.

```sql
SQL> ALTER TABLESPACE fsdata READ WRITE;
SQL> ALTER TABLESPACE fsindex READ WRITE;
```

c. Exit from SQL*Plus.
5. On the Database service compute node, prepare the database by creating the required schemas.
   a. On the Database service compute node, invoke SQL*Plus and log in to the PDB as the SYSTEM user.
   b. If the owners of the objects that will be imported do not exist in the database, create them before performing the RESTORE.

   SQL> CREATE USER fsowner
   2  PROFILE default
   3  IDENTIFIED BY fspass
   4  TEMPORARY TABLESPACE temp
   5  ACCOUNT UNLOCK;

6. On the Database service compute node, invoke RMAN and use the RESTORE command with the foreignFileSpec subclause to restore the cross-platform backup.
   a. Create an operating system directory for the Data Pump Dump file.

   mkdir /tmp/from_onprem

   b. Invoke RMAN and log in to the PDB as a user that has been granted the SYSDBA or SYSBACKUP privilege.

   rman target username@pdb_servicename

   c. Execute the RESTORE command.

   RMAN> RESTORE FOREIGN TABLESPACE fsdata,fsindex TO NEW
   2> FROM BACKUPSET '/tmp/from_onprem/fs_tbs.bck'
   3> DUMP FILE DATAPUMP DESTINATION '/tmp/datapump'
   4> FROM BACKUPSET '/tmp/from_onprem/fs_tbs.dmp';

   d. Exit from RMAN.

7. On the Database service compute node, set the tablespaces to READ WRITE mode.
   a. Invoke SQL*Plus and log in to the PDB as the SYSTEM user.
   b. Set the FSDATA and FSINDEX tablespaces to READ WRITE.

   SQL> ALTER TABLESPACE fsdata READ WRITE;
   SQL> ALTER TABLESPACE fsindex READ WRITE;

   c. Exit from SQL*Plus.

8. After verifying that the data has been imported successfully, you can delete the backup set files that were transported from the on-premises host.

**RMAN Transportable Tablespace with Data Pump**

You can use this method only if the on-premises platform is little endian, and the database character sets of your on-premises database and the Database service database are compatible.

You can use this method to eliminate placing the tablespaces in READ ONLY mode, as required by the Data Pump Transportable Tablespace method.

To migrate an on-premises source database to a database deployment on the Database service using the RMAN Transportable Tablespace with Data Pump method, you perform these tasks:

1. On the on-premises database host, invoke RMAN and create the transportable tablespace set.
2. Use a secure copy utility to transfer the Data Pump Export dump file and the tablespace datafiles to the Database service compute node.
3. On the Database service compute node, prepare the database for the tablespace import.
4. On the Database service compute node, invoke Data Pump Import and connect to the database. Import the data into the database using the TRANSPORT_DATAFILES option.
5. After verifying that the data has been imported successfully, you can delete the dump file.
**RMAN Transportable Tablespace with Data Pump: Example**

This example provides a step-by-step demonstration of the tasks required to migrate tablespaces in an on-premises Oracle database to a Database service database.

This example performs a migration of the **FSDATA** and **FSINDEX** tablespaces.

In this example, the on-premises database is on a Linux host.

1. On the on-premises database host, invoke RMAN and create the transportable tablespace set.
   
   a. On the on-premises database host, create an operating system directory for the datafiles.
      
      ```bash
      mkdir /u01/app/oracle/admin/orcl/rman_transdest
      ```
   
   b. On the on-premises data host, create an operating system directory for the RMAN auxiliary instance files.
      
      ```bash
      mkdir /u01/app/oracle/admin/orcl/rman_auxdest
      ```
   
   c. Invoke RMAN and log in as the **SYSTEM** user. Enter the password for the **SYSTEM** user when prompted.
      
      ```bash
      rman target system
      ```
   
   d. Execute the **TRANSPORT TABLESPACE** command.
      
      ```bash
      RMAN> TRANSPORT TABLESPACE fsdata, fsindex
      2> TABLESPACE DESTINATION '/u01/app/oracle/admin/orcl/rman_transdest'
      3> AUXILIARY DESTINATION '/u01/app/oracle/admin/orcl/rman_auxdest';
      ```
   
   e. Log out of RMAN.
   
   f. Optionally, navigate to the directory you specified for the TABLESPACE DESTINATION and view the files that were created by the TRANSPORT TABLESPACE operation.
      
      ```bash
      cd /u01/app/oracle/admin/orcl/rman_transdest
      $ ls
      dmpfile.dmp fsdata01.dbf fsindex01.dbf impscrpt.sql
      ```

2. Use a secure copy utility to transfer the Data Pump Export dump file and the tablespace datafiles to the Database service compute node.

   In this example the dump file is copied to the `/u01` directory. Choose the appropriate location based on the size of the file that will be transferred.
   
   a. On the Database service compute node, create a directory for the dump file.
      
      ```bash
      mkdir /u01/app/oracle/admin/ORCL/dpdump/from_onprem
      ```
   
   b. Before using the `scp` command to copy files, make sure the SSH private key that provides access to the Database service compute node is available on your on-premises host.
   
   c. On the on-premises database host, use the SCP utility to transfer the dump file and all datafiles of the transportable set to the Database service compute node.
      
      ```bash
      scp -i private_key_file  
      /u01/app/oracle/admin/orcl/rman_transdest/dmpfile.dmp  
      oracle@IP_address_DBaaS_VM:/u01/app/oracle/admin/ORCL/dpdump/from_onprem
      $ scp -i private_key_file  
      /u01/app/oracle/admin/orcl/rman_transdest/fsdata01.dbf  
      oracle@IP_address_DBaaS_VM:/u02/app/oracle/oradata/ORCL
      $ scp -i private_key_file  
      /u01/app/oracle/admin/orcl/rman_transdest/fsindex01.dbf  
      oracle@IP_address_DBaaS_VM:/u02/app/oracle/oradata/ORCL
      ```
3. On the Database service compute node, prepare the database for the tablespace import.
   a. On the Database service compute node, invoke SQL*Plus and log in to the database as the SYSTEM user.
   b. Create a directory object in the Database service database.

   ```sql
   SQL> CREATE DIRECTORY dp_from_onprem AS '/u01/app/oracle/admin/ORCL/dpdump/from_onprem';
   ```
   c. If the owners of the objects that will be imported do not exist in the database, create them before performing
      the import. The transportable tablespace mode of import does not create the users.

   ```sql
   SQL> CREATE USER fsowner
       2   PROFILE default
       3   IDENTIFIED BY fsa
       4   TEMPORARY TABLESPACE temp
       5   ACCOUNT UNLOCK;
   ```

4. On the Database service compute node, invoke Data Pump Import and connect to the database.

   Import the data into the database using the `TRANSPORT_DATAFILES` option.

   ```sql
   impdp system DIRECTORY=dp_from_onprem DUMPFILE='dmpfile.dmp' \
   TRANSPORT_DATAFILES='/u02/app/oracle/oradata/ORCL/fsdata01.dbf', \
   '/u02/app/oracle/oradata/ORCL/fsindex01.dbf'
   ```

5. After verifying that the data has been imported successfully, you can delete the `dmpfile.dmp` dump file.

**RMAN CONVERT Transportable Tablespace with Data Pump**

You can use this method only if the database character sets of your on-premises database and the Database service

database are compatible.

This method is similar to the Data Pump Transportable Tablespace method, with the addition of the

RMAN `CONVERT` command to enable transport between platforms with different endianness. Query `V

$TRANSPORTABLE_PLATFORM` to determine if the on-premises database platform supports cross-platform
tablespace transport and to determine the endian format of the platform. The Database service platform is little-endian
format.

To migrate tablespaces from your on-premises Oracle database to a database deployment on the Database service
using RMAN, you perform these tasks:

1. On the on-premises database host, prepare the database for the Data Pump transportable tablespace export.
2. On the on-premises database host, invoke Data Pump Export to perform the transportable tablespace export.
3. On the on-premises database host, invoke RMAN and use the `CONVERT TABLESPACE` command to convert the
   tablespace datafile to the Database service platform format. Refer to the Oracle Database Backup and Recovery
   Reference for more information on the `CONVERT` command.
4. Use a secure copy utility to transfer the Data Pump Export dump file and the converted tablespace datafiles to the
   Database service compute node.
5. Set the on-premises tablespaces back to `READ WRITE`.
6. On the Database service compute node, prepare the database for the tablespace import.
7. On the Database service compute node, invoke Data Pump Import and connect to the database.
8. On the Database service compute node, set the tablespaces in the database to `READ WRITE` mode.
9. After verifying that the data has been imported successfully, you can delete the dump file.

**RMAN CONVERT Transportable Tablespace with Data Pump: Example**

This example provides a step-by-step demonstration of the tasks required to migrate tablespaces in an on-premises
Oracle database to a Database service database.

In this example, the on-premises database is on a Linux host.
1. On the on-premises database host, prepare the database for the Data Pump transportable tablespace export.
   a. On the on-premises database host, create a directory in the operating system to use for the on-premises export.
      
      ```bash
      mkdir /u01/app/oracle/admin/orcl/dpdump/for_cloud
      ```
   b. On the on-premises database host, invoke SQL*Plus and log in to the on-premises database as the `SYSTEM` user.
      
      ```sql
      sqlplus system
      Enter password: <enter the password for the SYSTEM user>
      ```
   c. Create a directory object in the on-premises database to reference the operating system directory.
      
      ```sql
      SQL> CREATE DIRECTORY dp_for_cloud AS '/u01/app/oracle/admin/orcl/dpdump/for_cloud';
      ```
   d. On the on-premises database host, set all tablespaces that will be transported (the transportable set) to READ ONLY mode.
      
      ```sql
      SQL> ALTER TABLESPACE fsindex READ ONLY;
      Tablespace altered.
      SQL> ALTER TABLESPACE fsdata READ ONLY;
      Tablespace altered.
      ```
   e. Exit from SQL*Plus.

2. On the on-premises database host, invoke Data Pump Export to perform the transportable tablespace export.
   On the on-premises database host, invoke Data Pump Export and connect to the on-premises database. Export the on-premises tablespaces using the `TRANSPORT_TABLESPACES` option. Provide the password for the `SYSTEM` user when prompted.
      
      ```sql
      expdp system TRANSPORT_TABLESPACES=fsdata,fsindex TRANSPORT_FULL_CHECK=YES DIRECTORY=dp_for_cloud
      ```

3. On the on-premises database host, invoke RMAN and use the `CONVERT TABLESPACE` command to convert the tablespace datafile to the Database service platform format.
   a. Invoke RMAN.
      
      ```sql
      rman target /
      ```
   b. Execute the RMAN `CONVERT TABLESPACE` command to convert the datafiles and store the converted files in a temporary location on the on-premises database host.
      
      ```sql
      RMAN> CONVERT TABLESPACE fsdata, fsindex
      2> TO PLATFORM 'Linux x86 64-bit'
      3> FORMAT '/tmp/%U ';
      ...
      input datafile file number=00006 name=/u01/app/oracle/oradata/orcl/fsdata01.dbf
      converted datafile=/tmp/data_D-ORCL_I-1410251631_TS-FSDATA_FNO-6_0aqc9un3
      ...
      input datafile file number=00007 name=/u01/app/oracle/oradata/orcl/fsindex01.dbf
      converted datafile=/tmp/data_D-ORCL_I-1410251631_TS-FSINDEX_FNO-7_0bqc9un6
      ...
      ```
   c. Take note of the names of the converted files. You will copy these files to the Database service compute node in the next step.
   d. Exit RMAN.
4. Use a secure copy utility to transfer the Data Pump Export dump file and the converted tablespace datafiles to the Database service compute node.

   In this example the dump file is copied to the /u01 directory. Choose the appropriate location based on the size of the file that will be transferred.

   a. On the Database service compute node, create a directory for the dump file.

   

   ```
   mkdir /u01/app/oracle/admin/ORCL/dpdump/from_onprem
   ```

   b. Before using the `scp` command to copy files, make sure the SSH private key that provides access to the Database service compute node is available on your on-premises host.

   c. On the on-premises database host, use the `scp` utility to transfer the dump file and all data files of the transportable set to the Database service compute node.

   ```
   scp -i private_key_file 
   /u01/app/oracle/admin/orcl/dpdump/for_cloud/expdat.dmp 
   oracle@IP_address_DBaaS_VM:/u01/app/oracle/admin/ORCL/dpdump/from_onprem
   
   $ scp -i private_key_file 
   /tmp/data_D-ORCL_I-1410251631_TS-FSDATA_FNO-6_0aqc9un3 
   oracle@IP_address_DBaaS_VM:/u02/app/oracle/oradata/ORCL/fsdata01.dbf
   
   $ scp -i private_key_file 
   /tmp/data_D-ORCL_I-1410251631_TS-FSINDEX_FNO-7_0bqc9un6 
   oracle@IP_address_DBaaS_VM:/u02/app/oracle/oradata/ORCL/fsindex01.dbf
   ```

5. Set the on-premises tablespaces back to READ WRITE.

   a. Invoke SQL*Plus and log in as the SYSTEM user.

   b. Set the FSDATA and FSINDEX tablespaces back to READ WRITE mode.

   ```
   SQL> ALTER TABLESPACE fsdata READ WRITE;
   Tablespace altered.
   SQL> ALTER TABLESPACE fsindex READ WRITE;
   Tablespace altered.
   ```

   c. Exit from SQL*Plus.

6. On the Database service compute node, prepare the database for the tablespace import.

   a. On the Database service compute node, invoke SQL*Plus and log in to the database as the SYSTEM user.

   b. Create a directory object in the Database service database.

   ```
   SQL> CREATE DIRECTORY dp_from_onprem AS '/u01/app/oracle/admin/ORCL/ 
   dpdump/from_onprem';
   ```

   c. If the owners of the objects that will be imported do not exist in the database, create them before performing the import. The transportable tablespace mode of import does not create the users.

   ```
   SQL> CREATE USER fsowner
   2  PROFILE default
   3  IDENTIFIED BY fspass
   4  TEMPORARY TABLESPACE temp
   5  ACCOUNT UNLOCK;
   ```

7. On the Database service compute node, invoke Data Pump Import and connect to the database.

   Import the data into the Database service database using the `TRANSPORT_DATAFILES` option.

   ```
   impdp system DIRECTORY=dp_from_onprem 
   TRANSPORT_DATAFILES='/u02/app/oracle/oradata/ORCL/fsdata01.dbf', 
   '/u02/app/oracle/oradata/ORCL/fsindex01.dbf'
   ```
8. On the Database service compute node, set the tablespaces in the database to READ WRITE mode.
   a. Invoke SQL*Plus and log in as the SYSTEM user.
   b. Set the FSDATA and FSINDEX tablespaces to READ WRITE mode.

```sql
SQL> ALTER TABLESPACE fsdata READ WRITE;
Tablespace altered.
SQL> ALTER TABLESPACE fsindex READ WRITE;
Tablespace altered.
```
   c. Exit from SQL*Plus.

9. After verifying that the data has been imported successfully, you can delete the expdat.dmp dump file.

RMAN DUPLICATE from an Active Database

This topic explains how to migrate an entire, active container database (CDB) or non-CDB database to Oracle Cloud Infrastructure by using RMAN Active Duplication. The database to be migrated can reside on-premises or in Oracle Cloud Infrastructure Classic. This topic does not cover duplicating a pluggable database, or migrating a pluggable database or non-CDB to a CDB in the cloud.

The following terms are used throughout this topic:

- **Source database**: The active database to be migrated.
- **Target database**: The new database (duplicated from the source database) on a DB system in the Oracle Cloud Infrastructure.

**Note:**

Version 11.2.0.4 databases running on bare metal DB systems will be migrated to a DB system using ACFS storage.

**Prerequisites**

For the source database to be migrated, you'll need:

- The source database name, database unique name, listener port, service name, database home patch level, and the password for SYS.
- A copy of the sqlpatch directory from the source database home. This is required for rollback in case the target DB system does not include these patches.
- If the source database is configured with Transparent Data Encryption (TDE), you'll need a backup of the wallet and the wallet password to allow duplication of a database with encrypted data.

When migrating a source database to an existing target database, Oracle recommends that you patch the source environment to the same database bundle patch level as the target database home. If the source environment has an interim patch (previously known as a "one-off" patch) that includes a sqlpatch component, and that sqlpatch is missing from the target environment (or a different cumulative patch is applied), the interim patch should be rolled back in the source environment before the migration, if possible.

**Tip:**

To check for interim patches installed on the source or target database, use the `$ORACLE_HOME/OPatch/opatch lspatches` command. To roll back SQL changes in the target database, copy the `$ORACLE_HOME/sqlpatch/&lt;patch#&gt;/postdeinstall.sql` script from the source environment to the cloud environment and execute the `postdeinstall.sql` script.

For the target database, you'll need:

- A target DB system that supports the same database edition as the source database edition. When you launch a DB system, an initial database is created on it. If necessary, you can delete that database and create a new one by using the dbcli command line interface. For more information on creating a DB system, see Creating Bare Metal
• The target database name, database unique name, auxiliary service name, and database home patch level.
• A free TCP port in the target database to setup the auxiliary instance.

If you need to roll back interim patches in the target environment so that the patch level matches that of the source environment, copy the source DB $ORACLE_HOME/sqlpatch/<patch_number> directory to the target database home.

**Migrating Source Databases That Include Patch Set Updates (PSUs)**

In Oracle Cloud Infrastructure DB systems, the database home includes an installation of Database Proactive Bundle Patches. If the source DB uses Patch Set Updates (PSUs), follow the instructions in MOS Note:1962125.1 (Oracle Database - Overview of Database Patch Delivery Methods) for migrating the DB into Oracle Cloud Infrastructure.

**Verifying the Environment**

Perform the following steps before you begin the migration:

1. Make sure the source DB system is reachable from the target DB system. You should be able to SSH between the two hosts.
2. On the target host, use the TNSPING utility to make sure the source host listener port works. For example:

   ```
   tnsping <source_host>:1521
   ```

3. On the target host, use Easy Connect to verify the connection to the source database:

   ```
   <host>:<port>/<service_name>
   ```

   For example:

   ```
   sqlplus system@129.145.0.164:1521/proddb
   ```

   Make sure the connection string does not exceed 64 characters.

4. Copy the required sqlpatch files (for rollback) from the source database home to the target database.
5. Make sure at least one archivelog has been created on the source database, otherwise, the RMAN duplication will fail with an error.
6. If the source database uses wallets, back up the password-based wallet and copy it to the standard location in the DB system:

   ```
   /opt/oracle/dcs/commonstore/wallets/tde/<db_unique_name>/
   ```

7. Make sure the compatibility parameters in the source database are set to at least:

   - 18.0.0.0.0 for an 18.1.0.0 database
   - 12.1.0.2.0 for a 12.1.0.2 or a 12.2.0.1 database
   - 11.2.0.4.0 for an 11.2.0.4 database

**Setting Up Storage on the DB System**

1. SSH to the DB System.

   ```
   ssh -i <private_key_path> opc@<db_system_ip_address>
   ```

2. Log in as opc and then sudo to the root user. Use sudo su – with a hyphen to invoke the root user's profile, which will set the PATH to the dbcli directory (/opt/oracle/dcs/bin).

   ```
   login as: opc
   ```
Use the Dbstorage Commands on page 1521 to set up directories for DATA, RECO, and REDO storage. The following example creates 10GB of ACFS storage for the tdest database.

```
[root@dbsys ~]# dbcli create-dbstorage --dbname tdest --dataSize 10 -- dbstorage ACFS
```

**Note:**
When migrating a version 11.2 database, ACFS storage must be specified.

4. Use the Dbstorage Commands on page 1521 command to list the storage ID. You'll need the ID for the next step.

```
[root@dbsys ~]# dbcli list-dbstorages
```

```
ID                                       Type   DBUnique Name
---------------------------------------- ------ --------------------
---------
9dcdfb8e-e589-4d5f-861a-e5ba981616ed     Acfs   tdest
Configured
```

5. Use the Dbstorage Commands on page 1521 command with the storage ID from the previous step to list the DATA, RECO and REDO locations.

```
[root@dbsys ~]# dbcli describe-dbstorage --id 9dcdfb8e-e589-4d5f-861a-e5ba981616ed
```

```
DBStorage details
------------------
ID: 9dcdfb8e-e589-4d5f-861a-e5ba981616ed
DB Name: tdest
DBUnique Name: tdest
DB Resource ID:
  Storage Type: Acfs
  DATA Location: /u02/app/oracle/oradata/tdest
  RECO Location: /u03/app/oracle/fast_recovery_area/
  REDO Location: /u03/app/oracle/redo/
  State: ResourceState(status=Configured)
Created: August 24, 2016 5:25:38 PM UTC
UpdatedTime: August 24, 2016 5:25:53 PM UTC
```

Note the locations. You'll use them later to set the `db_create_file_dest`, `db_create_online_log_dest`, and `db_recovery_file_dest` parameters for the database.

**Choosing an ORACLE_HOME**

Decide which ORACLE_HOME to use for the database restore and then switch to that home with the correct ORACLE_BASE, ORACLE_HOME, and PATH settings.

To get a list of existing ORACLE_HOMEs, use the Dbhome Commands on page 1518 command. To create a new ORACLE_HOME, use the Dbhome Commands on page 1518 command.

**Copying the Source Database Wallets**

Skip this section if the source database is not configured with TDE.

1. On the DB system, become the oracle user:

```
sudo su - oracle
```

2. Create the following directory if it does not already exist:

```
mkdir /opt/oracle/dcs/commonstore/wallets/tde/<db_unique_name>
```
3. Copy the ewallet.p12 file from the source database to the directory you created in the previous step.

4. On the target host, make sure that $ORACLE_HOME/network/admin/sqlnet.ora contains the following line:

   ```
   ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/
   opt/oracle/dcs/commonstore/wallets/tde/$ORACLE_UNQNAME)))
   ```

   Add the line if it doesn't exist in the file. (The line might not be there if this is a new home and no database has been created yet on this host.)

5. Create the autologin wallet from the password-based wallet to allow auto-open of the wallet during restore and recovery operations.

   For version 12c, use the `ADMINISTER KEY MANAGEMENT` command:

   ```bash
   $ cat create_autologin_12.sh
   
   #!/bin/sh
   if [ $# -lt 2 ]; then
     echo "Usage: $0 <db_unique_name> <remote_wallet_location>"
     exit 1;
   fi
   mkdir /opt/oracle/dcs/commonstore/wallets/tde/$1
   cp $2/ewallet.p12* /opt/oracle/dcs/commonstore/wallets/tde/$1
   rm -f autokey.ora
   echo "db_name=$1" > autokey.ora
   autokeystoreLog="autologinKeystore_`date +%Y%m%d_%H%M%S_%N`.log"
   echo "Enter Keystore Password:" read -s keystorePassword
   echo "Creating AutoLoginKeystore -> "
   sqlplus "/as sysdba" <<EOF
   spool $autokeystoreLog
   set echo on
   startup nomount pfile=autokey.ora
   ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE
   FROM KEYSTORE '/opt/oracle/dcs/commonstore/wallets/tde/$1' -- Keystore
   location
   IDENTIFIED BY "$keystorePassword";
   shutdown immediate;
   EOF
   ```

   For version 11g, use the `orapki` command:

   `orapki wallet create -wallet wallet_location -auto_login [-pwd <password>]`

### Setting Up the Static Listener

Set up the static listener for the auxiliary instance for RMAN duplication.

1. On the DB system, create `$ORACLE_HOME/network/admin/listener.ora` and add the following content to it.

   ```
   LISTENER_aux_<db_unique_name> =
   (DESCRIPTION=
     (ADDRESS_LIST=
       (ADDRESS=(PROTOCOL=TCP)(HOST=<hostname> or <ip_address>)(PORT=<available_TCP_port>))
     )
   )
   SID_LIST_LISTENER_aux_<db_unique_name> =
   (SID_LIST=
     (SID_DESC=
   ```
(GLOBAL_DBNAME=<auxServiceName_with_domain>)
(ORACLE_HOME=<Oracle_home_for_target_database>)
(SID_NAME=<database_name>)
(ENVS="TNS_ADMIN=<path_to_tnsnames.ora>")
(ENVS="ORACLE_UNQNAME=<db_unique_name(in lower case)>")
)

2. Make sure the port specified in (PORT=<available_TCP_port>) is open in the DB system's iptables and in the DB system's cloud network Security List.

Using the RMAN Duplicate Command to Migrate the Database

1. Set the following environment variables for RMAN and SQL Plus sessions for the database:

   ORACLE_HOME=<path_of_Oracle_home_where_the_database_is_to_be_restored>
   ORACLE_SID=<database_name>
   ORACLE_UNQNAME=<db_unique_name(in lower case)>
   NLS_DATE_FORMAT="mm/dd/yyyy hh24:mi:ss"

2. Start the listener:

   lsnrctl start listener_aux_<db_unique_name>

3. Create an init.ora file with the minimal required parameters as described in Creating an Initialization Parameter File and Starting the Auxiliary Instance and use it for the auxiliary instance.

4. Start the auxiliary instance in nomount mode:

   startup nomount

5. Run the following commands to duplicate the database. Note that the example below uses variables to indicate the values to be specified:

   rman target sys/$sourceSysPassword@$sourceNode:$sourceListenerPort/
   $sourceDb auxiliary sys/$auxSysPassword@$targetNode:$targetListenerPort/
   $auxService<<EOF
   spool log to "`date +%Y%m%d_%H%M%S_%N`_duplicate_"=
   $targetDbUniqueName}_from_"$sourceDb).log"
   set echo on
   duplicate target database to $targetDb from active database
   password file
   spfile
   PARAMETER_VALUE_CONVERT $sourceDb $targetDb $sourceDbUniqueNameCaps
   $targetDbUniqueNameCaps
   set cluster_database='false'
   set db_name='$targetDb'
   set db_unique_name='$targetDbUniqueName'
   set db_create_file_dest='$dataLoc'
   set db_create_online_log_dest_1='$redoLoc'
   set db_recovery_file_dest='$recoLoc'
   set audit_file_dest = '$auditFileDest'
   reset control files
   nofilenamesearch
; EOF

Preparing to Register the Database

Before you register the database:
1. Make sure the database COMPATIBLE parameter value is acceptable.
   For a 11.2 database, the minimum compatibility value is 11.2.0.4.
   For a 12c database, the minimum compatibility value is 12.1.0.2.
   If the value is less than the minimum, the database cannot be registered until you upgrade the database compatibility.

2. Use the following command to verify that the database has registered with the local listener and service name.
   
   ```bash
   lsnrctl services
   ```

3. Use the following command to verify that the password file was restored or created for a new database.
   
   ```bash
   ls -ltr $ORACLE_HOME/dbs/orapw<$ORACLE_SID>
   ```
   If the file does not exist, create it using the orapwd command.
   
   ```bash
   orapwd file=<$ORACLE_HOME/dbs/orapw<$ORACLE_SID>> password=<sys_password>
   ```

4. Use the following command to verify that the restored database is open in read write mode.
   
   ```sql
   select open_mode from v$database;
   ```
   Read write mode is required to register the database later. Any PDBs must also be in read write mode.

5. From oracle home on the migrated database host, use the following command verify the connection to SYS.
   
   ```bash
   conn sys/<password>@<service_name> as sysdba
   ```
   This connection is required to register the database later. Fix any connection issues before continuing.

6. Copy the folder $ORACLE_HOME/sqlpatch from source database to the target database. This will enable the 
dbcli register-database command to rollback any conflicting patches.

   **Note:**
   If you are migrating a version 11.2 database, additional steps are required
   after you register the database. For more information, see Rolling Back
   Patches on a Version 11.2 Database on page 1642.

7. Use the following SQL*Plus command to make sure the database is using the spfile.
   
   ```sql
   SHOW PARAMETERS SPFILE
   ```

---

### Registering the Database on the DB System

The Database Commands on page 1505 command registers the migrated database to the dcs-agent so it can be managed by the dcs-agent stack.

**Note:**
The `dbcli register-database` command is not available on 2-node RAC DB Systems.

As the root user, use the `dbcli register-database` command to register the database on the DB system, for example:

```bash
[root@dbsys ~]# dbcli register-database --dbclass OLTP --dbshape odb1 --servicename crmdb.example.com --syspassword
Password for SYS:
{
  "jobId" : "317b430f-ad5f-42ae-bb07-13f053d266e2",
  "status" : "Created",
  "message" : null,
}
Migrating a Version 12.1 or Later Database That Includes SQL Patch Components

For a 1-node DB system at version 12.1 or higher, the `dbcli register-database` command automates the datapatch execution. Before executing the `dbcli register-database` command, open all PDBs in read-write mode. If you have already run the `dbcli register-database` command and did not open all PDBs, or did not copy the SORACLE_HOME/sqlpatch directory from the source database home, manually rerun the datapatch utility to configure the SQL portion of existing interim patches. This can be done by executing the command 

```bash
$ORACLE_HOME/OPatch/opatch datapatch
```

Tip:  
If the source database includes patch 23170620 and the target database is running with the October 2017 patch or a later one, the `$ORACLE_HOME/sqlpatch` directory does not need to be copied to the target database, because the contents of the patch are already installed in the target database.

Rolling Back Patches on a Version 11.2 Database

For version 11.2 databases, the sqlpatch application is not automated, so any interim patches (previously known as a "one-off" patches) applied to the source database that are not part of the installed PSU must be rolled back manually in the target database. After registering the database, execute the `catbundle.sql` script and then the `postinstall.sql` script with the corresponding PSU patch (or the overlay patch on top of the PSU patch), as described below.

Tip:  
Some interim patches may include files written to the SORACLE_HOME/rdbms/admin directory as well as the SORACLE_HOME/sqlpatch directory. Oracle recommends that you roll back these patches in the source database using the instructions in the patch read-me prior to migrating the database to OCI environment. Contact Oracle Support if you need assistance with rolling back these patches.

1. On the DB System, use the `dbcli list-dbhomes` command to find the PSU patch number for the version 11.2 database home. In the following sample command output, the PSU patch number is the second number in the DB Version column:

```bash
[root@dbsys ~]# dbcli list-dbhomes
ID                                   Name               DB Version
Home Location                             Status
------------------------------------ -----------------  
-------------------------------------  ----------
59d9bc6f-3880-4d4f-b5a6-c140f16f8c64 OraDB11204_home1 11.2.0.4.160719
(23054319, 23054359)   /u01/app/oracle/product/11.2.0.4/dbhome_1
Configured
```

(The first patch number, 23054319 in the example above, is for the OCW component in the database home.)

2. Find the overlay patch, if any, by using the `lsinventory` command. In the following example, patch number 24460960 is the overlay patch on top of the 23054359 PSU patch.

```bash
$ $ORACLE_HOME/OPatch/opatch lsinventory ...
```
Installed Top-level Products (1):

Oracle Database 11g
11.2.0.4.0

There are 1 products installed in this Oracle Home.

Interim patches (5):

Patch 24460960: applied on Fri Sep 02 15:28:17 UTC 2016
Unique Patch ID: 20539912
Created on 31 Aug 2016, 02:46:31 hrs PST8PDT
Bugs fixed:
23513711, 23065323, 21281607, 24006821, 23315889, 22551446, 21174504
This patch overlays patches:
23054359
This patch needs patches:
23054359
as prerequisites

3. Start SQL*Plus and execute the catbundle.sql script, for example:

```sql
SQL> startup
SQL> connect / as sysdba
SQL> @$ORACLE_HOME/rdbms/admin/catbundle.sql psu apply
exit
```

4. Apply the sqlpatch, using the overlay patch number from the previous step, for example:

```sql
SQL> connect / as sysdba
SQL> @$ORACLE_HOME/sqlpatch/24460960/postinstall.sql
exit
```

Creating a Backup Configuration (Optional)

If you would like to manage the database backup with the dbcli command line interface, you can associate a new or existing backup configuration with the migrated database when you register it or after you register it. A backup configuration defines the backup destination and recovery window for the database. As the root user, use the following commands to create, list, and display backup configurations:

- [Backupconfig Commands](#) on page 1491
- [Backupconfig Commands](#) on page 1491
- [Backupconfig Commands](#) on page 1491

Post Migration Checklist

After the database is migrated and registered on the DB system, use the following checklist to verify the results of the migration and perform any post-migration customizations.

1. Make sure the database files were restored in OMF format.
2. Make sure the database is listed in the [Database Commands](#) on page 1505 command output.
3. Check for the following external references in the database and update them if necessary:
   - External tables: If the source database uses external tables, back up that data and migrate it to the target host.
   - Directories: Customize the default directories as needed for the migrated database.
   - Database links: Make sure all the required TNS entries are updated in the tnsnames.ora file in ORACLE_HOME.
   - Email and URLs: Make sure any email addresses and URLs used in the database are still accessible from the DB system.
   - Scheduled jobs: Review the jobs scheduled in source database and schedule similar jobs as needed in the migrated database.
4. If you associated a backup configuration when you registered the database, run a test back up using the Backup Commands on page 1487 command.
5. Verify that patches have been applied to all PDBs if the migrated database contains CDB and PDBs.
6. Validate the database performance by using Database Replay and SQL Performance Analyzer for SQL. For more information, see the Database Testing Guide.

**SQL Developer and INSERT Statements to Migrate Selected Objects**

You can use SQL Developer to create a cart into which you add selected objects to be loaded into an Oracle Database 12c database in the Oracle Cloud Infrastructure Database service.

In this method, you use SQL INSERT statements to load the data into your cloud database.

To migrate selected objects to an Oracle Database 12c database in a Database service deployment using SQL Developer and INSERT statements, you perform these tasks:

1. Launch SQL Developer, connect to your on-premises database and create a cart containing the objects you want to migrate.
2. In SQL Developer, click the Export Cart icon and select “Insert” in the Format menu.
3. In SQL Developer, open a connection to the Oracle Database 12c database in the Database service and execute the generated script to create the database objects.
4. In SQL Developer, open a connection to the Oracle Database 12c database in the Database service and run the generated script to create the objects and load the data.

**SQL Developer and SQL*Loader to Migrate Selected Objects**

You can use SQL Developer to create a cart into which you add selected objects to be loaded into an Oracle Database 12c database in the Oracle Cloud Infrastructure Database.

In this method, you use SQL*Loader to load the data into your cloud database.

To migrate selected objects to an Oracle Database 12c database in the Database service deployment using SQL Developer and SQL*Loader, you perform these tasks:

1. Launch SQL Developer, connect to your on-premises database and create a cart containing the objects you want to load into your cloud database.
2. In SQL Developer, click the Export Cart icon and select “loader” in the Format menu.
3. In SQL Developer, open a connection to the Oracle Database 12c database on the Database service and execute the generated script to create the database objects.
4. Use a secure copy utility to transfer the SQL*Loader control files and the SQL*Loader data files to the Database service compute node.
5. On the Database service compute node, invoke SQL*Loader to load the data using the SQL*Loader control files and data files for each object.

**Unplugging/Plugging a PDB**

You can use this method only if the on-premises platform is little endian, and the on-premises database and the Oracle Cloud Infrastructure Database service database have compatible database character sets and national character sets.

You can use the unplug/plug method to migrate an Oracle Database 12c PDB to a PDB in an Oracle Database 12c database on a Database service database deployment.

To migrate an Oracle Database 12c PDB to a PDB in the Oracle Database 12c database on an Oracle Cloud Infrastructure Database service database deployment using the plug/unplug method, you perform these tasks:

1. On the on-premises database host, invoke SQL*Plus and close the on-premises PDB.
2. On the on-premises database host, execute the ALTER PLUGGABLE DATABASE UNPLUG command to generate an XML file containing the list of datafiles that will be plugged in to the database on the Database service.
3. Use a secure copy utility to transfer the XML file and the datafiles to the Databaseservice compute node.
4. On the Database service compute node, invoke SQL*Plus and execute the `CREATE PLUGGABLE DATABASE` command to plug the database into the CDB.

5. On the Database service compute node, open the new PDB by executing the `ALTER PLUGGABLE DATABASE OPEN` command.

For more information, see "Creating a PDB by Plugging an Unplugged PDB into a CDB" in *Oracle Database Administrator's Guide* for Release 12.2 or 12.1.

### Unplugging/Plugging Non-CDB

You can use this method only if the on-premises platform is little endian, and the on-premises database and the Oracle Cloud Infrastructure Database database have compatible database character sets and national character sets.

You can use the unplug/plug method to migrate an Oracle Database 12c non-CDB database to a PDB in an Oracle Database 12c database on a Database service database deployment. This method provides a way to consolidate several non-CDB databases into a single Oracle Database 12c multitenant database on the Database service.

To migrate an Oracle Database 12c non-CDB database to the Oracle Database 12c database on a Database service deployment using the plug/unplug method, you perform these tasks:

1. On the on-premises database host, invoke SQL*Plus and set the on-premises database to `READ ONLY` mode.
2. On the on-premises database host, execute the `DBMS_PDB.DESCRIBE` procedure to generate an XML file containing the list of datafiles that will be plugged in on the cloud database.
3. Use a secure copy utility to transfer the XML file and the datafiles to the Database service compute node.
4. On the Database service compute node, invoke SQL*Plus and execute the `CREATE PLUGGABLE DATABASE` command to plug the database into the CDB.
5. On the Database service compute node, execute the `$ORACLE_HOME/rdbms/admin/noncdb_to_pdb.sql` script to delete unnecessary metadata from the `SYSTEM` tablespace of the new PDB.
6. On the Database service compute node, open the new PDB by executing the `ALTER PLUGGABLE DATABASE OPEN` command.
7. Optionally, on the on-premises database host invoke SQL*Plus and set the on-premises database back to `READ WRITE` mode.

For more information, see "Creating a PDB Using a Non-CDB" in *Oracle Database Administrator's Guide* for Release 12.2 or 12.1.

### Troubleshooting

These topics cover some common issues you might run into and how to address them.

#### Bare Metal and Virtual Machine DB Systems

- Backup Failures on Bare Metal and Virtual Machine DB Systems on page 1646
- Patching Failures on Bare Metal and Virtual Machine DB Systems on page 1659
- Shape Change Failures for Virtual Machine DB Systems on page 1663

#### Exadata DB Systems

- Backup Failures on Exadata DB Systems on page 1665

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For bare metal and VM DB systems, you can create serial console connections to troubleshoot your system in single-user mode. See To create a serial console connection to your database system on page 1387 for information on creating a serial console connection in the Oracle Cloud Infrastructure Console.</td>
</tr>
</tbody>
</table>
Backup Failures on Bare Metal and Virtual Machine DB Systems

Database backups can fail for various reasons. Typically, a backup fails because either the database host cannot access the object store, or there are problems on the host or with the database configuration.

This topic includes information to help you determine the cause of a failure and fix the problem. The section that includes troubleshooting information is organized into several subsections, based on the error condition. If you already know the cause, you can skip to the section with the suggested solution. Otherwise, use the procedure in Finding the Problem on page 1646 to get started.

Finding the Problem

In the Console, a failed database backup either displays a status of Failed or hangs in the Backup in Progress or Creating state. If the error message does not contain enough information to point you to a solution, you can use the database CLI and log files to gather more data. Then, refer to the applicable section in this topic for a solution.

To identify the root cause of the backup failure

1. Log on to the host as the root user and navigate to /opt/oracle/dcs/bin/.
2. Determine the sequence of operations performed on the database.
   
   dbcli list-jobs | grep -i <dbname>

   Note the last job ID listed with a status other than Success.
3. With the job ID you noted from the previous step, use the following command to check the details of that job:
   
   dbcli describe-job -i <job_ID> -j

   Typically, running this command is enough to reveal the root cause of the failure.
4. If you require more information, review the /opt/oracle/dcs/log/dcs-agent.log file.
   
   You can find the job ID in this file by using the timestamp returned by the job report in step 2.
5. If the problem details suggest an RMAN issue, review the RMAN logs in the /opt/oracle/dcs/log/<hostname>/rman/bkup/<db_unique_name>/rman_backup/<yyyy-mm-dd> directory.

   Note:
   
   If the database failure is on a 2-node RAC database, perform steps 3 and 4 on both nodes.

Database Service Agent Issues

Your Oracle Cloud Infrastructure Database makes use of an agent framework to allow you to manage your database through the cloud platform. Occasionally you might need to restart the dcsagent program if it has the status of stop/waiting to resolve a backup failure.

To restart the database service agent

1. From a command prompt, check the status of the agent:
   
   initctl status initdcsagent

2. If the agent is in the stop/waiting state, try to restart the agent:
   
   initctl start initdcsagent

3. Check the status of the agent again to confirm that it has the start/running status:
   
   initctl status initdcsagent
Oracle Clusterware Issues

Oracle Clusterware enables servers to communicate with each other so that they can function as a collective unit. Occasionally you might need to restart the Clusterware program to resolve a backup failure.

To restart the Oracle Clusterware

1. From command prompt, check the status of Oracle Clusterware:

   `crsctl check crs`
   
   `crsctl stat res -t`

2. If Oracle Clusterware is not online, try to restart the program:

   `crsctl start crs`

3. Check the status of Oracle Clusterware to confirm that it is online:

   `crsctl check crs`

Object Store Connectivity Issues

Backing up your database to Oracle Cloud Infrastructure Object Storage requires that the host can connect to the applicable Swift endpoint. You can test this connectivity by using a Swift user.

To ensure your database host can connect to the object store

1. Create a Swift user in your tenancy. See Working with Auth Tokens on page 2456.

2. With the user you created in the previous step, use the following command to verify the host can access the object store.

   `curl -v -X HEAD -u <user_ID>:<auth_token>' https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/<object_storage_namespace>`

   See Object Storage FAQ for the correct region to use. See Understanding Object Storage Namespaces on page 3395 for information about your Object Storage namespace.

3. If you cannot connect to the object store, refer to Prerequisites on page 1436 for how to configure object store connectivity.

Host Issues

One or more of the following conditions on the database host can cause backups to fail:

Interactive Commands in the Oracle Profile

If an interactive command such as `oraenv`, or any command that might return an error or warning message, was added to the `.bash_profile` file for the grid or oracle user, Database service operations like automatic backups can be interrupted and fail to complete. Check the `.bash_profile` file for these commands, and remove them.

The File System Is Full

Backup operations require space in the `/u01` directory on the host file system. Use the `df -h` command on the host to check the space available for backups. If the file system has insufficient space, you can remove old log or trace files to free up space.

Incorrect Version of the Oracle Database Cloud Backup Module

Your system might not have the required version of the backup module (opc_installer.jar). See Unable to use Managed Backups in your DB System for details about this known issue. To fix the problem, you can follow the procedure in that section or simply update your DB system and database with the latest bundle patch.
Changes to the Site Profile File (glogin.sql)

Customizing the site profile file ($ORACLE_HOME/sqlplus/admin/glogin.sql) can cause managed backups to fail in Oracle Cloud Infrastructure. In particular, interactive commands can lead to backup failures. Oracle recommends that you not modify this file for databases hosted in Oracle Cloud Infrastructure.

Database Issues

An improper database state or configuration can lead to failed backups.

Database Not Running During Backup

The database must be active and running (ideally on all nodes) while the backup is in progress.

To check that the database is active and running

Use the following command to check the state of your database, and ensure that any problems that might have put the database in an improper state are resolved:

```
srvctl status database -d <db_unique_name> -verbose
```

The system returns a message including the database's instance status. The instance status must be Open for the backup to succeed. If the database is not running, use the following command to start it:

```
srvctl start database -d <db_unique_name> -o open
```

If the database is mounted but does not have the Open status, use the following commands to access the SQL*Plus command prompt and set the status to Open:

```
sqlplus / as sysdba
alter database open;
```

Archiving Mode Set to NOARCHIVELOG

When you provision a new database, the archiving mode is set to ARCHIVELOG by default. This is the required archiving mode for backup operations. Check the archiving mode setting for the database and change it to ARCHIVELOG, if applicable.

To check and set the archiving mode

Open an SQL*Plus command prompt and enter the following command:

```
select log_mode from v$database;
```

If you need to set the archiving mode to ARCHIVELOG, start the database in Mount status (and not Open status), and use the following command at the SQL*Plus command prompt:

```
alter database archivelog;
```

Confirm that the db_recovery_file_dest parameter points to +RECO, and that the log_archive_dest_n parameter is set to USE_DB_RECOVERY_FILE_DEST.

For RAC databases, one instance must have the Mount status when enabling archivelog mode. To enable archivelog mode for a RAC database, perform the following steps:

1. Shut down all database instances:

```
srvctl stop database -d
```
2. Start one of the database instances in mount state:

```
srvc1 start instance -d <db_unique_name> -i <instance_name> -o mount
```

3. Access the SQL*Plus command prompt:

```
sqlplus / as sysdba
```

4. Enable archive log mode:

```
alter database archivelog;
```

```
exit;
```

5. Stop the database:

```
srvc1 stop instance -d <db_unique_name> -i <instance_name>
```

6. Restart all database instances:

```
srvc1 start database -d <db_unique_name>
```

7. At the SQL*Plus command prompt, confirm the archiving mode is set to ARCHIVELOG:

```
select log_mode from v$database;
```

**Stuck Database Archiver Process and Backup Failures**

Backups can fail when the database instance has a stuck archiver process. For example, this can happen when the flash recovery area (FRA) is full. You can check for this condition using the `srvc1 status database - db <db_unique_name> -v` command. If the command returns the following output, you must resolve the stuck archiver process issue before backups can succeed:

```
Instance <instance_identifier> is running on node *<node_identifier>.
Instance status: Stuck Archiver
```

Refer to ORA-00257: Archiver Error (Doc ID 2014425.1) for information on resolving a stuck archiver process.

After resolving the stuck process, the command should return the following output:

```
Instance <instance_identifier> is running on node *<node_identifier>.
Instance status: Open
```

If the instance status does not change after you resolve the underlying issue with the device or resource being full or unavailable, try one of the following workarounds:

- Restart the database using the `srvc1` command to update the status of the database in the clusterware
- Upgrade the database to the latest patchset levels

**Temporary Tablespace Errors**

If fixed table statistics are not up to date on the database, backups can fail with errors referencing temporary tablespace present in the `dcs-agent.log` file. For example:

```
select status from v$rman_status where COMMAND_ID=<backup_id>
```

```
ERROR at line 1:
ORA-01652: unable to extend temp segment by 128 in tablespace TEMP
```
Gather your fixed table statics as follows to resolve this issue:

```
conn / as sysdba
exec dbms_stats.gather_fixed_objects_stats();
```

### RMAN Configuration and Backup Failures

Editing certain RMAN configuration parameters can lead to backup failures in Oracle Cloud Infrastructure. To check your RMAN configuration, use the `show all` command at the RMAN command line prompt.

See the following list of parameters for details about RMAN the configuration settings that should not be altered for databases in Oracle Cloud Infrastructure.

**RMAN configuration settings that should not be altered**

```
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 30 DAYS;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 5 BACKUP TYPE TO COMPRESSED BACKUPSET;
CONFIGURE CHANNEL DEVICE TYPE DISK MAXPIECESIZE 2 G;
CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' MAXPIECESIZE 2 G FORMAT '%d_%I_%U_%T_%t' PARMS 'SBT_LIBRARY=/opt/oracle/dcs/commonstore/pkgrepos/oss/odbcso/robipso.so ENV=(OPC_PFILE=/opt/oracle/dcs/commonstore/objectstore/odc_pofile/1578318329/odc_tiger_lad3c8.ora)';
CONFIGURE ARCHIVELOG DELETION POLICY TO BACKED UP 1 TIMES TO 'SBT_TAPE';
CONFIGURE CHANNEL DEVICE TYPE DISK MAXPIECESIZE 2 G;
CONFIGURE ENCRYPTION FOR DATABASE ON;
```

### RMAN Retention Policy and Backup Failures

The RMAN retention policy configuration can be the source of backup failures. Using the REDUNDANCY retention policy configuration instead of the RECOVERY WINDOW policy can lead to backup failures. Be sure to use the RECOVERY WINDOW OF 30 DAYS configuration.

**To configure the RMAN retention policy setting**

1. Find the database ID using the following command:

   ```
   dbcli list-databases
   ```

2. Find the `BackupConfigId` value for the database using the following command:

   ```
   dbcli describe-database -i <database_id>
   ```

3. Update the retention policy configuration to RECOVERY WINDOW OF 30 DAYS:

   ```
   dbcli update-backupconfig -i <backup_config_id> --recoverywindow 30
   ```
Loss of Object Store Wallet File and Backup Failures

RMAN backups fail when an object store wallet file is lost. The wallet file is necessary to enable connectivity to the object store.

To confirm that the object store wallet file exists and has the correct permissions

1. Find the database ID using the following command:

   `dbcli list-databases`

2. Find the BackupConfigId value for the database using the following command:

   `dbcli describe-database -i <database_id>`

3. Find the BackupLocation value for the database using the following command:

   `dbcli describe-backupconfig <backup_config_id>`

4. Find the file path of the backup config parameter file (`opc_<backup_location_value>_BC.ora`) using the following command:

   `locate opc_<backup_location_value>_BC.ora`

   For example:

   ```
   [root@orcl 13aef284-9d6b-4eb6-8751-2988aexample]# locate opc_b9naijWMAXzi9example_BC.ora
   /opt/oracle/dcs/commonstore/objectstore/opc_pfile/13aef284-9d6b-4eb6-8751-2988a9example/
   opc_b9naijWMAXzi9example_BC.ora
   ```

5. Find the file path to the wallet file in the backup config parameter file by inspecting the value stored in the `OPC_WALLET` parameter. To do this, navigate to the directory containing the backup config parameter file and use the following `cat` command:

   `cat <backup_config_parameter_file>`

   For example:

   ```
   [root@orcl 13aef284-9d6b-4eb6-8751-2988aexample]# cat opc_b9naijWMAXzi9example_BC.ora
   OPC_HOST=https://swift.objectstorage.us-ashburn-1.oraclecloud.com/v1/dbbackupiad
   OPC_WALLET='LOCATION=file:/opt/oracle/dcs/commonstore/objectstore/wallets/13aef284-9d6b-4eb6-8751-2988aexample CREDENTIAL_ALIAS=alias_opc'
   OPC_CONTAINER=b9naijWMAXzi9example
   ```

6. Confirm that the `cwallet.sso` file exists in the directory specified in the `OPC_WALLET` parameter, and confirm that the file has the correct permissions. The file permissions should have the octal value of "600" (`-rw-------`). Use the following command:

   `ls -ltr /opt/oracle/dcs/commonstore/objectstore/wallets/<backup_config_id>`

   For example:
TDE Wallet and Backup Failures

Incorrect TDE Wallet Location Specification

For backup operations to work, the `ORACLE_HOME/network/admin/sqlnet.ora` file must contain the `ENCRYPTION_WALLET_LOCATION` parameter formatted exactly as follows:

```
ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/opt/oracle/dcs/commonstore/wallets/tde/$ORACLE_UNQNAME)))
```

**Important:**

In this wallet location entry, `$ORACLE_UNQNAME` is an environment variable and should not be replaced with an actual value.

To check the TDE wallet location specification

Use the `cat` command to check the TDE wallet location specification. For example:

```
[oracle@orcl tde]$ cat $ORACLE_HOME/network/admin/sqlnet.ora

ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/opt/oracle/dcs/commonstore/wallets/tde/$ORACLE_UNQNAME)))
```

Incorrect State of the TDE Wallet

Database backups fail if the TDE wallet is not in the proper state. The following scenarios can cause this problem:

*The ORACLE_UNQNAME environment variable was not set when the database was started using SQL*Plus*

If the database was started using SQL*Plus, and the `ORACLE_UNQNAME` environment variable was not set, the wallet is not opened correctly.

To fix the problem, start the database using the `srvctl` utility:

```
srvctl start database -d <db_unique_name>
```

*A pluggable database was added with an incorrectly configured master encryption key*

In a multitenant environment for Oracle Database versions that support PDB-level keystore, each PDB has its own master encryption key. This encryption key is stored in a single keystore used by all containers. After you create or plug in a new PDB, you must create and activate a master encryption key for it. If you do not do so, the `STATUS` column in the `v$encryption_wallet` view shows the value `OPEN_NO_MASTER_KEY`.

To check the master encryption key status and create a master key, do the following:

1. Review the `STATUS` column in the `v$encryption_wallet` view, as shown in the following example:

```
SQL> alter session set container=pdb2;
```
Session altered.

```sql
SQL> select WRL_TYPE, WRL_PARAMETER, STATUS, WALLET_TYPE from v$encryption_wallet;
```

<table>
<thead>
<tr>
<th>WRL_TYPE</th>
<th>WRL_PARAMETER</th>
<th>STATUS</th>
<th>WALLET_TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE</td>
<td>/opt/oracle/dcs/commonstore/wallets/tde/example_iadxyz/</td>
<td>OPEN_NO_MASTER_KEY</td>
<td>AUTOLOGIN</td>
</tr>
</tbody>
</table>

2. Confirm that the PDB is in READ WRITE open mode and is not restricted, as shown in the following example:

```sql
SQL> show pdbs
```

<table>
<thead>
<tr>
<th>CON_ID</th>
<th>CON_NAME</th>
<th>OPEN MODE</th>
<th>RESTRICTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>PDB$SEED</td>
<td>READ ONLY</td>
<td>NO</td>
</tr>
<tr>
<td>3</td>
<td>PDB1</td>
<td>READ WRITE</td>
<td>NO</td>
</tr>
<tr>
<td>4</td>
<td>PDB2</td>
<td>READ WRITE</td>
<td>NO</td>
</tr>
</tbody>
</table>

The PDB cannot be open in restricted mode (the RESTRICTED column must show NO). If the PDB is currently in restricted mode, review the information in the PDB_PLUG_IN_VIOLATIONS view and resolve the issue before continuing. For more information on the PDB_PLUG_IN_VIOLATIONS view and the restricted status, review the documentation on pluggable database for your Oracle database version.

3. Run the following DBCLI commands to change the status to OPEN:

```
$ sudo su -
# dbcli list-database
# dbcli update-tdekey -i <database_ID> -n <PDB_name> -p
```

The `update-tdekey` command shown will prompt you for the admin password.

4. Confirm that the status of the wallet has changed from OPEN_NO_MASTER_KEY to OPEN by querying the v$encryption_wallet view as shown in step 1.

**Incorrect Configuration Related to the TDE Wallet**

Several configuration parameters related to the TDE wallet can cause backups to fail.

*To check configuration related to the TDE wallet*

- Check that the environment's database unique name parameter (ORACLE_UNQNAME) is set correctly using the following command:

```
srvctl getenv database -d <db_unique_name>
```

For example:

```
[oracle@orcl tde]$ srvctl getenv database -d orclbkp_iadxyz
```
orclbkp_iadxyz:
ORACLE_UNQNAME=orclbkp_iadxyz
TZ=UTC

• Check your sqlnet.ora settings to confirm that the file has an ENCRYPTION_WALLET_LOCATION parameter with the correct DIRECTORY value. Use the following command:
cat $ORACLE_HOME/network/admin/sqlnet.ora

For example:

[oracle@orcl tde]$ cat $ORACLE_HOME/network/admin/sqlnet.ora
ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)
(METHOD_DATA=(DIRECTORY=/opt/oracle/dcs/commonstore/wallets/tde/
$ORACLE_UNQNAME)))

• Confirm that the wallet status is open and the wallet type is auto login by checking the v $encryption_wallet view. For example:

    SQL> select status, wrl_parameter,wallet_type from v $encryption_wallet;

    STATUS                WRL_PARAMETER
    ------------------------
    ------------------------
    OPEN
    tde/example_iadxyz/ AUTOLOGIN

For pluggable databases (PDBs), be sure that you switch to the appropriate container before querying v $encryption_wallet view. For example:

    [oracle@paulo ~]$ sqlplus / as sysdba
    SQL> alter session set container=pdb1;
    Session altered.
    SQL> select WRL_TYPE,WRL_PARAMETER,STATUS,WALLET_TYPE from v $encryption_wallet;

    WRL_TYPE      WRL_PARAMETER
    STATUS        WALLET_TYPE
    ------------- ------------------------
    ------------- ------------------------
    FILE
    OPEN AUTOLOGIN
    /opt/oracle/dcs/commonstore/wallets/tde/tiger_iad3c8/
    AUTOLOGIN
**Missing TDE Wallet File**

The TDE wallet file (ewallet.p12) can cause backups to fail if it is missing, or if it has incompatible file system permissions or ownership. Check the file as shown in the following example:

```
[oracle@orcl tde]$ ls -ltr /opt/oracle/dcs/commonstore/wallets/tde/
$ORACLE_UNQNAME/ewallet.p12
-rwx------ 1 oracle oinstall 5680 Apr 18 13:09 /opt/oracle/dcs/
commonstore/wallets/tde/orclbkp_iadxzy/ewallet.p12
```

The TDE wallet file should have file permissions with the octal value ”700” (rwx------), and the owner of this file should be a part of the oinstall operating system group.

**Missing Auto Login Wallet File**

The auto login wallet file (cwallet.sso) can cause backups to fail if it is missing, or if it has incompatible file system permissions or ownership. Check the file as shown in the following example:

```
[oracle@orcl tde]$ ls -ltr /opt/oracle/dcs/commonstore/wallets/tde/
$ORACLE_UNQNAME/cwallet.sso
-rwx------ 1 oracle oinstall 5725 Apr 18 13:09 /opt/oracle/dcs/
commonstore/wallets/tde/orclbkp_iadxyz/cwallet.sso
```

The auto login wallet file should have file permissions with the octal value ”700” (rwx------), and the owner of this file should be a part of the oinstall operating system group.

**Other Causes of Backup Failures**

**Unmounted Commonstore Mount Point**

The mount point /opt/oracle/dcs/commonstore must be mounted, or backups will fail.

*To check the commonstore mount point*

Confirm that the mount point /opt/oracle/dcs/commonstore is mounted, as shown in the following example:

```
[root@orcl ~]# srvctl config filesystem -volume commonstore -diskgroup
data
Volume device: /dev/asm/commonstore-5
Diskgroup name: data
Volume name: commonstore
Canonical volume device: /dev/asm/commonstore-5
Accelerator volume devices:
Mountpoint path: /opt/oracle/dcs/commonstore
Mount point owner: oracle
Mount users:
Type: ACFS
```
To confirm that ora.data.commonstore.acfs is online

The state for ora.data.commonstore.acfs must be online, or backups will fail. Confirm as shown in the following example:

```
[root@orcl ~]# crsctl stat resource ora.data.commonstore.acfs -v
NAME=ora.data.commonstore.acfs
TYPE=ora.acfs.type
LAST_SERVER=orcl
STATE=OFFLINE
TARGET=OFFLINE
... 
STATE_DETAILS=admin unmounted /opt/oracle/dcs/commonstore
...
[root@orcl ~]# ls -ltr /opt/oracle/dcs/commonstore
```

If the STATE_DETAILS value is unmounted, mount the file system as shown in the following example:

```
[root@orcl ~]# srvctl start filesystem -volume commonstore -diskgroup data
```

Confirm that the change was successful as shown in the following example:

```
[root@orcl ~]# crsctl stat resource ora.data.commonstore.acfs -v
NAME=ora.data.commonstore.acfs
TYPE=ora.acfs.type
LAST_SERVER=orcl
STATE=ONLINE on orcl
TARGET=ONLINE
CARDINALITY_ID=ONLINE
...
STATE_DETAILS=mounted on /opt/oracle/dcs/commonstore
```

List the contents of the commonstore directory to confirm that it is mounted, as shown in the following example:

```
[root@orcl ~]# ls -ltr /opt/oracle/dcs/commonstore
```

```
   total 220
   drwx------  2 root    root 65536 Apr 18 10:50 lost+found
   drwx------  3 oracle oinstall 20480 Apr 18 11:02 wallets
```
The Database Is Not Properly Registered

Database backups fail if the database is not registered with the dcs-agent. This scenario can occur if you manually migrate the database to Oracle Cloud Infrastructure and do not run the `dbcli register-database` command.

To check whether the database is properly registered, review the information returned by running the `srvctl config database` command and the `dbcli list-databases` command. If either command does not return a record of the database, contact Oracle Support Services.

For instructions on how to register the database, refer to the following topics:

- Registering the Database on the DB System on page 1459
- Database Commands on page 1505

Getting Help

If you were unable to resolve the problem using the information in this topic, follow the procedures below to collect relevant database and diagnostic information. After you have collected this information, contact Oracle Support.

**To collect database information for use in problem reports**

Use the following commands to collect details about your database. Record the output of each command for reference:

```
dbcli list-databases
```

```
dbcli describe-database -i <database_id>
```

```
dbcli describe-component
```

**To collect diagnostic information regarding failed jobs**

1. Log on to the host as the root user and navigate to the `/opt/oracle/dcs/bin/` directory.
2. Run the following two commands to generate information about the failed job:

   ```
dbcli list-jobs | grep -i <dbname>
dbcli describe-job -i <job_ID> -j
   ```

   The `<job_ID>` in the second command should be the ID of the latest failed job reported from the first command.
3. Run the diagnostics collector script to create a zip file with the diagnostic information for Oracle Support Services.

   ```
diagcollector.py
   ```

   This command creates a file named `diagLogs-<timestamp>.zip` in the `/tmp` directory.

**To collect DCS agent log files**

To collect DCS agent log files, do the following:

1. Log in as opc user.
2. Run the following command:

   ```
sudo /opt/oracle/dcs/bin/diagcollector.py
   ```
3. The system returns a message indicating that agent logs are available in a zip file at a specified directory. For example:

```
[opc@prodpr ~]$ sudo /opt/oracle/dcs/bin/diagcollector.py
Log files collected to :/tmp/dcsdiag/diagLogs-1234567890.zip
Logs are being collected to:
/tmp/dcsdiag/diagLogs-1234567890.zip
```

To collect TDE configuration details

1. Run the `srvctl getenv database -d <db_unique_name>` command and record the output for reference.

2. Record the output of the view `v$encryption_wallet`. For example:

```
SQL> select status, wrl_parameter, wallet_type from v$encryption_wallet;

<table>
<thead>
<tr>
<th>STATUS</th>
<th>WRL_PARAMETER</th>
<th>WALLET_TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN</td>
<td>/opt/oracle/dcs/commonstore/wallets/tde/example_iadxyz/ AUTOLOGIN</td>
<td></td>
</tr>
</tbody>
</table>
```

3. Record the output of the `ls -ltr <wrl_parameter>` command. For example:

```
[oracle@patchtst ~]$ ls -ltr /opt/oracle/dcs/commonstore/wallets/tde/example_iadxyz/
```

To collect the RMAN backup report file

Generate RMAN Backup Report File using the following command:

```
dbcli create-rmanbackupreport -i <db_id> -w detailed -rn <report_name>
```

For example:

```
[root@patchtst ~]# dbcli create-rmanbackupreport -i 57fvwxyz-9dc4-45d3-876b-5f850example -w detailed -rn bkpreport1
```

Locate the report file using the `dbcli describe-rmanbackupreport -in <report_name>` command. The location of the report is given in output. For example:

```
[root@patchtst ~]# dbcli describe-rmanbackupreport -in bkpreport1
```
Patching Failures on Bare Metal and Virtual Machine DB Systems

Patching operations can fail for various reasons. Typically, an operation fails because a database node is down, there is insufficient space on the file system, or the database host cannot access the object store.

This topic includes information to help you determine the cause of the failure and fix the problem. The information is organized into several sections, based on the error condition. If you already know the cause, you can skip to the section with the suggested solution. Otherwise, use the procedure in Determining the Problem on page 1659 to get started.

Determining the Problem

In the Console, you can identify a failed patching operation by viewing the patch history of a DB system or an individual database. A patch that was not successfully applied displays a status of Failed and includes a brief description of the error that caused the failure. If the error message does not contain enough information to point you to a solution, you can use the database CLI and log files to gather more data. Then, refer to the applicable section in this topic for a solution.

To identify the root cause of the patching operation failure

1. Log on to the host as the root user and navigate to the /opt/oracle/dcs/bin/ directory.
2. Determine the sequence of operations performed on the database.
   
   dbcli list-jobs

   Note the last job ID listed with a status other than Success.
3. With the job ID you noted from the previous step, use the following command to check the details of that job:

   dbcli describe-job -i <job_ID> -j

   Typically, running this command is enough to reveal the root cause of the failure.
4. If you require more information, review the /opt/oracle/dcs/log/dcs-agent.log file.
   You can find the job ID in this file by using the timestamp returned by the job report in step 2.
5. If the patching failure is on a 2-node RAC database, perform steps 3 and 4 on both nodes.

Database Service Agent Issues

Your Oracle Cloud Infrastructure Database makes use of an agent framework to allow you to manage your database through the cloud platform.

Resolving Patching Failures Caused By a Stopped Agent

Occasionally you might need to restart the dcsagent program if it has the status of stop/waiting to resolve a patching failure.
To restart the database service agent

1. From a command prompt, check the status of the agent:

   ```
   initctl status initdcsagent
   ```

2. If the agent is in the **stop/waiting** state, try to restart the agent:

   ```
   initctl start initdcsagent
   ```

3. Check the status of the agent again to confirm that it has the **start/running** status:

   ```
   initctl status initdcsagent
   ```

Resolving Patching Failures Caused By an Agent That Needs to Be Updated

Patching can also fail if your agent needs to be updated. The system gives the following error message for this failure:

```
Current DcsAgent version is less than or equal to minimum required version.
```

To resolve this issue, perform the steps in To have Oracle Support update the Oracle Cloud Infrastructure Database service agent on page 1660.

To have Oracle Support update the Oracle Cloud Infrastructure Database service agent

1. Confirm that the agent (dcsagent) and DCS Admin program (dcsadmin) are running using the following commands:

   ```
   initctl status initdcsagent
   ```

   ```
   initctl status initdcsadmin
   ```

   If these programs are not running, use the following commands to restart them:

   ```
   initctl start initdcsagent
   ```

   ```
   initctl start initdcsadmin
   ```

2. Follow the instructions in Obtaining Further Assistance on page 1662 to collect your DCS agent log files.

3. Contact Oracle Support for assistance with updating the agent.

Object Store Connectivity Issues

Oracle Cloud Infrastructure DB system and database patches are stored in Oracle Cloud Infrastructure Object Storage. Therefore, successful patching operations require connectivity between the DB system host and the Object Storage location from which the patches are downloaded.

To ensure your database host can connect to Oracle Cloud Infrastructure Object Storage

1. Use the following command to verify the host can access Oracle Cloud Infrastructure Object Storage:

   ```
   dbcli describe-latestpatch
   ```

   Example output indicating success:

   ```
   [root@<host> ~]# dbcli describe-latestpatch
   componentType availableVersion
   -------------------------------
   gi 12.2.0.1.180417
   gi 12.1.0.2.180417
   ```
Example output indicating failure:
```
[root@<host> ~]# dbcli describe-latestpatch
DCS-10032:Resource patch metadata is not found.Failed to download patchmetadata from objectstore
```

2. If you cannot connect to the object store, refer to Prerequisites on page 1436 for how to configure object store connectivity.

**Host and Oracle Clusterware Issues**

One or more of the following conditions on the database host can cause patching operations to fail:

**Database Node Not Running During the Patching Operation**

All nodes of the database must be active and running while a patching operation is in progress, whether you are patching the DB system or the database home. Use the Console to check that the status of each node is AVAILABLE, and start the node, if needed.

**The File System Is Full**

Patching operations require a minimum of 15 GB of free space in the `/u01` directory on the host file system. Use the `df -h` command on the host to check the available space. If the file system has insufficient space, you can remove old log or trace files to free up space.

**The Oracle Clusterware Is Not Running**

Oracle Clusterware enables servers to communicate with each other so that they can function as a collective unit. The cluster software program must be up and running on the DB system for patching operations to complete. Occasionally you might need to restart the Oracle Clusterware to resolve a patching failure.

*To restart the Oracle Clusterware*

1. From command prompt, check the status of Oracle Clusterware:

   ```
   crsctl check crs
   ```

   Example output:
   ```
   [grid@<host> ~]$/crsctl check crs
   CRS-4638: Oracle High Availability Services is online
   CRS-4537: Cluster Ready Services is online
   CRS-4529: Cluster Synchronization Services is online
   CRS-4533: Event Manager is online
   ```

   For more detailed status information, you can run `crsctl stat res -t`.

2. If Oracle Clusterware is not online, try to restart the program:

   ```
   crsctl start crs
   ```
3. Check the status of Oracle Clusterware to confirm that it is online:

   crsctl check crs

**The Oracle Grid Infrastructure (GI) Is Not Updated**

This problem occurs when you try to patch a database before you patch the DB system of that database. The error description indicates that the Oracle Grid Infrastructure must be updated first. To resolve this issue, patch the DB system to latest available version. After you patch the DB system, you can retry the database patching operation.

To get the current and latest-available GI versions for the DB system, use the following command:

   dbcli describe-component

**Database Issues**

An improper database state can lead to patching failures.

**Database Not Running During the Patching Operation**

The database must be active and running for all of the patching tasks to complete. Otherwise, you must run the datapatch task manually.

*To check that the database is active and running*

Use the following command to check the state of your database, and ensure that any problems that might have put the database in an improper state are resolved:

   srvctl status database -d <db_unique_name> -verbose

The system returns a message including the database instance status. The instance status must be **Open** for the patching operation to succeed.

If the database is not running, use the following command to start it:

   srvctl start database -d <db_unique_name> -o open

If the database is mounted but does not have the **Open** status, use the following commands to access the SQL*Plus command prompt and set the status to **Open**:

   sqlplus / as sysdba
   alter database open;

*To run the datapatch task*

Before you run the datapatch command, ensure that all pluggable databases (PDBs) are open. To open a PDB, you can use SQL*Plus to execute ALTER PLUGGABLE DATABASE `<pdb_name>` OPEN READ WRITE; against the PDB.

   $ORACLE_HOME/OPatch/datapatch

The datapatch command should be run on each database home.

**Obtaining Further Assistance**

If you were unable to resolve the problem using the information in this topic, follow the procedures below to collect relevant database and diagnostic information. After you have collected this information, contact Oracle Support.
To collect diagnostic information regarding failed jobs

1. Log on to the host as the root user and navigate to the /opt/oracle/dcs/bin/ directory.
2. Run the following two commands to generate information about the failed job:

   `dbcli list-jobs`

   `dbcli describe-job -i <job_ID> -j`

   The `<job_ID>` in the second command should be the ID of the latest failed job reported from the first command.
3. Run the diagnostics collector script to create a zip file with the diagnostic information for Oracle Support Services.

   `diagcollector.py`

   This command creates a file named `diagLogs-<timestamp>.zip` in the /tmp directory.

To collect DCS agent log files

To collect DCS agent log files, do the following:

1. Log in as opc user.
2. Run the following command:

   `sudo /opt/oracle/dcs/bin/diagcollector.py`

3. The system returns a message indicating that agent logs are available in a zip file at a specified directory. For example:

   `[opc@prodpr ~]$ sudo /opt/oracle/dcs/bin/diagcollector.py`
   
   Log files collected to :/tmp/dcsdiag/diagLogs-1234567890.zip
   Logs are being collected to:
   /tmp/dcsdiag/diagLogs-1234567890.zip

To collect Oracle Grid Infrastructure and Database log files

If an Oracle Grid Infrastructure or Oracle Database patch failed, you can find log files for these failures in the following locations:

**Oracle Grid Infrastructure**

$GI_HOME/cfgtoollogs/

**Oracle Database**

$ORACLE_HOME/cfgtoollogs/

Shape Change Failures for Virtual Machine DB Systems

If your virtual machine DB system shape change does not successfully complete, you can use the procedures in this topic to troubleshoot and fix the issue. For multi-node DB systems, shape change operations proceed in a rolling fashion. Depending on where in the shape change operation the failure occurs, you may be able to re-try the operation using the console.
Using the Console to Troubleshoot

If your shape change operation fails, a message banner appears on the DB System Details page to provide details about the failure. If the failure happens on the first node of a multi-node system, and the operation is rolled back successfully, the Change Shape button remains available and the system remains online, in the Available state. Contact Oracle Support to get additional details about the failure. You can also follow the steps in Using dbcli to Troubleshoot on page 1664 to learn more about the failure and what issues need to be resolved. After determining that no issues remain, you can try the operation again.

If the failure leaves the system in a state where the operation cannot be rolled back, the system state is Needs Attention. In this case, contact Oracle Support as soon as you are aware of the issue so Oracle can help you resolve the issue and complete the shape change operation.

Using dbcli to Troubleshoot

Determine What Stage of the Shape Change Operation Failed

1. Login to the DB system as the root user.
2. Navigate to /opt/oracle/dcs/bin:
   
   ```
   cd /opt/oracle/dcs/bin
   ```
3. Update the CLI tool:
   
   ```
   ./cliadm update-dbcli
   ```
4. List the failed jobs:
   
   ```
   dbcli list-jobs | grep -i failed
   ```

5. Note if the failed job (or jobs) occurred during the pre_action, action, or post_action stage. Also note the job_id value of the failed job, which you will need to resolve the issue.

Troubleshooting Failures That Occur in the Pre_action Stage

1. Use the job_id value to get more information about the failure:
   
   ```
   dbcli describe-job -i <job_id>
   ```
2. Search for the error in the dcs-agent.log and dcs-agent-debug.log files (which are located in the /opt/oracle/dcs/log/ directory):
   
   For example:
   
   ```
   cd /opt/oracle/dcs/log
   grep -ir "DCS-10063:Failed to get node names from olsnodes." *
   ```
3. Using the information about the error recorded in the log file, correct the system configuration if possible.
4. Re-try the shape change operation. If the operation is still not successful, follow the instructions in Getting Additional Help on page 1664.

Getting Additional Help

If your failure occurs in the post_action stage, or if you are unable to resolve failures that occur in the pre_action stage, do the following:

1. Gather the information listed in the document Diagnostic Data Collection For Oracle Database Cloud Service Instance (OCI) (Doc ID 2397481.1)
2. Open a Support Request with My Oracle Support
Backup Failures on Exadata DB Systems

If your Exadata managed backup does not successfully complete, you can use the procedures in this topic to troubleshoot and fix the issue. The most common causes of backup failure are the following:

- The host cannot access Object Storage
- The database configuration on the host is not correct

The information that follows is organized by the error condition. If you already know the cause, you can skip to the section with the suggested solution. Otherwise, use the procedure in Determining the Problem on page 1665 to get started.

Determining the Problem

In the Console, a failed database backup either displays a status of Failed or hangs in the Backup in Progress or Creating state. If the error message does not contain enough information to point you to a solution, you can gather more information by using the dbaascli tool and by viewing the log files. Then, refer to the applicable section in this topic for a solution.

To identify the root cause of the backup failure

Database backups can fail during the RMAN configuration stage or during a running RMAN backup job. RMAN configuration tasks include validating object store connectivity, backup module installation, and RMAN configuration changes. The log files you examine depend on which stage the failure occurs.

1. Log on to the host as the root user.
2. Check the applicable log file:
   - If the failure occurred during RMAN configuration, navigate to the /var/opt/oracle/log/<database_name>/bkup/ directory and check the bkup.log file.
   - If the failure occurred during the backup job, navigate to the /var/opt/oracle/log/<database_name>/obkup/ directory and check the obkup.log file.

   **Note:**
   - Each execution of bkup and obkup commands generates a separate log file but bkup.log and obkup.log are symbolic links that point to the most recently generated log file.
   - Ensure that you check the log files on all of the Exadata DB system compute nodes because all nodes send backup pieces to Object Storage.

Database Service Agent Issues

Your Oracle Cloud Infrastructure Database makes use of an agent framework to allow you to manage your database through the cloud platform. Occasionally you might need to restart the dcsagent program if it has the status of stop/waiting to resolve a backup failure. View the /opt/oracle/dcs/log/dcs-agent.log file to identify issues with the agent.

To restart the database service agent

1. From a command prompt, check the status of the agent:
   
   ```
   systemctl status dcsagent.service
   ```

2. If the agent is in the stop/waiting state, try to restart the agent:
   
   ```
   systemctl start dcsagent.service
   ```

3. Check the status of the agent again to confirm that it has the start/running status:
   
   ```
   systemctl status dcsagent.service
   ```
Object Store Connectivity Issues

Back up your database to Oracle Cloud Infrastructure Object Storage requires that the host can connect to the applicable Swift endpoint. Though Oracle controls the actual Swift user credentials for the storage bucket for managed backups, verifying general connectivity to Object Storage in your region is a good indicator that object store connectivity is not the issue. You can test this connectivity by using another Swift user.

To ensure your database host can connect to the object store

1. Create a Swift user in your tenancy. See Working with Auth Tokens on page 2456.
2. With the user you created in the previous step, use the following command to verify the host can access the object store.

```bash
curl -v -X HEAD -u <user_ID>:'<auth_token>' https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/<object_storage_namespace>
```

See Object Storage FAQ for the correct region to use. See Understanding Object Storage Namespaces on page 3395 for information about your Object Storage namespace.

3. If you cannot connect to the object store, refer to the Prerequisites on page 1320 section of the Managing Exadata Database Backups on page 1320 topic for information on configuring object store connectivity.

Host Issues

One or more of the following conditions on the database host can cause backups to fail:

Interactive Commands in the Oracle Profile

If an interactive command such as `oraenv`, or any command that might return an error or warning message, was added to the `.bash_profile` file for the grid or oracle user, Database service operations like automatic backups can be interrupted and fail to complete. Check the `.bash_profile` file for these commands, and remove them.

The File System Is Full

Backup operations require space in the `/u01` directory on the host file system. Use the `df -h` command on the host to check the space available for backups. If the file system has insufficient space, you can remove old log or trace files to free up space.

Incorrect Version of the Oracle Database Cloud Backup Module

Your system might not have the required version of the backup module (opc_installer.jar). See Unable to use Managed Backups in your DB System for details about this known issue. To fix the problem, you can follow the procedure in that section or simply update your DB system and database with the latest bundle patch.

Changes to the Site Profile File (glogin.sql)

Customizing the site profile file (`$ORACLE_HOME/sqlplus/admin/glogin.sql`) can cause managed backups to fail in Oracle Cloud Infrastructure. In particular, interactive commands can lead to backup failures. Oracle recommends that you not modify this file for databases hosted in Oracle Cloud Infrastructure.

Database Issues

An improper database state or configuration can lead to failed backups.

Database Not Running During Backup

The database must be active and running (ideally on all nodes) while the backup is in progress.
**To check that the database is active and running**

Use the following command to check the state of your database, and ensure that any problems that might have put the database in an improper state are resolved:

```
srvctl status database -d <db_unique_name> -verbose
```

The system returns a message including the database's instance status. The instance status must be **Open** for the backup to succeed. If the database is not running, use the following command to start it:

```
srvctl start database -d <db_unique_name> -o open
```

If the database is mounted but does not have the **Open** status, use the following commands to access the SQL*Plus command prompt and set the status to **Open**:

```
sqlplus / as sysdba
alter database open;
```

**Archiving Mode Set to NOARCHIVELOG**

When you provision a new database, the archiving mode is set to ARCHIVELOG by default. This is the required archiving mode for backup operations. Check the archiving mode setting for the database and change it to ARCHIVELOG, if applicable.

**To check and set the archiving mode**

Open an SQL*Plus command prompt and enter the following command:

```
select log_mode from v$database;
```

If you need to set the archiving mode to ARCHIVELOG, start the database in **Mount** status (and not **Open** status), and use the following command at the SQL*Plus command prompt:

```
alter database archivelog;
```

Confirm that the `db_recovery_file_dest` parameter points to `+RECO`, and that the `log_archive_dest_1` parameter is set to USE_DB_RECOVERY_FILE_DEST.

For RAC databases, one instance must have the **Mount** status when enabling archivelog mode. To enable archivelog mode for a RAC database, perform the following steps:

1. Shut down all database instances:
   ```
srvctl stop database -d
```
2. Start one of the database instances in mount state:
   ```
srvctl start instance -d <db_unique_name> -i <instance_name> -o mount
```
3. Access the SQL*Plus command prompt:
   ```
sqlplus / as sysdba
```
4. Enable archive log mode:
   ```
alter database archivelog;
exit;
```
5. Stop the database:

```
srvctl stop instance -d <db_unique_name> -i <instance_name>
```

6. Restart all database instances:

```
srvctl start database -d <db_unique_name>
```

7. At the SQL*Plus command prompt, confirm the archiving mode is set to ARCHIVELOG:

```
select log_mode from v$database;
```

### Stuck Database Archiver Process and Backup Failures

Backups can fail when the database instance has a stuck archiver process. For example, this can happen when the flash recovery area (FRA) is full. You can check for this condition using the `srvctl status database -db <db_unique_name> -v` command. If the command returns the following output, you must resolve the stuck archiver process issue before backups can succeed:

```
Instance <instance_identifier> is running on node *<node_identifier>.
Instance status: Stuck Archiver
```

Refer to ORA-00257:Archiver Error (Doc ID 2014425.1) for information on resolving a stuck archiver process.

After resolving the stuck process, the command should return the following output:

```
Instance <instance_identifier> is running on node *<node_identifier>.
Instance status: Open
```

If the instance status does not change after you resolve the underlying issue with the device or resource being full or unavailable, try restarting the database using the `srvctl` command to update the status of the database in the clusterware.

### RMAN Configuration and Backup Failures

Editing certain RMAN configuration parameters can lead to backup failures in Oracle Cloud Infrastructure. To check your RMAN configuration, use the `show all` command at the RMAN command line prompt.

See the following list of parameters for details about RMAN the configuration settings that should not be altered for databases in Oracle Cloud Infrastructure.

**RMAN configuration settings that should not be altered**

```
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 30 DAYS;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 5 BACKUP TYPE TO COMPRESSED BACKUPSET;
CONFIGURE CHANNEL DEVICE TYPE DISK MAXPIECESIZE 2 G;
CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/var/opt/oracle/dbaas_acfs/<db_name>/opc/libopc.so, ENV=(OPC_PFILE=/var/opt/oracle/dbaas_acfs/<db_name>/opc/opc<db_name>.ora)';
CONFIGURE ARCHIVELOG DELETION POLICY TO BACKED UP 1 TIMES TO 'SBT_TAPE';
CONFIGURE CHANNEL DEVICE TYPE DISK MAXPIECESIZE 2 G;
```
CONFIGURE ENCRYPTION FOR DATABASE ON;

**Loss of Object Store Wallet File and Backup Failures**

RMAN backups fail when an object store wallet file is lost. The wallet file is necessary to enable connectivity to the object store.

*To confirm that the object store wallet file exists and has the correct permissions*

1. Get the name of the database with the backup failure:

   ```sql
   SQL> show parameter db_name
   ```

2. Determine the file path of the backup config parameter file that contains the RMAN wallet information:

   ```bash
   locate opc_<database_name>.ora
   ```

   The default location is `/var/opt/oracle/dbaas_acfs/<database_name>/opc/opc<database_name>.ora`.

   For example:

   ```bash
   [root@khdyygw-mpjxb1Example /] # find / -name "opctestdb30.ora" -print
   /var/opt/oracle/dbaas_acfs/testdb30/opc/opctestdb30.ora
   ```

3. Find the file path to the wallet file in the backup config parameter file by inspecting the value stored in the `OPC_WALLET` parameter. To do this, navigate to the directory containing the backup config parameter file and use the following `cat` command:

   ```bash
   cat opc<database_name>.ora
   ```

   For example:

   ```bash
   [root@khdyygw-mpjxb1Example ]# cd /var/opt/oracle/dbaas_acfs/testdb30/opc/
   [root@khdyygw-mpjxb1Example ]# ls -altr *.ora
   opc3testdb30.ora
   [root@khdyygw-mpjxb1Example ]# cat opctestdb30.ora
   OPC_HOST=https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/dbbackupphx
   OPC_WALLET='LOCATION=file:/var/opt/oracle/dbaas_acfs/testdb30/opc/opc_wallet CREDENTIAL_ALIAS=alias_opc'
   OPC_CONTAINER=bUG3TFsSi8QzjWfuTxqqExample
   _OPC_DEFERRED_DELETE=false
   ```

4. Confirm that the `cwallet.sso` file exists in the directory specified in the `OPC_WALLET` parameter, and confirm that the file has the correct permissions. The file permissions should have the octal value of "600" (`-rw-------`). Use the following command:

   ```bash
   ls -ltr /var/opt/oracle/dbaas_acfs/<database_name>/opc/opc_wallet
   ```

   For example:

   ```bash
   [root@khdyygw-mpjxb1Example]# ls -altr /var/opt/oracle/dbaas_acfs/testdb30/opc/opc_wallet
   -rw------- 1 oracle oinstall 0 Oct 29 01:59 cwallet.sso.lck
   -rw------- 1 oracle oinstall 111231 Oct 29 01:59 cwallet.sso
   ```
TDE Wallet and Backup Failures

Incorrect TDE Wallet Location Specification

For backup operations to work, the $ORACLE_HOME/network/admin/sqlnet.ora file must contain the ENCRYPTION_WALLET_LOCATION parameter formatted exactly as follows:

```
ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/var/opt/oracle/dbaas_acfs/<database_name>/tde_wallet))
```

To check the TDE wallet location specification

Use the `cat` command to check the TDE wallet location specification. For example:

```
[oracle@orcl tde]$ cat $ORACLE_HOME/network/admin/sqlnet.ora
ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/var/opt/oracle/dbaas_acfs/<database_name>/tde_wallet))
```

Incorrect State of the TDE Wallet

Database backups fail if the TDE wallet is not in the proper state. The following scenarios can cause this problem:

**The ORACLE_UNQNAME environment variable was not set when the database was started using SQL*Plus**

If the database was started using SQL*Plus, and the ORACLE_UNQNAME environment variable was not set, the wallet is not opened correctly.

To fix the problem, start the database using the `srvctl` utility:

```
srvctl start database -d <db_unique_name>
```

**A pluggable database was added with an incorrectly configured master encryption key**

In a multitenant environment for Oracle Database versions that support PDB-level keystore, each PDB has its own master encryption key. For Oracle 18c databases, this encryption key is stored in a single keystore used by all containers. (Oracle Database 19c does not support a keystore at the PDB level.) After you create or plug in a new PDB, you must create and activate a master encryption key for it. If you do not do so, the STATUS column in the `v$encryption_wallet` view shows the value OPEN_NO_MASTER_KEY.

To check the master encryption key status and create a master key, do the following:

1. Review the the STATUS column in the `v$encryption_wallet` view, as shown in the following example:

```
SQL> alter session set container=pdb2;
Session altered.

SQL> select WRL_TYPE,WRL_PARAMETER,STATUS,WALLET_TYPE from v$encryption_wallet;

WRL_TYPE   WRL_PARAMETER                                       STATUS   WALLET_TYPE
---------- ----------------------------------------------- -------- --------------------
FILE       /var/opt/oracle/dbaas_acfs/testdb30/tde_wallet/      OPEN_NO_MASTER_KEY AUTOLOGIN
```
2. Confirm that the PDB is in READ WRITE open mode and is not restricted, as shown in the following example:

```
SQL> show pdbs
```

<table>
<thead>
<tr>
<th>CON_ID</th>
<th>CON_NAME</th>
<th>OPEN MODE</th>
<th>RESTRICTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>PDB$SEED</td>
<td>READ ONLY</td>
<td>NO</td>
</tr>
<tr>
<td>3</td>
<td>PDB1</td>
<td>READ WRITE</td>
<td>NO</td>
</tr>
<tr>
<td>4</td>
<td>PDB2</td>
<td>READ WRITE</td>
<td>NO</td>
</tr>
</tbody>
</table>

The PDB cannot be open in restricted mode (the RESTRICTED column must show NO). If the PDB is currently in restricted mode, review the information in the PDB_PLUG_IN_VIOLATIONS view and resolve the issue before continuing. For more information on the PDB_PLUG_IN_VIOLATIONS view and the restricted status, review the documentation on pluggable database for your Oracle database version.

3. Create and activate a master encryption key for the PDB:

- Set the container to the PDB:
  ```
  SQL> ALTER SESSION SET CONTAINER = pdb;
  ```
- Create and activate a master encryption key in the PDB by executing the following command:
  ```
  SQL> ADMINISTER KEY MANAGEMENT SET KEY USING TAG '<tag>' FORCE KEYSTORE IDENTIFIED BY <keystore-password> WITH BACKUP USING '<backup_identifier>';
  ```

Note the following:
- The USING TAG clause is optional and can be used to associate a tag with the new master encryption key.
- The WITH BACKUP clause is optional and can be used to create a backup of the keystore before the new master encryption key is created.

You can also use the dbaascli commands `dbaascli tde status` and `dbaascli tde rotate masterkey` to investigate and manage your keys.

4. Confirm that the status of the wallet has changed from OPEN_NO_MASTER_KEY to OPEN by querying the `v$encryption_wallet` view as shown in step 1.

**Incorrect Configuration Related to the TDE Wallet**

Configuration parameters related to the TDE wallet can cause backups to fail.

*To check configuration related to the TDE wallet*

Confirm that the wallet status is open and the wallet type is auto login by checking the `v$encryption_wallet` view. For example:

```
SQL> select status, wrl_parameter, wallet_type from v$encryption_wallet;
```

<table>
<thead>
<tr>
<th>STATUS</th>
<th>WRL_PARAMETER</th>
<th>WALLET_TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN</td>
<td>/var/opt/oracle/dbaas_acfs/testdb30/tde_wallet/</td>
<td>AUTOLOGIN</td>
</tr>
</tbody>
</table>
For pluggable databases (PDBs), ensure that you switch to the appropriate container before querying `v$encryption_wallet` view. For example:

```
[oracle@paulo ~]$ sqlplus / as sysdba
SQL> alter session set container=pdb1;
Session altered.
SQL> select WRL_TYPE,WRL_PARAMETER,STATUS,WALLET_TYPE from v$encryption_wallet;
```

<table>
<thead>
<tr>
<th>WRL_TYPE</th>
<th>WRL_PARAMETER</th>
<th>STATUS</th>
<th>WALLET_TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE</td>
<td>/var/opt/oracle/dbaas_acfs/testdb30/tde_wallet/</td>
<td>OPEN</td>
<td>AUTOLOGIN</td>
</tr>
</tbody>
</table>

**Missing TDE Wallet File**

The TDE wallet file (`ewallet.p12`) can cause backups to fail if it is missing, or if it has incompatible file system permissions or ownership. Check the file as shown in the following example:

```
[root@khdyygw-mpjxb1example /]# ls -altr /var/opt/oracle/dbaas_acfs/<database_name>/tde_wallet/ewallet.p12
```

```
total 76
-rw------ 1 oracle oinstall 5467 Oct 1 20:17 ewallet.p12
```

The TDE wallet file should have file permissions with the octal value "600" (`-rw-------`), and the owner of this file should be a part of the `oinstall` operating system group.

**Missing Auto Login Wallet File**

The auto login wallet file (`cwallet.sso`) can cause backups to fail if it is missing, or if it has incompatible file system permissions or ownership. Check the file as shown in the following example:

```
[root@khdyygw-mpjxb1example /]# ls -altr /var/opt/oracle/dbaas_acfs/<database_name>/tde_wallet/cwallet.sso
```

```
total 76
-rw------ 1 oracle oinstall 5512 Oct 1 20:18 cwallet.sso
```

The auto login wallet file should have file permissions with the octal value "600" (`-rw-------`), and the owner of this file should be a part of the `oinstall` operating system group.

**Obtaining Further Assistance**

If you were unable to resolve the problem using the information in this topic, follow the instructions in Diagnostic Data Collection For Oracle Database Cloud Service Instances (OCI-C) (Doc ID 2219701.1) to collect relevant database and diagnostic information. After you have collected this information, contact Oracle Support.

**Deprecated Database Service APIs**

This topic lists deprecated APIs for the Database service.
**Deprecated Exadata Cloud Service APIs**

Oracle Cloud Infrastructure's Exadata DB system APIs were deprecated on November 15, 2020. Existing Exadata systems can be converted to the [new Exadata resource model](#) to use the new APIs. See [Switching an Exadata DB System to the New Resource Model and APIs](#) on page 1228 for more information.

**Important!** Support for the Exadata DB system APIs will end on **May 15, 2021**. Oracle recommends that you migrate your Exadata Cloud Service instances to the new resource model APIs as soon as possible. Converting to the new resource model does not involve any system downtime.

<table>
<thead>
<tr>
<th>Unsupported API</th>
<th>Replacement APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LaunchDbSystem</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>CreateCloudExadataInfrastructure and CreateCloudVmCluster</td>
</tr>
<tr>
<td><strong>ListDbSystems</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>ListCloudExadataInfrastructures and ListCloudVmClusters</td>
</tr>
<tr>
<td><strong>GetDbSystem</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>GetCloudExadataInfrastructure and GetCloudVmCluster</td>
</tr>
<tr>
<td><strong>ChangeDbSystemCompartment</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>ChangeCloudExadataInfrastructureCompartment and ChangeCloudVmClusterCompartment</td>
</tr>
<tr>
<td><strong>UpdateDbSystem</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>UpdateCloudExadataInfrastructure and UpdateCloudVmCluster</td>
</tr>
<tr>
<td><strong>GetExadataIormConfig</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>GetCloudVmClusterIormConfig</td>
</tr>
<tr>
<td><strong>UpdateExadataIormConfig</strong> <em>(Exadata systems only)</em></td>
<td>UpdateVmClusterIormConfig</td>
</tr>
<tr>
<td><strong>TerminateDbSystem</strong> <em>(deprecated for Exadata systems only)</em></td>
<td>DeleteCloudExadataInfrastructure and DeleteCloudVmCluster</td>
</tr>
</tbody>
</table>

**Deprecated Autonomous Data Warehouse APIs**

Oracle Cloud Infrastructure's Autonomous Data Warehouse APIs were deprecated on Feb. 15, 2019.

**Important!** Support for these Autonomous Data Warehouse APIs will end on **Jul. 1, 2020**. Oracle recommends that you migrate your database workloads to the replacement APIs as soon as possible.

<table>
<thead>
<tr>
<th>Unsupported API</th>
<th>Replacement API</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CreateAutonomousDataWarehouse</strong></td>
<td>CreateAutonomousDatabase</td>
</tr>
<tr>
<td><strong>ListAutonomousDataWarehouses</strong></td>
<td>ListAutonomousDatabases</td>
</tr>
<tr>
<td><strong>GetAutonomousDataWarehouse</strong></td>
<td>GetAutonomousDatabase</td>
</tr>
<tr>
<td><strong>StartAutonomousDataWarehouse</strong></td>
<td>StartAutonomousDatabase</td>
</tr>
<tr>
<td><strong>StopAutonomousDataWarehouse</strong></td>
<td>StopAutonomousDatabase</td>
</tr>
<tr>
<td><strong>UpdateAutonomousDataWarehouse</strong></td>
<td>UpdateAutonomousDatabase</td>
</tr>
<tr>
<td><strong>GenerateAutonomousDataWarehouseWallet</strong></td>
<td>GenerateAutonomousDatabaseWallet</td>
</tr>
<tr>
<td><strong>RestoreAutonomousDataWarehouse</strong></td>
<td>RestoreAutonomousDatabase</td>
</tr>
<tr>
<td><strong>DeleteAutonomousDataWarehouse</strong></td>
<td>DeleteAutonomousDatabase</td>
</tr>
<tr>
<td><strong>CreateAutonomousDataWarehouseBackup</strong></td>
<td>CreateAutonomousDatabaseBackup</td>
</tr>
<tr>
<td><strong>ListAutonomousDataWarehouseBackups</strong></td>
<td>ListAutonomousDatabaseBackups</td>
</tr>
<tr>
<td><strong>GetAutonomousDataWarehouseBackup</strong></td>
<td>GetAutonomousDatabaseBackup</td>
</tr>
</tbody>
</table>
This chapter explains how to create and manage your DNS zones and guide traffic to your endpoints based on various conditions.

DNS and Traffic Management

**DNS**
The DNS service helps you create and manage your DNS zones.

**Traffic Management Steering Policies**
Traffic Management helps you guide traffic to your endpoints based on various conditions, including endpoint health and the geographic origins of DNS requests.

**DDoS Protection**
DDoS Protection is an always-on detection and mitigation platform for common DDoS volumetric attacks. The service protects against common layer 3 and 4 attacks like SYN floods, UDP floods, ICMP floods, and NTP Amplification attacks. DDoS Protection is included with all Oracle Cloud Infrastructure accounts and no configuration or monitoring is required.

**Overview of the DNS Service**
The Oracle Cloud Infrastructure Domain Name System (DNS) service lets you create and manage your DNS zones. You can create zones, add records to zones, and allow Oracle Cloud Infrastructure's edge network to handle your domain's DNS queries.

See Supported Resource Records on page 1686 for additional information.

**DNS Service Components**
The following list describes the components used to build a DNS zone and make it accessible from the internet.

**DOMAIN**
Domain names identify a specific location or group of locations on the Internet as a whole. A common definition of "domain" is the complete portion of the DNS tree that has been delegated to a user's control. For example, example.com or oracle.com.

**ZONE**
A zone is a portion of the DNS namespace. A Start of Authority record (SOA) defines a zone. A zone contains all labels underneath itself in the tree, unless otherwise specified.
LABEL

Labels are prepended to the zone name, separated by a period, to form the name of a subdomain. For example, the "www" section of www.example.com or the "docs" and "us-ashburn-1" sections of docs.us-ashburn-1.oraclecloud.com are labels. Records are associated with these domains.

CHILD ZONE

Child zones are independent subdomains with their own Start of Authority and Name Server (NS) records. The parent zone of a child zone must contain NS records that refer DNS queries to the name servers responsible for the child zone. Each subsequent child zone creates another link in the delegation chain.

RESOURCE RECORDS

A record contains specific domain information for a zone. Each record type contains information called record data (RDATA). For example, the RDATA of an A or AAAA record contains an IP address for a domain name, while MX records contain information about the mail server for a domain. OCI normalizes all RDATA into the most machine readable format. The returned presentation of your RDATA may differ from its initial input. For more information about RDATA, please see Supported DNS Resource Record Types.

DELEGATION

The name servers where your DNS is hosted and managed.

Ways to Access the DNS Service

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide.

To access the Console, you must use a supported browser. You can use the Console link at the top of this page to go to the sign-in page. Enter your tenancy, user name, and your password.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about available DNS service metrics and how to view them, see DNS Metrics on page 1704.

DNS Service Capabilities and Limits

The Oracle Cloud Infrastructure DNS service is limited to 1000 zones per account and 25,000 records per zone. Customers with zone and record size needs exceeding these values are encouraged to contact support at support.oracle.com. Zone file uploads are limited to 1 megabyte (MB) in size per zone file. If your zone file is larger than 1 MB, you will need to split the zone file into smaller batches to upload all of the zone information.
Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies. For more details about policies for DNS, see Details for the DNS Service.

Permissions are required for managing DNS. The level of access is cumulative as you go from inspect > read > use > manage. For example, the read verb covers permissions to read and inspect. The manage verb covers permissions for inspect, read, update, create, delete, and move.

Policy examples:

- To enable all operations on zones for a specific user group:
  
  Allow group <GroupName> to manage dns in tenancy <TenancyName>

- To enable a specific group to read zones:
  
  Allow group <GroupName> to read zones in tenancy <TenancyName>

- To create a read only DNS management group:
  
  Allow group <GroupName> to read dns in tenancy <TenancyName>

Using the DNS Management Overview to Manage DNS Services

This topic describes the Overview page in the DNS Management section of the Oracle Cloud Infrastructure Console. The Overview provides information on all of the available DNS services.

Manage DNS Services Section

The Manage DNS Services section provides you with details on Zones and Traffic Management Steering Policies and links to set them up.

Public DNS Zones hold the trusted DNS records that will reside on Oracle Cloud Infrastructure's nameservers. You can create public zones with publicly available domain names. Private DNS zones contain domain names that resolve DNS queries for private IP addresses within a VCN. You can create private zones to define your own domain name for private address resolution.

Traffic Management Steering Policies help you guide traffic to your endpoints based on various conditions, including endpoint health and the geographic origins of DNS requests.

Service Health and Documentation Section

The Service Health tile displays the availability status of all DNS zone management systems in the selected region, and allows you to easily navigate to the Console's Oracle Cloud Infrastructure status page to check the availability status of all Oracle Cloud Infrastructure services, by region.

The Documentation list provides quick access to information about DNS offerings.

Supporting Services Section

The Supporting Services section provides links to additional DNS Management services available in the Console.

- Private Views allows you to logically group a set of private DNS zones.
- HTTP Redirects allows you to redirect HTTP traffic to another URL.
- TSIG Keys ensures that DNS packets originate from an authorized sender.
Getting Started Section

To make it easier to set up DNS Management, the Console has the following quickstart links to set up DNS services.

- **Set Up a Zone** creates and publishes a zone, complete with the necessary records.
- **Private DNS** allows you to define your own domain name for private endpoints.
- **Set Up Steering Policies** allows you to define the traffic management behavior for your zones.

Getting Started with DNS

If you're new to Oracle Cloud Infrastructure DNS, this topic gives guidance on how to proceed.

**What is DNS?**

The Domain Name System (DNS) translates human-readable domain names to machine-readable IP addresses. A DNS nameserver stores the DNS records for a zone, and responds with answers to queries against its database. When you type a domain name into your browser, your operating system queries several DNS nameservers until it finds the authoritative nameserver for that domain. The authoritative nameserver then responds with an IP address or other requested record data. The answer is then relayed back to your browser and the DNS record is resolved to the web page.

**Creating a Zone**

In this step, you will create a zone. A zone holds the trusted DNS records that will reside on Oracle Cloud Infrastructure’s nameservers.

*To add a zone*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click **Create Zone**.
3. In the **Create Zone** dialog box, choose one of the following methods:
   - **Manual** - Enter the following:
     - **Zone Name**: Enter the name of a zone you want to create. Avoid entering confidential information.
     - **Zone Type**: If you want to control the zone contents directly within Oracle Cloud Infrastructure, select **Primary**. If you want Oracle Cloud Infrastructure to pull zone contents from an external server, select **Secondary** and enter your **Zone Master Server IP** address.
   - **Import** - Drag and drop, select, or paste a valid zone file into the Import Zone File window. The zone is imported as a primary zone. For information about formatting a zone file, see **Formatting a Zone File**.
4. Click **Submit**.

The system creates and publishes the zone, complete with the necessary SOA and NS records. For more information on adding a record to your zone, see To add a zone record.

**Delegating Your Zone**

In this step, you will delegate your domain with your registrar. Delegating your domain with your domain's registrar makes your Oracle Cloud Infrastructure hosted zone accessible through the internet.

*To delegate a zone*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the Zone Name for the zone you want to delegate. Zone details and a list of records appear.
3. Use the **Type** sort filter to locate the NS records for your zone.
4. Note the name servers in the RDATA field within each NS record.
5. You can use the noted name servers to change your domain's DNS delegation. Refer to your registrar's documentation for instructions.

   **Note:**

   Once delegation has completed, allow 24 hours for your delegation to propagate across the internet.
To add a zone record

**Tip:**

There are many record types you can add to your zone, depending on your goals for the zone and its DNS management.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the **Zone Name** in which you want to add a record. Zone details and a list of records appear.

**Tip:**

You can use the Zone Name sort filter to list to sort zone names alphanumerically in ascending or descending order.

3. Click **Add Record**.
4. In the **Add Record** dialog box, select a record type from the drop-down list, and then enter the information for the record. Avoid entering confidential information. For more information about record types, see **Supported Resource Records** on page 1686.
5. (Optional) Click the **Add Another Record** check box to add multiple records in succession.
6. Click **Submit**.
7. Once your records have been added, click **Publish Changes**.
8. In the confirmation dialog box, click **Publish Changes**.

**Common DNS Zone Record Types**

For a complete list of records supported by Oracle Cloud Infrastructure DNS, see **Supported Resource Records** on page 1686.

**A**

An address record used to point a hostname to an IPv4 address. For more information about A records, see **RFC 1035**.

**AAAA**

An address record used point a hostname at an IPv6 address. For more information about AAAA records, see **RFC 3596**.

**CNAME**

A Canonical Name record identifies the canonical name for a domain. For more information about CNAME records, see **RFC 1035**.

**Note:**

Per **RFC 1912**, CNAMEs cannot be placed at the apex of the zone.

**MX**

A Mail Exchanger record defines the mail server accepting mail for a domain. MX records must point to a hostname. MX records must not point to a CNAME or IP address. For more information about MX records, see **RFC 1035**.

**TXT**

A Text record holds descriptive, human readable text, and can also include non-human readable content for specific uses. It is commonly used for SPF records and DKIM records that require non-human readable text items. For more information about TXT records, see **RFC 1035**.

**Testing DNS Using BIND's dig Tool**

Using the Domain Information Groper (dig) command line tool, you can test against the delegation where your domain is hosted, and you will immediately see whether the change took place without accounting for the cache or TTL (Time to Live) that you have configured.
For more information on using dig to test your DNS, see Testing DNS Using BIND'S dig Tool on page 1696.

Managing DNS Service Zones

The Oracle Cloud Infrastructure DNS service enables you to manage zones within the Console.

Using the Console

Managing Zones and Zone Records

For information on creating private DNS zone, see Private DNS on page 1698.

To add a zone

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click Create Zone.
3. In the Create Public Zone dialog box, choose one of the following methods:
   - Manual - Enter the following:
     - Zone Name: Enter the name of a zone you want to create. Avoid entering confidential information.
     - Zone Type:
       - Primary - Select this option if you want to control the zone contents directly within Oracle Cloud Infrastructure.
       - Secondary - Select this option if you want Oracle Cloud Infrastructure to pull zone contents from an external server. Enter your Master Server IP address. Optionally, you can select an existing TSIG key in a specified compartment that is associated with the master server. For more information, see Managing TSIG Keys on page 1694.
   - Import - Drag and drop, select, or paste a valid zone file into the Import Zone File window. The zone is imported as a primary zone. For information about formatting a zone file or how to amend a zone file exported from GoDaddy.com, see Formatting a Zone File.
4. Click Create.

The system creates and publishes the zone, complete with the necessary SOA and NS records. For more information on adding a record to your zone, see To add a zone record.

To update a secondary zone

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the secondary Zone Name you want to update.
   
   Tip:
   You can use the Zone Type sort filter to sort zone type alphanumerically in ascending or descending order.
3. Click Master Server IPs.
4. Select the checkbox for the Master Server IP you want to update, and then select Edit from the Actions drop-down menu.
5. Make the needed changes, and then click Submit.
6. (Optional) Click Add Master Server to add another Master Server IP address.
7. Click Publish Changes.
8. In the confirmation dialog box, click Publish Changes.

Tip:
For OCI to transfer data from your zone, your nameservers must be able to accept a transfer request from the following IP addresses: 208.78.68.65, 204.13.249.65, 2600:2001:0:1::65, 2600:2003:0:1::65
**To delete a zone**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletion permanently removes a zone from your DNS service.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Select the checkbox for the zone you want to delete.
3. Click **Delete**. The zone is staged for deletion.
4. Click **Publish Changes** to delete the zone.
5. In the confirmation dialog box, click **Publish Changes**.

**To add a zone record**

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are many record types you can add to your zone, depending on your goals for the zone and its DNS management.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the **Zone Name** in which you want to add a record. If you are adding a record to a private zone, click the **Private Zones** tab and then click the zone name. Zone details and a list of records appear.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To locate zones in the Private Zones tab, you can use filters to sort by zones that are protected (system generated) or by associated private view names.</td>
</tr>
</tbody>
</table>

3. Click **Add Record**.
4. In the **Add Record** dialog box, select a record type from the drop-down list, and then enter the information for the record. Avoid entering confidential information. For more information about record types, see **Supported Resource Records** on page 1686.
5. (Optional) Click the **Add Another Record** check box to add multiple records in succession.
6. Click **Submit**.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When records are added, they are staged to allow for multiple records to be combined into a set. Before records take effect, they must be published.</td>
</tr>
</tbody>
</table>

7. Once your records have been added, click **Publish Changes**.
8. In the confirmation dialog box, click **Publish Changes**.

**To update a zone record**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Records</td>
</tr>
<tr>
<td>You can change various components of the records within your zones, such as time-to-live (TTL) and relevant RDATA. However, some records contain information that cannot be changed. You can attempt changes to such records through the <strong>Actions</strong> menu, but the system might not permit updates to some fields.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the **Zone Name** in which you want to update a record. If you are updating a record in a private zone, click the **Private Zones** tab and then click the zone name. Zone details and a list of records appear.

   **Tip:**

   To locate zones in the Private Zones tab, you can use filters to sort by zones that are protected (system generated) or by associated private view names.

3. To help find a record, you can use the following filter options:
   - Enter the name of the record's domain in the **Search** field.
   - To find unpublished records, select the **Staged** check box.
   - To find published records, select the **Unstaged** check box.
   - Use the **Is Protected** sort filter to sort by records that are protected.
   - Use the **Record Type** sort filter to sort records.

4. Select the check box for the record you want to update, and select **Edit** from the **Actions** drop-down menu.

5. In the **Edit Record** dialog box, make the needed changes, and then click **Submit**.

   **Note:**

   When records are added, they are staged to allow for multiple records to be combined into a set. Before records take effect, they must be published.

6. Click **Publish Changes**.

7. In the confirmation dialog box, click **Publish Changes**.

**Reverting Changes Before Publishing**

You can revert records to their current published state before you publish changes. Once a record has been published, it cannot be reverted. Select the check box for the record you want to revert, and then select **Revert** from the **Actions** drop-down menu.

**To delete a zone record**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.

2. Click the **Zone Name** in which you want to delete a record. If you are deleting a record in a private zone, click the **Private Zones** tab and then click the zone name. Zone details and a list of records appear.

   **Tip:**

   To locate zones in the Private Zones tab, you can use filters to sort by zones that are protected (system generated) or by associated private view names.

3. Select the check box for the record you want to delete, and then select **Delete** from the **Actions** drop-down menu.

4. Click **Publish Changes**.

5. In the confirmation dialog box, click **Publish Changes**.

**To delegate a zone**

To make your Oracle Cloud Infrastructure hosted zone accessible through the internet, you must delegate your domain with your domain's registrar.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.

2. Click the **Zone Name** for the zone you want to delegate. Zone details and a list of records appear.

3. Use the **Type** sort filter to locate the NS records for your zone.

4. Note the name servers in the RDATA field within each NS record.

5. You can use the noted name servers to change your domain's DNS delegation. Refer to your registrar's documentation for instructions.
To move a zone to a different compartment

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. In the List Scope section, select a compartment.
3. Find the zone in the list, click the the Actions icon (three dots), and then click Choose New Compartment.
4. Choose the destination compartment from the list.
5. Click Move Resource.

For more information, see Managing Compartments on page 2431.

To add a TSIG key

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the secondary Zone Name you want to update. Zone details and a list of master server IPs appear.
3. Under Zone Information, click Add beside the TSIG field.
4. In the Add TSIG Key dialog box, select one of the following options:
   * Create New TSIG Key - Enter the following information:
     * Name: The name of the key used in domain name syntax. The name should reflect the names of the hosts and uniquely identify the key among a set of keys these two hosts may share at any given time.
     * Algorithm: Select the public key's algorithm used to encrypt or decrypt data. Applicable algorithms include hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-h384, and hmac-sha512.
     * Secret: The base64 string encoding the binary shared secret that corresponds to the key. A maximum value of 255 characters is allowed.
     * Tags: Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
   * Select Existing TSIG Key - Select a TSIG Key from the drop-down menu.
5. Click Add.
6. Click Publish.
7. In the confirmation dialog box, click Publish Changes.

For more information, see Managing TSIG Keys on page 1694.

To remove a TSIG key from a zone

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the secondary Zone Name you want to update. Zone details and a list of master server IPs appear.
3. Under Zone Information, click Remove beside the TSIG key name.
4. Click Publish.
5. In the confirmation dialog box, click Publish Changes. Changes cannot be made to this zone while it is updating.

For more information, see Managing TSIG Keys on page 1694.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage your DNS zones:

* GetZone
* ListZones
* CreateZone
* UpdateZone
* DeleteZone
* PatchZoneRecords (add or delete records)
Setting Up Reverse DNS Zones

Reverse DNS, or rDNS, maps an IP address to a hostname. Reverse DNS serves a number of different purposes from email to network troubleshooting. Some of the benefits include:

- Adding a label for network troubleshooting tools such as traceroute.
- Populating the “Received:” header field in an SMTP email.
- Checking for generic reverse DNS such as 1-2-3-4.example.com to identify spammers.
- Verifying a relationship between the owner of a domain name and the owner of the server (IP address).
- Writing a human readable hostname to the log files for system monitoring tools.
- Determining which hostname is affected when maintenance is performed on an IP address.

Before getting started with setting up reverse DNS within your Oracle Cloud Infrastructure account, contact your IP provider and confirm that they allow delegation of your reverse DNS zone. If they do not allow delegation, typically they can host your pointer record (PTR) for you and no reverse DNS configurations are required within your Oracle Cloud Infrastructure account. If they do allow delegation, confirm the exact syntax of the reverse DNS hostname with them, as some providers use slashes and some use dashes. Additionally, if you are delegating a reverse DNS zone, confirm that this zone matches exactly what you configure in your Oracle Cloud Infrastructure account as this is necessary in order for delegation to work properly.

After you create and publish your reverse DNS zone and PTR records, you can update your reverse DNS zone delegation with your IP provider. Delegation changes are not required with your domain registrar with a reverse DNS zone.

Setting up a reverse DNS zone is different for the two types of IP address blocks. Use the following procedures to set up a reverse DNS zone for your IP address block type.

Setting Up Reverse DNS for Classless Address Block (Partial Range of IP Addresses)

To find your reverse DNS zone name using classless address block

1. Make a note of your network IP address. For example, 192.168.15.224/27.
2. Remove the netmask portion of the address. This is the number after the slash (/). For example, remove the ‘27’ after your IP address, 192.168.15.224/27.
3. Reverse the order of the remaining octets. For example, 224.15.168.192.
4. Append ‘in-addr.arpa’ to the end of the IP address. For example, 224.15.168.192.in-addr.arpa.

5. Add the netmask back into the address. For example, 224-27.15.168.192.in-addr.arpa.

In this example, 224-27.15.168.192.in-addr.arpa is your reverse DNS zone name.

To create your DNS zone

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click Create Zone.
3. In the Create Zone dialog box, choose one of the following methods:

- **Manual** - Enter the following:
  
  a. **Zone Name**: Enter the name of a zone you want to create. Avoid entering confidential information.
  
  b. **Zone Type**: If you want to control the zone contents directly within OCI, select **Primary**. If you want OCI to pull zone contents from an external server, select **Secondary** and enter your **Zone Master Server IP** address.

- **Import** - Drag and drop, select, or paste a valid zone file into the Import Zone File window. The zone is imported as a primary zone. For information about formatting a zone file or how to amend a zone file exported from GoDaddy.com, see **Formatting a Zone File** on page 1689.

4. Click **Submit**.

The system creates and publishes the zone, complete with the necessary SOA and NS records.

**To create a pointer record (PTR) for each host address**

As part of the process of setting up a reverse DNS zone, you need to add a PTR record for each host address. This is done specifically for reverse DNS zones to ensure requests are properly routed for resolution.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the Zone Name in which you want to add the PTR record. Zone details and a list of records appear.

   **Tip:**
   
   You can use the Zone Name sort filter to list to sort zone names alphanumerically in ascending or descending order.

3. Click **Add Record**.
4. In the Add Record dialog box, select the **PTR – Pointer** record type from the drop-down list. Enter the following information:

   - **Name**: Optional. Name of the subdomain.
   - **TTL**: Click the lock icon to unlock this field. All PTR records in the zone will be updated to reflect the last changes to TTL. This value indicates how long you want to allow external nameservers to cache the information about a given DNS record.
   - **TTL Unit**: Select the unit of time used for the TTL value.
   - **RData Mode**: Select Basic or Advanced format. If you select Advanced, enter the canonical hostname (for example, *example.com*) that the record is going to point to in the RDATA field.
   - **Hostname**: The web address of your zone.

   For more information about the PTR record type, see **Supported Resource Records** on page 1686.

5. Click **Submit**.
6. Once your record has been added, click **Publish Changes**.
7. In the confirmation dialog box, click **Publish Changes**.

**To add CNAME records for each host at your ISP**

If your IP provider does not automatically configure the CNAME record on your behalf, you will need to add a CNAME record for each host at your ISP. This is done specifically for reverse DNS zones to ensure requests are properly routed for resolution.

1. Make a note of the IP address and your desired CNAME for each host in your new reverse DNS zone.
2. Contact your ISP and request that they append a CNAME record for each host in your Oracle Cloud Infrastructure DNS zone to your account with them.
3. Test the reverse DNS path by running the following command:

   ```
   dig -x <insert any regular forward-formatted IP address from the zone> +trace
   ```

   See **Testing DNS Using BIND’S dig Tool** on page 1696 for more information.
The returned information should show that your reverse domain is now being resolved.

To update your zone delegation

To make your Oracle Cloud Infrastructure hosted zone accessible through the internet, you must delegate your domain with your domain's registrar (usually the website where you purchased your domain, such as GoDaddy.com or Bluehost.com).

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Zone Name for the zone you want to delegate. Zone details and a list of records appear.
3. Use the Type sort filter to locate the NS records for your zone.
4. Note the name servers in the RDATA field within each NS record.

You can use the noted name servers to change your domain's DNS delegation. Refer to your registrar's documentation for instructions.

Setting Up Reverse DNS for Full Address Block

To find your reverse DNS zone name using full address block

1. Make a note of your network IP address. For example, 192.168.15.0.
2. Remove the netmask portion of the address (the last number in the set of 4). For example, 192.168.15.
3. Reverse the order of the remaining three octets. For example, 15.168.192.
4. Append ‘in-addr.arpa’ to the end. For example, 15.168.192.in-addr.arpa

In this example, 15.168.192.in-addr.arpa is your reverse DNS zone name.

To create your DNS zone

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click Create Zone.
3. In the Create Zone dialog box, choose one of the following methods:
   • Manual - Enter the following:
     a. Zone Name: Enter the name of a zone you want to create. Avoid entering confidential information.
     b. Zone Type: If you want to control the zone contents directly within OCI, select Primary. If you want OCI to pull zone contents from an external server, select Secondary and enter your Zone Master Server IP address.
   • Import - Drag and drop, select, or paste a valid zone file into the Import Zone File window. The zone is imported as a primary zone. For information about formatting a zone file or how to amend a zone file exported from GoDaddy.com, see Formatting a Zone File on page 1689.
4. Click Submit.

The system creates and publishes the zone, complete with the necessary SOA and NS records.

To create a pointer record (PTR) for each host address

As part of the process of setting up a reverse DNS zone, you need to add a PTR record for each host address. This is done specifically for reverse DNS zones to ensure requests are properly routed for resolution.

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Zone Name in which you want to add the PTR record. Zone details and a list of records appear.

   Tip:
   You can use the Zone Name sort filter to list to sort zone names alphanumerically in ascending or descending order.

3. Click Add Record.
4. In the Add Record dialog box, select the **PTR – Pointer** record type from the drop-down list. Enter the following information:

   a. **Name**: Optional. Name of the subdomain.
   
   b. **TTL**: Click the lock icon to unlock this field. All PTR records in the zone will be updated to reflect the last changes to TTL. This value indicates how long you want to allow external nameservers to cache the information about a given DNS record.
   
   c. **TTL Unit**: Select the unit of time used for the TTL value.
   
   d. **RData Mode**: Select Basic or Advanced format. If you select Advanced, enter the canonical hostname (for example, `example.com`) that the record is going to point to in the RDATA field.
   
   e. **Hostname**: The web address of your zone.

   For more information about the PTR record type, see [Supported Resource Records](#) on page 1686.

5. Click **Submit**.

6. Once your record has been added, click **Publish Changes**.

7. In the confirmation dialog box, click **Publish Changes**.

To update your zone delegation

To make your Oracle Cloud Infrastructure hosted zone accessible through the internet, you must delegate your domain with your domain's registrar.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the Zone Name for the zone you want to delegate. Zone details and a list of records appear.
3. Use the **Type** sort filter to locate the NS records for your zone.
4. Note the name servers in the RDATA field within each NS record.

You can use the noted name servers to change your domain's DNS delegation. Refer to your registrar's documentation for instructions.

**Supported Resource Records**

The Oracle Cloud Infrastructure DNS service supports many resource record types. The following list provides a brief explanation of the purpose of each supported record type. Avoid entering confidential information when entering record data. The RFC links direct you to further information about the record types and data structure.

**Note About RDATA**

Oracle Cloud Infrastructure normalizes all RDATA into the most machine readable format. The returned presentation of your RDATA may differ from its initial input.

**Example:**

The RDATA for the ALIAS, CNAME, DNAME, MX, and NS record types may contain one or more absolute domain names. If the specified RDATA for one of these record types does not end in a dot or period to represent the root, the period will be added.

```
```

You can use various DNS libraries to normalize your RDATA before input.

<table>
<thead>
<tr>
<th>Programming Language</th>
<th>Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go</td>
<td>DNS Library in Go</td>
</tr>
<tr>
<td>Java</td>
<td>dnsjava</td>
</tr>
<tr>
<td>Python</td>
<td>dnspython</td>
</tr>
</tbody>
</table>
DNS Resource Record Types

A
An address record used to point a hostname to an IPv4 address. For more information about A records, see RFC 1035.

AAAA
An address record used point a hostname at an IPv6 address. For more information about AAAA records, see RFC 3596.

ALIAS
A private pseudo-record that allows CNAME functionality at the apex of a zone.

CAA
A Certification Authority Authorization record allows a domain name holder to specify one or more Certification Authorities authorized to issue certificates for that domain. For more information about CAA records, see RFC 6844.

CDNSKEY
A Child DNSKEY moves a CDNSSEC key from a child zone to a parent zone. The information provided in this record must match the CDNSKEY information for your domain at your other DNS provider. This record is automatically created if you enable DNSSEC on a primary zone in Oracle Cloud Infrastructure DNS. For more information about CDNSKEY, see RFC 7344.

CDS
A Child Delegation Signer record is a child copy of a DS record, for transfer to a parent zone. For more information about CDS records, see RFC 7344.

CERT
A Certificate record stores public key certificates and related certificate revocation lists in the DNS. For more information about CERT records, see RFC 2538 and RFC 4398.

CNAME
A Canonical Name record identifies the canonical name for a domain. For more information about CNAME records, see RFC 1035.

CSYNC
A Child-to-Parent Synchronization record syncs records from a child zone to a parent zone. For more information about CNAME records, see RFC 7477.

DHCID
A DHCP identifier record provides a way to store DHCP client identifiers in the DNS to eliminate potential hostname conflicts within a zone. For more information about DHCID, see RFC 4701.

DKIM
A Domain Keys Identified Mail is a special TXT record set up specifically to supply a public key used to authenticate arriving mail for a domain. For more information about DKIM records, see RFC 6376.

DNAME
A Delegation Name record has similar behavior to a CNAME record, but allows you to map an entire subtree beneath a label to another domain. For more information about DNAME records, see RFC 6672.

DNSKEY
A DNS Key record documents public keys used for DNSSEC. The information in this record must match the DNSKEY information for your domain at your other DNS provider. For more information about DNSKEY records, see RFC 4034.
DS
A Delegation Signer record resides at the top-level domain and points to a child zone's DNSKEY record. DS records are created when DNSSEC security authentication is added to the zone. For more information about DS records, see RFC 4034.

IPSECKEY
An IPSec Key record stores public keys for a host, network, or application to connect to IP security (IPSec) systems. For more information on IPSECKEY records, see RFC 4025.

KEY
A Key record stores a public key that is associated with a domain name. Currently only used by SIG and TKEY records. IPSECKEY and DNSKEY have replaced key for use in IPSec and DNSSEC, respectively. For more information about KEY records, see RFC 4025.

KX
A Key Exchanger record identifies a key management agent for the associated domain name with some cryptographic systems (not including DNSSEC). For more information about KX records, see RFC 2230.

LOC
A Location record stores geographic location data of computers, subnets, and networks within the DNS. For more information about LOC records, see RFC 1876.

MX
A Mail Exchanger record defines the mail server accepting mail for a domain. MX records must point to a hostname. MX records must not point to a CNAME or IP address. For more information about MX records, see RFC 1035.

NS
A Nameserver record lists the authoritative nameservers for a zone. Oracle Cloud Infrastructure DNS automatically generates NS records at the apex of each new primary zone. For more information about NS records, see RFC 1035.

PTR
A Pointer record reverse maps an IP address to a hostname. This behavior is the opposite of an A Record, which forward maps a hostname to an IP address. PTR records are commonly found in reverse DNS zones. For more information about PTR records, see RFC 1035.

PX
A resource record used in X.400 mapping protocols. For more information about PX records, see RFC 822 and RFC 2163.

SOA
A Start of Authority record specifies authoritative information about a DNS zone, including:
- The primary nameserver.
- The email of the domain administrator.
- The domain serial number.
- Several timers relating to refreshing the zone.

The Oracle Cloud Infrastructure DNS automatically generates an SOA record when a zone is created. For more information about SOA records, see RFC 1035.
DNS and Traffic Management

SPF
A Sender Policy Framework record is a special TXT record used to store data designed to detect email spoofing. For more information about SPF records, see RFC 4408.

SRV
A Service Locator record allows administrators to use several servers for a single domain. For more information about SRV records, see RFC 2782.

SSHFP
An SSH Public Key Fingerprint record publishes SSH public host key fingerprints using the DNS. For more information about SSHFP records, see RFC 6594.

TLSA
A Transport Layer Security Authentication record associates a TLS server certificate, or public key, with the domain name where the record is found. This relationship is called a TLSA certificate association. For more information about TLSA records, see RFC 6698.

TXT
A Text record holds descriptive, human readable text, and can also include non-human readable content for specific uses. It is commonly used for SPF records and DKIM records that require non-human readable text items. For more information about TXT records, see RFC 1035.

Formatting a Zone File
A zone file is a text file that describes a DNS zone. The BIND file format is the industry preferred zone file format and has been widely adopted by DNS server software. The format is defined in RFC 1035.

Example of a Zone File
This is an example of a zone file downloaded from Oracle Cloud Infrastructure DNS.

```
$ORIGIN example.com.
@ 3600 SOA ns1.p30.oraclecloud.net. (zone-admin.dyndns.com. ; address of responsible party
  2016072701 ; serial number
  3600 ; refresh period
  600 ; retry period
  604800 ; expire time
  1800 ) ; minimum ttl
86400 NS ns1.p68.dns.oraclecloud.net.
86400 NS ns2.p68.dns.oraclecloud.net.
86400 NS ns3.p68.dns.oraclecloud.net.
86400 NS ns4.p68.dns.oraclecloud.net.
3600 MX 10 mail.example.com.
3600 MX 20 vpn.example.com.
3600 MX 30 mail.example.com.
60 A 204.13.248.106
3600 TXT "v=spf1 includespf.oraclecloud.net ~all"
mail 14400 A 204.13.248.106
vpn 60 A 216.146.45.240
webapp 60 A 216.146.46.10
webapp 60 A 216.146.46.11
www 43200 CNAME example.com.
```

Note:

Record Classes
DNS and Traffic Management

In the example zone file above, no record classes are displayed. Oracle Cloud Infrastructure DNS only works with Internet (IN) class records but omits the class information in zone files for efficiency purposes.

Anatomy of a Zone File

$ORIGIN indicates a DNS node tree and will typically start a DNS zone file. Any host labels below the origin will append the origin hostname to assemble a fully qualified hostname. Any host label within a record that uses a fully qualified domain terminating with an ending period will not append the origin hostname.

Example: With $ORIGIN example.com., any record where the host label field is not followed by a period, example.com. will be appended to them.

The “@” symbol is a special label that indicates the $ORIGIN should replace the “@” symbol. This is typically used for the apex of a zone.

SOA Record – The $ORIGIN is followed by the zone’s Start Of Authority (SOA) record. An SOA record is required for each zone. It contains the name of the zone, the e-mail address of the party responsible for administering the domain’s zone file, the current serial number of the zone, the primary nameserver of the zone, and various timing elements (measured in seconds).

SOA Record Format

```
@     IN     SOA    {primary-name-server}     {hostmaster-email} (
{serial-number}
{time-to-refresh}
{time-to-retry}
{time-to-expire}
{minimum-TTL} )
```

- **Primary Name Server** – The nameserver that contains the original zone file and not an AXFR transferred copy.
- **Hostmaster Email** – Address of the party responsible for the zone. A period “.” is used in place of an “@” symbol. For email addresses that contain periods, replace the periods with a slash “/”.
- **Serial Number** – Version number of the zone. The serial number will increase with each subsequent update to your zone.
- **Time To Refresh** – How long a nameserver should wait prior to checking for a serial number increase within the primary zone file, in seconds. An increased serial number detected by a secondary DNS nameserver means a transfer is needed to sync your records. Only applies to zones using secondary DNS.
- **Time To Retry** – How long a nameserver should wait prior to retrying to update a zone after a failed attempt, in seconds. Only applies to zones using secondary DNS.
- **Time To Expire** – How long a nameserver should wait prior to considering data from a secondary zone invalid and stop answering queries for that zone, in seconds. Only applies to zones using secondary DNS.
- **Minimum TTL** – Minimum Time To Live (TTL). How long a nameserver or resolver should cache a negative response, in seconds.

Anatomy of a Record Within a Zone File

A zone file is a collection of resource records with each record entry described in the following sequence:

<table>
<thead>
<tr>
<th>Format:</th>
<th>Host Label</th>
<th>TTL</th>
<th>Record Class</th>
<th>Record Type</th>
<th>Record Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>example.com.</td>
<td>60</td>
<td>IN</td>
<td>A</td>
<td>104.255.228.125</td>
</tr>
</tbody>
</table>

- **Host Label** – A host label helps to define the hostname of a record and whether the $ORIGIN hostname will be appended to the label. Fully qualified hostnames terminated by a period will not append the origin.
- **TTL** – The Time To Live (TTL) is the amount of time that a DNS record will be cached by an outside DNS server or resolver, in seconds.
- **Record Class** – There are three classes of DNS records: IN (Internet), CH (Chaosnet), and HS (Hesiod). Oracle Cloud Infrastructure DNS only uses the IN class of records.
• **Record Type** – The type of a record, such as CNAME, AAAA, or TXT.
• **Record Data** – The data within a DNS answer, such as an IP address, hostname, or other information. Different record types will contain different types of record data.

**Amending Zone Files Exported from GoDaddy.com for Import**

GoDaddy.com exports zone files in a proprietary format. To get the Oracle Cloud Infrastructure DNS service to correctly import a zone file exported from GoDaddy.com, you must directly alter the file. Follow these instructions to update the zone file.

1. Export your zone file from GoDaddy.com. Reference GoDaddy.com's documentation to see how this is done.
2. Open the file in your preferred text editor.
3. Prepend a new line to the file before the SOA record with the following information, including the trailing period: $ORIGIN [yourdomain].
4. Once the file has been amended, save the changes to the file and use the zone import function to import the file into your DNS configuration. For more information about zone import, see Managing DNS Zones.

**Note:**

If your zone file includes dynamic A records, such as @ 600 IN A GoCentral Published Site, you will need to amend these records with the correct IP addresses of your website. Please contact GoDaddy.com for information about how to obtain this information. Example: @ 600 IN A 192.0.2.255

**Example:**

This is an example of a zone file exported from GoDaddy.com. The code in bold is the code that needs to be removed from the file for it to be eligible for import into Oracle Cloud Infrastructure DNS.

**Tip:**

Placing a semi-colon at the beginning of a line is valid comment syntax for a zone file, per RFC 1035, but for ease of use and formatting it is recommended to remove the large section of comments from the beginning of the zone file provided by GoDaddy.com, as shown below.

```plaintext
Domain: example.com
; Exported (y-m-d hh:mm:ss): 2019-01-10 13:05:04
;
; This file is intended for use for informational and archival purposes ONLY and MUST be edited before use on a production DNS server.
;
; In particular, you must update the SOA record with the correct authoritative name server and contact e-mail address information, and add the correct NS records for the name servers which will be authoritative for this domain.
;
; For further information, please consult the BIND documentation located on the following website:
;
; http://www.isc.org/
;
; And RFC 1035:
;
; http://www.ietf.org/rfc/rfc1035.txt
;
; Please note that we do NOT offer technical support for any use of this zone data, the BIND name server, or any other third-party DNS software.
;```
Below is an example of an amended zone file ready to import into Oracle Cloud Infrastructure DNS. The code in bold needs to be prepended to your zone file before import.

$ORIGIN example.com.
example.com. 3600 IN SOA ns41.domaincontrol.com. dns.net. ( 2018122702 28800 7200 604800 3600 )

; A Records
@    600  IN     A   192.0.2.249
blog 10800 IN A 192.0.2.255
dev 1800 IN A 192.0.2.254
dev01 1800 IN A 192.0.2.253
dev02 1800 IN A 192.0.2.252
dev03 1800 IN A 192.0.2.251
dev04 1800 IN A 192.0.2.250

; CNAME Records
abc123b432dc7785b7ef31f04f25c3e71 1800 IN CNAME verify.bing.com.
akamai  600   IN     CNAME   www.example.com.edgekey.net.
email   3600 IN CNAME email.secureserver.net.

; MX Records
@     604800 IN MX 10 amlxe.l.google.com.
@     604800 IN MX 10 aplxe.l.google.com.

; TXT Records
@     3600 IN TXT "google-site-verification=3J82-80dbMyCo5Q5C1G11JszeOnZPGCSY1HcPcXg"

Below is an example of an amended zone file ready to import into Oracle Cloud Infrastructure DNS. The code in bold needs to be prepended to your zone file before import.
Managing HTTP Redirects

The HTTP Redirect service allows you to redirect HTTP traffic to another URL. You can use HTTP Redirect to:

- Redirect all HTTP traffic for an entire zone to another zone. For example, if a company owns example.net and example.com, HTTP Redirect lets the company redirect all HTTP traffic for example.net to example.com. This is a one-to-one mapping; wildcards are not supported.
- Redirect a specific subdomain to an HTTP URL. For example, test.example.com can be redirected to http://example.net/test/test.php.
- Redirect a subdomain to a URL with a port number. For example, camera.example.com can be redirected to http://office.example.com:8080 so a user can view their camera system without typing in the port number each time.
- Permanently redirect a domain name that has been deprecated by displaying a 301 response code. Permanently redirecting a domain name informs search engines and browsers what to do with the information.

Required IAM Policies

To work with HTTP Redirects, you need to have a user login to the Console, and your user needs sufficient authority (by way of an IAM policy) to perform all the instructions that follow. If your user is in the Administrators group, you have the required authority.

If your user is not, then a policy like this would allow a specific group to manage HTTP Redirects:

```
Allow group <GroupName> to manage http-redirects in compartment <CompartmentName>
```

If you're new to policies, see Getting Started with Policies and Common Policies. For more details about policies for HTTP Redirect, see Details for the WAF Service on page 2353.

Using the Console

To create an HTTP redirect

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click HTTP Redirects.
2. Select a zone.
3. Click Create HTTP Redirect.
4. In the Create Redirect dialog box, enter the following information:
   - **Name:** (Optional) Enter the name of the redirect zone you want to create. Avoid entering confidential information.
   - **Select a Zone:** (Optional) Select a zone from a list of configured zones. If the Create DNS Record check box is selected, the zone will be used to build an alias record for the redirect.
   - **Domain:** Enter the domain name from which traffic is redirected.
   - **Target -** Enter the following information for the endpoint where the traffic will be redirected:
     - **Protocol:** The network protocol used to interact with the target.
     - **Host:** The hostname of the target.
     - **Port:** (Optional) The port used to connect to the endpoint. The default is 80 for HTTP and 443 for HTTPS.
     - **Path:** (Optional) The specific path on the target for the redirect. A value of `{path}` will copy the path from the incoming request.
     - **Query:** (Optional) The query component of the target URL (for example, "?redirected" in "https://target.example.com/path/to/resource?redirected"). Use of the "\" character is not permitted except to escape a following "\", "{", or "}". An empty value results in a redirection target URL with no query component. A static value must begin with a leading ", optionally followed by other query characters. A request-
copying value must exactly match "(query)", and will be replaced with the query component of the request URL (including a leading "?" if the request URL includes a query component).

- **Response Code**: The response code that is returned with the redirect. If your website was permanently moved to the redirection URL and you want it to be indexed by search engines, select **301 - Moved Permanently**. If you want to indicate that the URL has been temporarily changed to a different address, select **302 - Found**.

- **Create DNS Record**: Select this check box to create an associated ALIAS record for the redirect in the specified zone. If a record for the zone specified already exists, the DNS record will not be created.

- **ALIAS TTL in Seconds** - The Time to Live for the ALIAS record before a new ALIAS record is retrieved. The default value is 300.

- **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Create**. The redirect zone is added to the redirects list.

**To edit an HTTP redirect**

1. Open the navigation menu. Under **Core Infrastructure**, go to Networking, DNS Management, and click **HTTP Redirects**.
2. Click the name of a redirect zone.
3. Click **Edit**.
4. In the Edit Redirect dialog box, make the needed changes and then click **Save Changes**.

**To delete an HTTP redirect**

1. Open the navigation menu. Under **Core Infrastructure**, go to Networking, DNS Management, and click **HTTP Redirects**.
2. Select a redirect zone.
3. Click **Delete**.
4. In the Delete Resource dialog box, click **Delete HTTP Redirect**. Any attached records will need to be managed in DNS Zone Management.

**To move an HTTP redirect to another compartment**

1. Open the navigation menu. Under **Core Infrastructure**, go to Networking, DNS Management, and click **HTTP Redirects**.
2. Click the name of a redirect zone.
3. Click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**Using the API**

Use the following operations to manage your HTTP redirect zones:

- **GetHttpRedirect**
- **ListHttpRedirects**
- **CreateHttpRedirect**
- **UpdateHttpRedirect**
- **DeleteHttpRedirect**
- **ChangeHttpRedirectCompartment**

**Managing TSIG Keys**

TSIG (Transaction Signature), also referred to as Secret Key Transaction Authentication, ensures that DNS packets originate from an authorized sender by using shared secret keys and one-way hashing to add a cryptographic signature to the DNS packets. TSIG keys are used to enable DNS to authenticate updates to secondary zones. TSIG keys provide an added layer of security for IXFR and AXFR transactions. A TSIG key consists of a key name, a
signing algorithm, and a secret. See RFC 2845 for more information. TSIG keys can also be managed in DNS Zone Management. See Managing DNS Service Zones on page 1679 for more information.

**Using the Console**

*To create a TSIG key*

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click TSIG Keys.
2. Click Create TSIG key.
3. In the Create TSIG Key dialog box, enter the following:
   - **Name:** The name of the key used in domain name syntax. The name should reflect the names of the hosts and uniquely identify the key among a set of keys these two hosts may share at any given time.
   - **Algorithm:** Select the public key's algorithm used to encrypt or decrypt data. Applicable algorithms include hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-h384, and hmac-sha512.
   - **Secret:** The base64 string encoding the binary shared secret that corresponds to the key. A maximum value of 255 characters is allowed.
   - **Tags:** Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
4. Click Create TSIG Key. The TSIG key details appear.

*To view the details of a TSIG key*

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click TSIG Keys.
2. Click the name of the TSIG key you want to view. TSIG key details and a list of associated zones appear.
3. To view the Secret assigned to the key, click Show beside the Secret field.
4. In the View Secret dialog box, click Close.

*To delete a TSIG key*

1. **Note:** A TSIG key attached to a zone must be removed from the zone in DNS Zone Management. See Managing DNS Service Zones on page 1679 for more information.

*To move a TSIG key to another compartment*

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click TSIG Keys.
2. Find the TSIG key in the list, click the Actions icon (three dots), and then click Delete.
3. In the confirmation dialog box, click Delete.

*Using the API*

Use the following operations to manage TSIG keys:

- ListTsigKeys
- CreateTsigKey
DNS and Traffic Management

- GetTsigKey
- UpdateTsigKey
- DeleteTsigKey
- ChangeTsigKeyCompartment

**Testing DNS Using BIND’S dig Tool**

Using the Domain Information Groper (dig) command line tool, you can test against the delegation where your domain is hosted, and you will immediately see whether the change took place without accounting for the cache or TTL (Time to Live) that you have configured.

![Note:]

Windows users can download the tool from BIND’s [website](#). Use Terminal to access dig on Linux and Macintosh systems.

**Using dig**

Before using BIND’s dig tool, you must access or install dig on your system. Once you have access to dig, you can use dig to test your DNS.

*To access dig (Mac)*

1. From your Applications folder, open the Utilities folder, and then select **Terminal**.
2. When Terminal is open, type a dig command using a hostname you want to look up.

*To install dig (Windows)*

1. Go to [BIND’s website](#) and download the most current, stable version of BIND.

![Note:]

BIND supports both 32 and 64 bit Windows systems. Confirm which version of Windows you are using and download the correct version of BIND. View Microsoft’s [documentation](#) to determine which version of Windows you are using.

2. Extract the downloaded file and install BIND in the following directory: C:\Program Files\ISC BIND 9. Select the **Tools Only** check box.
3. Once BIND is installed, on the Windows menu open the Control Panel, and then open your System properties.
4. On the **Advanced** tab, click **Environment Variables**.
5. Under **System Variables**, select **Path**, and then click **Edit**.
6. At the end of the path in the Edit System Variable window, add C:\Program Files\ISC BIND 9\bin, and then click **OK**.
7. In the Edit Variables window, click **OK**. In the System properties window, click **OK**.

*To open the Command Prompt*

For Windows versions 8 -10:

1. Click the Windows menu icon.
2. In the **Search** field, type **CMD**.
3. Click **Command Prompt**.

For Windows version 7:

1. On the **Start** menu click **Run**.
2. Enter **CMD**, and then click **OK**.

*To use dig to test your DNS*

1. Open Terminal (Mac and Linux) or Command Prompt (Windows).
2. Type `dig <any hostname>`, and then press **Enter**.
The following information is returned:

```
$ dig oracle.com
+-------------------+---------------------------+
| Command            | Description               | Example                  |
+-------------------+---------------------------+--------------------------|
| dig [hostname]    | Returns any A record found within the queried hostname's zone. | dig oracle.com            |
|                   |                           |                          |
| dig [hostname] [record type] | Returns the records of that type found within the queried hostname's zone. | dig oracle.com MX         |
|                   |                           |                          |
| dig [hostname] +short | Provides a brief answer, usually just an IP address. | dig oracle.com +short     |
|                   |                           |                          |
| dig @[nameserver address] [hostname] | Queries the nameserver directly instead of your ISP's resolver. | dig @dnsmaster6.oracle.com |
+-------------------+---------------------------+--------------------------+
```

- **Question section**: The query made to the DNS. In this example, we asked for the first available A record for the hostname, oracle.com.
- **Answer section**: The first available answer for the query made to the DNS. In this example, we received the A record for the IP address 137.254.16.101.
- **Authority section**: The authoritative nameservers from which the answer to the query was received. These nameservers house the zones for a domain.
- **Additional section**: Additional information the resolver may need but not the answer to the query.
### DNS and Traffic Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dig [hostname] +trace</code></td>
<td>Adding <code>+trace</code> instructs <code>dig</code> to resolve the query from the root nameserver downwards and to report the results from each query step.</td>
<td><code>dig dyn.com +trace</code></td>
</tr>
<tr>
<td><code>dig -X [IP address]</code></td>
<td>Reverse lookup for IP addresses.</td>
<td><code>dig -X 137.254.16.101</code></td>
</tr>
<tr>
<td><code>dig [hostname] any</code></td>
<td>Returns all records for a hostname.</td>
<td><code>dig oracle.com any</code></td>
</tr>
</tbody>
</table>

### Private DNS

This topic describes how to create and manage private DNS zones. Private DNS allows you to use your own private DNS domain names and fully manage the associated zones and records to provide hostname resolution for your applications running within and between VCNs, as well as your on-premises or other private network. Private DNS also provides DNS resolution across networks (for example, another VCN within the same region, cross region, or external network). Private DNS can be managed in the OCI DNS API and Console.

**Overview of Private DNS**

- **Private DNS Zones**: Private DNS zones contain DNS data only accessible from within a VCN, such as private IP addresses. A private DNS zone has similar capabilities to an internet DNS zone, but provides responses only for clients that can reach it through a VCN. Private DNS allows you to duplicate zones across multiple VCNs. A full or partial domain tree can be created. It also supports split-horizon DNS which allows you to use the same domain name for public and private zones. Different answers can be served for public queries versus private queries from within your VCN.

- **Private DNS Views**: A private DNS view is a collection of private zones. You can reference private views from a resolver to manage how DNS queries are answered. A zone can only belong to a single view. The same zone name can be used in multiple views, but the zones will have unique OCIDs to differentiate. You can use those views to create DNS resolvers configured to handle DNS queries from your VCNs. Any given view can be used by an arbitrary number of resolvers, allowing you to share private DNS data across VCNs.

- **Private DNS Resolver**: A private DNS resolver provides responses to DNS queries. It provides responses by checking each customer-referenced view in order, then the default view, then each rule in order, and finally by using internet DNS. The first item in that sequence able to provide an answer does so, and later items are not checked. Rules allow you to define the logic for how queries should be answered. The resolver listens on 169.254.169.254 by default, but also allows you to define endpoints for listening for queries and forwarding them to other resolvers in other VCNs, a customer's on-premises network, or other private network. Multiple views can be resolved within a VCN. You can specify an ordered list of views within a resolver. For more information, see [Private DNS resolvers](#)

**Required IAM Policies**

To work with private DNS, a user needs sufficient authority (by way of an IAM policy). If your user is in the Administrators group, you have the required authority. If your user is not in the Administrators group, then a policy like this will allow a specific group to manage private DNS:

```text
Allow group <GroupName> to manage dns in tenancy where target.dns.scope = 'private'
```

If you're new to policies, see [Getting Started with Policies](#) and [Common Policies](#). For more details about policies for private DNS, see [Details for the DNS Service](#) on page 2262.

**Using the Console**

To create a private zone with a private view

**Note:**

- Private zones can only be viewed in the region in which they are created.
1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the **Private Zones** tab.
3. Click **Create Zone**.
4. In the Create Private Zone dialog box, enter the following information:
   - **Zone Name**: Enter the name of the zone you want to create. Avoid entering confidential information. A domain name identifies a particular space within a zone for the purposes of naming systems and/or associating DNS records.
   - **Create in Compartment**: Select the compartment where you want to create the zone.
   - **Zone Type**: This field is read-only. The zone contents will be controlled directly within Oracle Cloud Infrastructure.
   - **DNS Private View**: A private zone must be created within a private view, which cannot be changed. When a private zone is attached to a private view, the private zone cannot be moved to a new private view.
     - **Select Existing Private DNS View**: To select an existing private view in the current compartment, select a private view from the drop-down menu. You can click **Change Compartment** to change the compartment where the private view exists.
     - **Create New Private DNS View**: Enter a name for the private view. Avoid entering confidential information. This resource is created in the compartment selected previously.
   - **Tags**: Optionally, you can apply tags. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click **Create**.

The system creates and publishes the zone, complete with the necessary SOA and NS records. The details for the zone appear. You can view the private view associated with this zone by clicking the Private View name in the Zone Information section. For information on adding a record to your zone, see **To add a zone record** on page 1680.

### To create a private view

**Note:** Private views can only be viewed in the region in which they are created.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Private Views**.
2. Click **Create Private View**.
3. In the Create Private View dialog box, enter the following:
   - **Name**: Enter the name of the private view you want to create. Avoid entering confidential information.
   - **Create in Compartment**: Select the compartment where you want to create the private view.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
4. Click **Create**.

### To create a private view with a new private zone

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Private Views**.
2. Click **Create Private View**.
3. In the Create Private Zone dialog box, enter the following information:
   • **Name**: Enter the name of the private view you want to create. Avoid entering confidential information.
   • **Create in Compartment**: Select the compartment where you want to create the private view.
   • **Tags**: Optionally, you can apply tags. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

4. Click **Create**.
   The details for the private view appear.

5. Click **Create Zone**.

6. In the Create Private Zone dialog box, enter the following:
   • **Zone Name**: Enter the name of the zone you want to create. Avoid entering confidential information. A domain name identifies a particular space within a zone for the purposes of naming systems and/or associating DNS records.
   • **Create in Compartment**: Select the compartment where you want to create the zone.
   • **Zone Type**: This field is read-only. The zone contents will be controlled directly within Oracle Cloud Infrastructure.
   • **Tags**: Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

7. Click **Create**.
   The new zone appears in the zone list associated with the private view you created.

To add a zone record

Tip:
There are many record types you can add to your zone, depending on your goals for the zone and its DNS management.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Zones**.
2. Click the **Zone Name** in which you want to add a record. If you are adding a record to a private zone, click the **Private Zones** tab and then click the zone name. Zone details and a list of records appear.

   Tip:
   To locate zones in the Private Zones tab, you can use filters to sort by zones that are protected (system generated) or by associated private view names.

3. Click **Add Record**.
4. In the **Add Record** dialog box, select a record type from the drop-down list, and then enter the information for the record. Avoid entering confidential information. For more information about record types, see Supported Resource Records on page 1686.
5. (Optional) Click the **Add Another Record** check box to add multiple records in succession.
6. Click **Submit**.

   Note:
   When records are added, they are staged to allow for multiple records to be combined into a set. Before records take effect, they must be published.

7. Once your records have been added, click **Publish Changes**.
8. In the confirmation dialog box, click **Publish Changes**.
To update a zone record

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Records</td>
</tr>
</tbody>
</table>

You can change various components of the records within your zones, such as time-to-live (TTL) and relevant RDATA. However, some records contain information that cannot be changed. You can attempt changes to such records through the Actions menu, but the system might not permit updates to some fields.

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Zone Name in which you want to update a record. If you are updating a record in a private zone, click the Private Zones tab and then click the zone name. Zone details and a list of records appear.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To locate zones in the Private Zones tab, you can use filters to sort by zones that are protected (system generated) or by associated private view names.</td>
</tr>
</tbody>
</table>

3. To help find a record, you can use the following filter options:
   - Enter the name of the record's domain in the Search field.
   - To find unpublished records, select the Staged check box.
   - To find published records, select the Unstaged check box.
   - Use the Is Protected sort filter to sort by records that are protected.
   - Use the Record Type sort filter to sort records.
4. Select the check box for the record you want to update, and select Edit from the Actions drop-down menu.
5. In the Edit Record dialog box, make the needed changes, and then click Submit.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When records are added, they are staged to allow for multiple records to be combined into a set. Before records take effect, they must be published.</td>
</tr>
</tbody>
</table>

6. Click Publish Changes.
7. In the confirmation dialog box, click Publish Changes.

Reverting Changes Before Publishing

You can revert records to their current published state before you publish changes. Once a record has been published, it cannot be reverted. Select the check box for the record you want to revert, and then select Revert from the Actions drop-down menu.

To delete a zone record

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Zone Name in which you want to delete a record. If you are deleting a record in a private zone, click the Private Zones tab and then click the zone name. Zone details and a list of records appear.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To locate zones in the Private Zones tab, you can use filters to sort by zones that are protected (system generated) or by associated private view names.</td>
</tr>
</tbody>
</table>

3. Select the check box for the record you want to delete, and then select Delete from the Actions drop-down menu.
4. Click Publish Changes.
5. In the confirmation dialog box, click Publish Changes.
To edit a private view

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Private Views.
2. Click the name of the private view you want to update.
   
   **Tip:**
   You can use the Protected filter to sort private views by views that are protected (system generated).
3. Click Edit.
4. In the Edit Private DNS View dialog box, make the needed changes and then click Save Changes.

To edit a private zone

**Note:**
Private zones are only viewable in the region they are created.

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Private Zones tab.
3. Click the name of the zone you want to update.
   
   **Tip:**
   You can use filters to sort private zones by zones that are protected (system generated) or by associated private view names.
4. Click Edit.
5. In the Edit Zone dialog box, make the needed changes and then click Save Changes.

To delete a private zone

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Private Zones tab.
3. Click the Actions icon (three dots) for the zone you want to delete, and then click Delete.
4. In the Delete Private Zone dialog box, click Delete.
   
   **Caution:**
   Deletion removes associated resources.

To delete a private view

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Private Views.
2. Click the name of the private view that you want to delete.
3. Click Delete.
4. In the Delete DNS Private View dialog box, click Delete.
   
   **Caution:**
   Deletion removes any associated private zones.

To delete a private zone from a private view

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Private Views.
2. Click the private view that contains the zone you want to delete.
3. Click the the Actions icon (three dots) for the zone you want to delete, and then click Delete.
4. In the Delete Private Zone dialog box, click Delete.
To move a private zone to another compartment

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
2. Click the Private Zones tab.
3. Click the name of the zone you want to move.
4. Find the zone in the list, click the the Actions icon (three dots), and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To move a private view to another compartment

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Private Views.
2. Click the name of the view you want to move.
3. Click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.

To create a VCN with a dedicated DNS resolver

See To create a VCN on page 2825 and DNS in Your Virtual Cloud Network on page 2910 for more information.

Using the API

Use the following operations to manage private zones and records:

- ChangeZoneCompartment
- CreateZone
- DeleteZone
- GetZone
- ListZones
- UpdateZone
- DeleteDomainRecords
- GetDomainRecords
- PatchDomainRecords
- UpdateDomainRecords
- GetZoneRecords
- PatchZoneRecords (add or delete records)
- UpdateZoneRecords
- DeleteRRSet
- GetRRSet
- PatchRRSet
- UpdateRRSet

Use the following operations to manage private views:

- ChangeViewCompartment
- CreateView
- DeleteView
- GetView
- ListViews
- UpdateView

Use the following operations to manage resolvers and resolver endpoints:

- ChangeResolverCompartment
- GetResolver
- ListResolvers
• UpdateResolver
• CreateResolverEndpoint
• DeleteResolverEndpoint
• GetResolverEndpoint
• ListResolverEndpoints
• UpdateResolverEndpoint

Troubleshooting
This topic covers some common Private DNS issues and how to address them.

Querying for a private zone after creation returns an NXDOMAIN error message or Public IP address
• If a query is sent before the private zone is published, the query recurses to the internet. An error message stating that the domain doesn’t exist or a public name response will be returned for the query.
• Wait until the Time To Live (TTL) expires before querying.

Network connectivity issues when configuring DNS resolution between VCNs or between a VCN and your on-premises network
• Ensure that the local peering gateway is set up correctly between VCNs, and the remote peering connection, IPSec tunnel, or FastConnect network connectivity is set up correctly between resolvers.
• Ensure that DHCP is enabled as a protocol over the local peering gateway, remote peering connection, FastConnect or VPN and that the IP addresses of the endpoints are allowed. For more information, see DHCP Options on page 2917.

DNS Metrics
You can monitor the health, capacity, and performance of your DNS services by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace oci_dns (the DNS service).

Overview of DNS Service Metrics
The DNS service metrics help you measure the number of queries for DNS zones and DNS zones with traffic management policies attached.

Prerequisites
• IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_dns
The metrics listed in the following table are automatically available. You do not need to enable monitoring on the resource to get these metrics.

Each metric includes the following dimensions:

RESOURCEID
The OCID of the zone to which the metric applies.
**Using the Console**

DNS service metrics are available using the Metrics Explorer feature in the Console. For more information about metrics, see Viewing Metric Charts.

*To view DNS metric charts*

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. For Metric Namespace, select oci_dns.
3. Select a metric to view from the Metric Name field.
4. Select a qualifier specified in the Dimension Name field. For example, the dimension resourceId is specified in the metric definition for DNSQueryCount.
5. Select the value you want to use for the specified dimension in the Dimension Value field. For example, the resource identifier for your instance of interest.
6. Click Update Chart.

The chart will be updated with the metrics that have been requested.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**Using the API**

Use the following APIs for monitoring:
- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

**Overview of the Traffic Management Steering Policies Service**

The Oracle Cloud Infrastructure Traffic Management Steering Policies service is a critical component of DNS. Traffic Management Steering Policies enables you to configure policies to serve intelligent responses to DNS queries, meaning different answers (endpoints) may be served for the query depending on the logic the customer defines in the policy. Traffic Management Steering Policies can account for health of answers to provide failover capabilities, provide the ability to load balance traffic across multiple resources, and account for the location where the query was initiated to provide a simple, flexible and powerful mechanism to efficiently steer DNS traffic.

**Traffic Management Steering Policies Service Components**

The following list describes the components used to build a traffic management steering policy.

STEERING POLICIES

A framework to define the traffic management behavior for your zones. Steering policies contain rules that help to intelligently serve DNS answers.

ATTACHMENTS

Allows you to link a steering policy to your zones. An attachment of a steering policy to a zone occludes all records at its domain that are of a covered record type, constructing DNS responses from its steering policy rather than from those domain's records. A domain can have at most one attachment covering any given record type.
DNS and Traffic Management

RULES

The guidelines steering policies use to filter answers based on the properties of a DNS request, such as the requests geo-location or the health of your endpoints.

ANSWERS

Answers contain the DNS record data and metadata to be processed in a steering policy.

Ways to Access the Traffic Management Steering Policies Service

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide.

To access the Console, you must use a supported browser. You can use the Console link at the top of this page to go to the sign-in page. Enter your tenancy, user name, and your password.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Traffic Management Steering Policies Service Capabilities and Limits

The Oracle Cloud Infrastructure Traffic Management Steering Policies service is limited to 100 policies and 1,000 attachments per tenant. See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies. For more details about policies for Traffic Management Steering Policies, see Details for the Traffic Management Steering Policies Service.

Managing Traffic Management Steering Policies

Policy Types

FAILOVER

Failover policies allow you to prioritize the order in which you want answers served in a policy (for example, Primary and Secondary). Oracle Cloud Infrastructure Health Checks are leveraged to determine the health of answers in the policy. If the Primary Answer is determined to be unhealthy, DNS traffic will automatically be steered to the Secondary Answer.
LOAD BALANCER
Load Balancer policies allow distribution of traffic across multiple endpoints. Endpoints can be assigned equal weights to distribute traffic evenly across the endpoints or custom weights may be assigned for ratio load balancing. Oracle Cloud Infrastructure Health Checks are leveraged to determine the health of the endpoint. DNS traffic will be automatically distributed to the other endpoints, if an endpoint is determined to be unhealthy.

GEOLOCATION STEERING
Geolocation steering policies distribute DNS traffic to different endpoints based on the location of the end user. Customers can define geographic regions composed of originating continent, countries or states/provinces (North America) and define a separate endpoint or set of endpoints for each region.

ASN STEERING
ASN steering policies enable you to steer DNS traffic based on Autonomous System Numbers (ASN). DNS queries originating from a specific ASN or set of ASNs can be steered to a specified endpoint.

IP PREFIX STEERING
IP Prefix steering policies enable customers to steer DNS traffic based on the IP Prefix of the originating query.

Typical Traffic Steering Scenarios
This section describes several typical scenarios for using Traffic Management Steering Policies.

Basic Failover
You can leverage Traffic Management Steering Policies to provide automated failover between primary and secondary servers.

Cloud Migration
Weighted load balancing supports controlled migration from your data center to Oracle Cloud Infrastructure servers. You can steer a small amount of traffic (1%) to your new resources in the cloud to verify everything is working as expected. You can then increase the ratios until you are comfortable with fully migrating all DNS traffic to the cloud.

Load Balancing Across Multiple Servers for Scale
You can configure load balancing pools of multiple servers. Traffic Management Steering Policies can automatically distribute DNS traffic across the set of servers. Health Checks may also be used and traffic will be automatically redirected to healthy servers, if a server is determined to be unhealthy.

Hybrid Environments
Since Traffic Management Steering Policies is an agnostic service, it may be used to not only steer traffic to Oracle Cloud Infrastructure resources, but can also be used to steer traffic to any publicly exposed (internet resolvable) resources, including other cloud providers and enterprise data centers.

Worldwide Geolocation Treatment
You can divide your global users into geographically defined regions (for example, state/province level in NA, country level for rest of world) and steer customers to specified resources based on their location. This helps to ensure global, high performing internet resolution, and supports functions such as ring fencing. For example, keeping traffic from China in China and block traffic outside of China into China.

Canary Testing
Leveraging IP Prefix steering, you can configure policies to serve different responses for your internal users versus external users.
**Zero-Rating Services**

ASN steering conditional steering based on the originating enterprise, mobile operator or other communications provider in support of various commercial agreements that may be in place. Essentially, preferred ASNs can be directed to free resources, while all other traffic can be directed to paid resources.

**Using the Console**

**Managing Traffic Management Steering Policies**

*To create a Load Balancer policy*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click **Create Traffic Management Steering Policy**.
3. In the **Create Traffic Management Steering Policy** dialog box, select **Load Balancer**.
4. Enter the following information:
   - **Policy Name**: The unique name that identifies policy.
   - **Policy TTL**: The Time to Live for responses from the steering policy. If not specified, the system will set this value on the steering policy.
   - **Maximum Answer Count**: The maximum number of answers returned for the policy.
   - **Answer(s)**: Answer pools contain the group of answers that will be served in response to DNS queries.
     - **Name**: A unique name to identify the answer. Avoid entering confidential information.
     - **Type**: The record type that will be provided as the answer.
     - **RDATA**: A valid domain name or IP address to add as an answer.
     - **Weight**: A number between 0 and 255 used to determine how often an answer is served in relation to other answers. Answers with higher values are more likely to be served.
     - **Eligible**: Select the check box to indicate that the answer is available within the pool to be used in response to queries. Alternatively, select **Mark pool answers eligible** or **Mark pool answers ineligible** from the **Actions** drop-down menu.
   - **Attach Health Check**: Select an existing Health Check to be included as part of the policy, add a new one, or select **None**.
   - **Attach Domain(s)**: (Optional) The domain name and domain OCID you want to attach to the policy. Additional domains can be added in this section.
5. Click **Create Policy**.

The system creates and publishes the policy.

*To create a Failover policy*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click **Create Traffic Management Steering Policy**.
3. In the **Create Traffic Management Steering Policy** dialog box, select **Failover**.
4. Enter the following information:
   - **Policy Name**: The unique name that identifies policy. Avoid entering confidential information.
   - **Policy TTL**: The Time to Live for responses from the steering policy. If not specified, the system will set this value on the steering policy.
   - **Maximum Answer Count**: The maximum number of answers returned for the policy. For priority-based policies, the first valid answer is returned.
   - **Answer Pool(s)**: Answer pools contain the group of answers that will be served in response to DNS queries.
     - **Answer Pool Name**: A user-friendly name for the answer pool, unique within the steering policy. Avoid entering confidential information.
     - **Name**: A unique name to identify the answer. Avoid entering confidential information.
     - **Type**: The record type that will be provided as the answer.
     - **RDATA**: A valid domain name or IP address to add as an answer.
     - **Weight**: A number between 0 and 255 used to determine how often an answer is served in relation to other answers. Answers with higher values are more likely to be served.
     - **Eligible**: Select the check box to indicate that the answer is available within the pool to be used in response to queries. Alternatively, select Mark pool answers eligible or Mark pool answers ineligible from the Actions drop-down menu.
     - **Pool Priority**: Failover priority rules specify the priority of answers that are served in a policy. If the primary answer is unavailable, traffic is steered to the next answer in the list.
     - **Pool**: Select the priority in which the answers are served.
   - **Attach Health Check**: Select an existing Health Check to be included as part of the policy, add a new one, or select None.
   - **Attach Domain(s)**: The domain name and domain OCID you want to attach to the policy. Additional domains can be added in this section.

5. Click **Create Policy**.

The system creates and publishes the policy.

*To create a Geolocation Steering policy*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click **Create Traffic Management Steering Policy**.
3. In the **Create Traffic Management Steering Policy** dialog box, select **Geolocation Steering**.
4. Enter the following information:
   - **Policy Name**: The unique name that identifies policy. Avoid entering confidential information.
   - **Policy TTL**: The Time to Live for responses from the steering policy. If not specified, the system will set this value on the steering policy.
   - **Maximum Answer Count**: The maximum number of answers returned for the policy. For priority-based policies, the first valid answer is returned.
   - **Answer Pool(s)**: Answer pools contain the group of answers that will be served in response to DNS queries.
     - **Answer Pool Name**: A user-friendly name for the answer pool, unique within the steering policy. Avoid entering confidential information.
     - **Name**: A unique name to identify the answer. Avoid entering confidential information.
     - **Type**: The record type that will be provided as the answer.
     - **RDATA**: A valid domain name or IP address to add as an answer.
     - **Eligible**: Select the check box to indicate that the answer is available within the pool to be used in response to queries. Alternatively, select **Mark pool answers eligible** or **Mark pool answers ineligible** from the Actions drop-down menu.
   - **Geolocation Steering Rules**: Geolocation steering rules specify the priority of answers that are served in a policy. If the primary answer is unavailable, traffic is steered to the next answer in the list. Additional rules and priorities can be added in this section.
     - **Geolocation**: Select a location that will be used to distribute DNS traffic.
     - **Pool Priority**: Select the priority in which the answers are served.
     - **Global Catch-all**: Adding a global catch-all allows you to specify answer pools for queries that do not match any of the specified rules you have added. Click **Add Global Catch-all** and select the pool priorities.
   - **Attach Health Check**: Select an existing Health Check to be included as part of the policy, add a new one, or select **None**.
   - **Attach Domain(s)**: The domain name and domain OCID you want to attach to the policy. Additional domains can be added in this section.

5. Click **Create Policy**.

The system creates and publishes the policy.

*To create an ASN Steering policy*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click **Create Traffic Management Steering Policy**.
3. In the **Create Traffic Management Steering Policy** dialog box, select **ASN Steering**.
4. Enter the following information:
   - **Policy Name**: The unique name that identifies policy. Avoid entering confidential information.
   - **Policy TTL**: The Time to Live for responses from the steering policy. If not specified, the system will set this value on the steering policy.
   - **Maximum Answer Count**: The maximum number of answers returned for the policy. For priority-based policies, the first valid answer is returned.
   - **Answer Pool(s)**: Answer pools contain the group of answers that will be served in response to DNS queries.
     - **Answer Pool Name**: A user-friendly name for the answer pool, unique within the steering policy. Avoid entering confidential information.
     - **Name**: A unique name to identify the answer. Avoid entering confidential information.
     - **Type**: The record type that will be provided as the answer.
     - **RDATA**: A valid domain name or IP address to add as an answer.
     - **Eligible**: Select the check box to indicate that the answer is available within the pool to be used in response to queries. Alternatively, select **Mark pool answers eligible** or **Mark pool answers ineligible** from the **Actions** drop-down menu.
   - **ASN Steering Rules**: ASN steering rules specify the priority of answers that are served in a policy. If the primary answer is unavailable, traffic is steered to the next answer in the list.
     - **ASN**: Enter an Autonomous System Number (ASN) that will be used to distribute DNS traffic.
     - **Pool Priority**: Select the priority in which the answers are served.
     - **Global Catch-all**: Adding a global catch-all allows you to specify answer pools for queries that do not match any of the specified rules you have added. Click **Add Global Catch-all** and select the pool priorities.
   - **Attach Health Check**: Select an existing Health Check to be included as part of the policy, add a new one, or select **None**.
   - **Attach Domain(s)**: The domain name and domain OCID you want to attach to the policy. Additional domains can be added in this section.

5. Click **Create Policy**.

The system creates and publishes the policy.

To create an IP Prefix Steering policy

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click **Create Traffic Management Steering Policy**.
3. In the **Create Traffic Management Steering Policy** dialog box, select **IP Prefix Steering**.
4. Enter the following information:
   - **Policy Name**: The unique name that identifies policy. Avoid entering confidential information.
   - **Policy TTL**: The Time to Live for responses from the steering policy. If not specified, the system will set this value on the steering policy.
   - **Maximum Answer Count**: The maximum number of answers returned for the policy. For priority-based policies, the first valid answer is returned.
   - **Answer Pool(s)**: Answer pools contain the group of answers that will be served in response to DNS queries.
     - **Answer Pool Name**: A user-friendly name for the answer pool, unique within the steering policy. Avoid entering confidential information.
     - **Name**: A unique name to identify the answer. Avoid entering confidential information.
     - **Type**: The record type that will be provided as the answer.
     - **RDATA**: A valid domain name or IP address to add as an answer.
     - **Eligible**: Select the check box to indicate that the answer is available within the pool to be used in response to queries. Alternatively, select **Mark pool answers eligible** or **Mark pool answers ineligible** from the **Actions** drop-down menu.
   - **IP Prefix Steering Rules**: IP prefix steering rules specify the priority of answers that are served in a policy. If the primary answer is unavailable, traffic is steered to the next answer in the list.
     - **Subnet Address**: Enter a subnet address that will be used to distribute DNS traffic.
     - **Pool Priority**: Select the priority in which the answers are served.
     - **Global Catch-all**: Adding a global catch-all allows you to specify answer pools for queries that do not match any of the specified rules you have added. Click **Add Global Catch-all** and select the pool priorities.
   - **Attach Health Check**: Select an existing Health Check to be included as part of the policy, add a new one, or select **None**.
   - **Attach Domain(s)**: The domain name and domain OCID you want to attach to the policy. Additional domains can be added in this section.

5. Click **Create Policy**.

The system creates and publishes the policy.

**To update a policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click the **Policy Name** you want to update. Policy information and a list of attached domains appear.

   **Tip:**
   You can use search for a policy by name in the **Search** field. You can also use the **Time Created** sort filter to sort the policies chronologically in ascending or descending order.

3. Click **Edit**.
4. Make the needed changes, and then click **Save**.

**To attach a domain to an existing policy**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking, DNS Management**, and click **Traffic Management Steering Policies**.
2. Click the **Policy Name** you want to update. Policy information and a list of attached domains appear.

   **Tip:**
   You can use search for a policy by name in the **Search** field. You can also use the **Time Created** sort filter to sort the policies chronologically in ascending or descending order.

3. Click **Add Attached Domain(s)**.
4. In the Add Attached Domain(s) dialog box, enter the domain and select a zone.
5. Click Submit.

To edit an attached domain

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Traffic Management Steering Policies.
2. Click the Policy Name you want to update. Policy information and a list of attached domains appear.

   Tip:
   You can use search for a policy by name in the Search field. You can also use the Time Created sort filter to sort the policies chronologically in ascending or descending order.

3. For the attached domain you want to edit, click the Actions icon (three dots), and then click Edit Attached Domain.
4. In the Attached Domain(s) dialog box, enter the domain and select a zone.
5. Click Save.

To delete a policy

1. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Traffic Management Steering Policies.
2. Select the check box for the policy you want to delete.
3. Click Delete. The policy is staged for deletion.
4. Click Publish Changes to delete the policy.
5. In the confirmation dialog box, click Publish Changes.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For more information about managing steering policies using the API, see Traffic Management Steering Policies API Guide.

Use the following operations to manage your steering policies:

- CreateSteeringPolicy
- ListSteeringPolicies
- GetSteeringPolicy
- UpdateSteeringPolicy
- DeleteSteeringPolicy

Use the following operations to manage your steering policy attachments:

- CreateSteeringPolicyAttachment
- ListSteeringPolicyAttachments
- GetSteeringPolicyAttachment
- UpdateSteeringPolicyAttachment
- DeleteSteeringPolicyAttachment

Traffic Management Steering Policies API Guide

Traffic Management Steering Policies allows you to build and configure traffic management policies using the Oracle Cloud Infrastructure DNS REST API. Use the following guide to learn how policies are constructed using the REST API.
**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Traffic Management Steering Policy Components**

The following list describes the components used to build a Traffic Management Steering Policy.

**STEERING POLICIES**

An overall framework to define the traffic management behavior for your zones. Steering policies contain rules that help to intelligently serve DNS answers.

**ATTACHMENTS**

Allows you to link a steering policy to your zones. An attachment of a steering policy to a zone occludes all records at its domain that are of a covered record type, constructing DNS responses from its steering policy rather than from those domain's records. A domain can have at most one attachment covering any given record type.

**RULES**

The guidelines steering policies use to filter answers based on the properties of a DNS request, such as the requests geo-location or the health of your endpoints.

**ANSWERS**

Answers contain the DNS record data and metadata to be processed in a steering policy.

**TEMPLATES**

Templates are predefined rule sequences that create a policy type and its intended behavior. Example: The FAILOVER template determines answers by checking DNS query against a FILTER rule first, then the following rules in succession: HEALTH, PRIORITY, and LIMIT. This gives the domain dynamic failover capability. Policies that define the template field with any policy other than CUSTOM, must follow the rule sequence outlined for that policy type, otherwise, a 400 status code error will be returned upon policy creation.

**CASES**

A rule may optionally include a sequence of cases defining alternate configurations for how it should behave during processing for any given DNS query. When a rule has no sequence of cases, it is always evaluated with the same configuration during processing. When a rule has an empty sequence of cases, it is always ignored during processing. When a rule has a non-empty sequence of cases, its behavior during processing is configured by the first matching case in the sequence. A rule case with no caseCondition always matches. A rule case with a caseCondition matches only when that expression evaluates to true for the given query.

**Create Steering Policies Using Templates**

The following section explains the rule configuration for each type of steering policy template followed by an example POST request (CreateSteeringPolicy) displaying how to configure each template.
FAILOVER

Failover policies allow you to prioritize the order in which you want answers served in a policy (for example, Primary and Secondary). Oracle Cloud Infrastructure Health Checks are leveraged to determine the health of answers in the policy. If the Primary Answer is determined to be unhealthy, DNS traffic will automatically be steered to the Secondary Answer. Each of the following rules must be defined in the order specified below in the rules field of your request body when using a FAILOVER template:

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule</th>
<th>Restrictions</th>
<th>Comments</th>
</tr>
</thead>
</table>
| 1     | FILTER | • No cases are allowed.  
• Answer data must be defined in defaultAnswerData using the following JSON:  

```json
{
   "answerCondition": "answer.isDisabled != true",
   "shouldKeep": true
}
```
| Only included if healthCheckMonitorId is defined for the policy. |
| 2     | HEALTH | • No cases are allowed. |
| 3     | PRIORITY | • No cases are allowed.  
• Answer data must be defined in the defaultAnswerData property for the rule.  
• Every answer must have a pool property.  
• defaultAnswerData restrictions:  
  • Answers cannot be referenced by their name property in answerCondition expressions, they must be referenced by their pool property.  
  • Every answer pool must be referenced once and only once.  
  • Every answer pool must have a unique value property.  
  • Each answer pool reference must match the pool property on one or more answers defined in the answer list for the policy. |
| 4     | LIMIT | • No cases are allowed. |

Example of a POST /steeringPolicies policy using the FAILOVER template:

```json
{
   "compartmentId": "ocid1...",
   "displayName": "failover between endpoints",
   "ttl": 30,
   "healthCheckMonitorId": "ocid1...",
   "template": "FAILOVER",
   "answers": [
      {
         "name": "server-primary",
         "rtype": "A",
         "rdata": "192.168.0.2",
         "pool": "primary"
      }
   ]
}
```
LOAD_BALANCE

Load Balancer policies allow distribution of traffic across multiple endpoints. Endpoints can be assigned equal weights to distribute traffic evenly across the endpoints or custom weights may be assigned for ratio load balancing. Oracle Cloud Infrastructure Health Checks are leveraged to determine the health of the endpoint. DNS traffic will be automatically distributed to the other endpoints, if an endpoint is determined to be unhealthy. Each of the following rules must be defined in the order specified below in the rules field of your request body when using a LOAD_BALANCE template:
<table>
<thead>
<tr>
<th>Order</th>
<th>Rule</th>
<th>Restrictions</th>
<th>Comments</th>
</tr>
</thead>
</table>
| 1     | FILTER   | • No cases are allowed.  
• Answer data must be defined in defaultAnswerData using the following JSON: |                                                                           |
|       |          | {  
  "answerCondition": "answer.isDisabled != true",  
  "shouldKeep": true  
} | Only included if healthCheckMonitorId is defined for the policy.          |
| 2     | HEALTH   | • No cases are allowed.  
Only included if healthCheckMonitorId is defined for the policy. |                                                                           |
| 3     | WEIGHTED | • No cases are allowed.  
• Answer data must be defined in the defaultAnswerData property for the rule.  
• Answers cannot be referenced by their pool property in answerCondition expressions, they must be referenced by their name property. |                                                                           |
| 4     | LIMIT    | • No cases are allowed.                                                                 |                                                                           |

Example of a POST /steeringPolicies policy using the LOAD_BALANCE template:

```json
{
  "compartmentId": "ocid1...",  
  "displayName": "Weighted load balance for a set of answers with health checks",  
  "ttl": 30,  
  "healthCheckMonitorId": "ocid1...",  
  "template": "LOAD_BALANCE",  
  "answers": [  
    {  
      "name": "server1",  
      "rtype": "A",  
      "rdata": "192.168.0.2"  
    },  
    {  
      "name": "server2",  
      "rtype": "A",  
      "rdata": "192.168.0.3"  
    }  
  ],  
  "rules": [  
    {  
      "ruleType": "FILTER",  
      "defaultAnswerData": [  
        {  
          "answerCondition": "answer.isDisabled != true",  
          "shouldKeep": true  
        }  
      ]  
    }  
  ]
}
```
ROUTE_BY_GEO

Geolocation-based steering policies distribute DNS traffic to different endpoints based on the location of the end user. Customers can define geographic regions composed of originating continent, countries or states/provinces (North America) and define a separate endpoint or set of endpoints for each region. Each of the following rules must be defined in the order specified below in the rules field of your request body when using a ROUTE_BY_GEO template:

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule</th>
<th>Restrictions</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FILTER</td>
<td>• No cases are allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Answer data must be defined in defaultAnswerData using the following JSON:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;answerCondition&quot;: &quot;answer.isDisabled != true&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;shouldKeep&quot;: true</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HEALTH</td>
<td>• No cases are allowed.</td>
<td>Only included if healthCheckMonitorId is defined for the policy.</td>
</tr>
</tbody>
</table>

```json
{
    "ruleType": "HEALTH"
},
{
    "ruleType": "WEIGHTED",
    "defaultAnswerData": [
        {
            "answerCondition": "answer.name == 'server1'",
            "value": 99
        },
        {
            "answerCondition": "answer.name == 'server2'",
            "value": 1
        }
    ]
},
{
    "ruleType": "LIMIT",
    "defaultCount": 1
}
```
### DNS and Traffic Management

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| 3     | PRIORITY                                                                 | - The defaultAnswerData property cannot be used on this rule.  
- At least one case must be defined. If there are multiple cases, the final case can provide a "catch-all" case.  
- The caseCondition property on cases can only use query.client.geoKey in the conditional expression.  
- Answers cannot be referenced by their name property in answerCondition expressions, they must be referenced by their pool property.  
- Every answer must have a pool property.  
- For each case's answerData:  
  - Every answer pool must be referenced once and only once.  
  - Every answer pool must have a unique value property (within the case).  
  - Each answer pool reference must match the pool property on one or more answers defined in the answer list for the policy.  |
| 4     | LIMIT                                                                 | - No cases are allowed.                                                                                                                                                                                    |

Example of a POST `/steeringPolicies` request body using the ROUTE_BY_GEO template:

```json
{
  "compartmentId": "ocid1...",
  "displayName": "Geolocations mapped to answer pools",
  "ttl": 30,
  "healthCheckMonitorId": "ocid1...",
  "template": "ROUTE_BY_GEO",
  "answers": [
    {
      "name": "US Server 1",
      "rtype": "A",
      "rdata": "192.168.0.2",
      "pool": "US"
    },
    {
      "name": "US Server 2",
      "rtype": "A",
      "rdata": "192.168.0.3",
      "pool": "US"
    },
    {
      "name": "EU Server 1",
      "rtype": "A",
      "rdata": "192.168.0.4",
      "pool": "EU"
    },
    {
      "name": "EU Server 2",
      "rtype": "A",
      "rdata": "192.168.0.5",
      "pool": "EU"
    },
    {
      "name": "rest of world 1",
      "rtype": "A",
      "rdata": "203.0.113.2",
      "pool": "Global"
    }
  ]
}```
},
  {
    "name": "rest of world 2",
    "rtype": "A",
    "rdata": "203.0.113.3",
    "pool": "Global"
  }
],
"rules": [
  {
    "ruleType": "FILTER",
    "defaultAnswerData": [
      {
        "answerCondition": "answer.isDisabled != true",
        "shouldKeep": true
      }
    ]
  },
  {
    "ruleType": "HEALTH"
  },
  {
    "ruleType": "PRIORITY",
    "cases": [
      {
        "caseCondition": "query.client.geoKey in (geoKey '6255149')",
        "answerData": [
          {
            "answerCondition": "answer.pool == 'US'",
            "value": 1
          },
          {
            "answerCondition": "answer.pool == 'EU'",
            "value": 2
          },
          {
            "answerCondition": "answer.pool == 'Global'",
            "value": 3
          }
        ]
      },
      {
        "caseCondition": "query.client.geoKey in (geokey '6255148')",
        "answerData": [
          {
            "answerCondition": "answer.pool == 'EU'",
            "value": 1
          },
          {
            "answerCondition": "answer.pool == 'US'",
            "value": 2
          },
          {
            "answerCondition": "answer.pool == 'Global'",
            "value": 3
          }
        ]
      },
      {
        "answerData": [
          {
            "answerCondition": "answer.pool == 'Global'",
            "value": 1
          }
        ]
      }
    ]
  }
]
ROUTE_BY_ASN

ASN-based steering policies enable you to steer DNS traffic based on Autonomous System Numbers (ASN). DNS queries originating from a specific ASN or set of ASNs can be steered to a specified endpoint. Each of the following rules must be defined in the order specified below in the rules field of your request body when using a ROUTE_BY_ASN template:

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule</th>
<th>Restrictions</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FILTER</td>
<td>• No cases are allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Answer data must be defined in defaultAnswerData using the following JSON:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;answerCondition&quot;: &quot;answer.isDisabled != true&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;shouldKeep&quot;: true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HEALTH</td>
<td>• No cases are allowed.</td>
<td>Only included if healthCheckMonitorId is defined for the policy.</td>
</tr>
<tr>
<td>Order</td>
<td>Rule</td>
<td>Restrictions</td>
<td>Comments</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>3</td>
<td>PRIORITY</td>
<td>- The defaultAnswerData property cannot be used on this rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- At least one case must be defined. If there are multiple cases, the final</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>case can provide a &quot;catch-all&quot; case.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The caseCondition property on cases can only use query.client.asn in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the conditional expression.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Answers cannot be referenced by their name property in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>answerCondition expressions, they must be referenced by their pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Every answer must have a pool property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For each case's answerData:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Every answer pool must be referenced once and only once.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Every answer pool must have a unique value property (within the case).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Each answer pool reference must match the pool property on one or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>more answers defined in the answer list for the policy.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>LIMIT</td>
<td>- No cases are allowed.</td>
<td></td>
</tr>
</tbody>
</table>

Example of a POST /steeringPolicies request body using the ROUTE_BY_ASN template:

```json
{
   "compartmentId": "ocid1...",
   "displayName": "ASNs mapped to pools",
   "ttl": 30,
   "template": "ROUTE_BY_ASN",
   "answers": [
      {
         "name": "ABC Server",
         "rtype": "A",
         "rdata": "192.168.0.2",
         "pool": "ABC"
      },
      {
         "name": "DEF Server",
         "rtype": "A",
         "rdata": "192.168.0.3",
         "pool": "DEF"
      },
      {
         "name": "Other",
         "rtype": "A",
         "rdata": "203.0.113.2",
         "pool": "Other"
      }
   ],
   "rules": [
      {
         "ruleType": "FILTER",
         "defaultAnswerData": [
            {
               "answerCondition": "answer.isDisabled != true",
               "shouldKeep": true
            }
         ]
      }
   ]
}
```
"ruleType": "PRIORITY",
"cases": [
  {
    "caseCondition": "query.client.asn == 3",
    "answerData": [
      {
        "answerCondition": "answer.pool == 'ABC'",
        "value": 1
      },
      {
        "answerCondition": "answer.pool == 'DEF'",
        "value": 2
      },
      {
        "answerCondition": "answer.pool == 'Other'",
        "value": 3
      }
    ]
  },
  {
    "caseCondition": "query.client.asn == 16591",
    "answerData": [
      {
        "answerCondition": "answer.pool == 'DEF'",
        "value": 1
      },
      {
        "answerCondition": "answer.pool == 'ABC'",
        "value": 2
      },
      {
        "answerCondition": "answer.pool == 'Other'",
        "value": 3
      }
    ]
  },
  {
    "answerData": [
      {
        "answerCondition": "answer.pool == 'Other'",
        "value": 1
      },
      {
        "answerCondition": "answer.pool == 'ABC'",
        "value": 2
      },
      {
        "answerCondition": "answer.pool == 'DEF'",
        "value": 3
      }
    ]
  }
],
"ruleType": "LIMIT",
"defaultCount": 1}
ROUTE_BY_IP

IP Prefix-based steering policies enable customers to steer DNS traffic based on the IP Prefix of the originating query. Each of the following rules must be defined in the order specified below in the rules field of your request body when using a ROUTE_BY_IP template:

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule</th>
<th>Restrictions</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FILTER</td>
<td>• No cases are allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Answer data must be defined in defaultAnswerData using the following JSON:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;answerCondition&quot;:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;answer.isDisabled != true&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;shouldKeep&quot;: true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HEALTH</td>
<td>• No cases are allowed.</td>
<td>Only included if healthCheckMonitorId is defined for the policy.</td>
</tr>
<tr>
<td>3</td>
<td>PRIORITY</td>
<td>• The defaultAnswerData property cannot be used on this rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At least one case must be defined. If there are multiple cases, the final</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>case can provide a &quot;catch-all&quot; case.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The caseCondition property on cases can only use query.client.address in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the conditional expression.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Answers cannot be referenced by their name property in answerCondition</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>expressions, they must be referenced by their pool property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Every answer must have a pool property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For each case's answerData:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Every answer pool must be referenced once and only once.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Every answer pool must have a unique value property (within the case).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Each answer pool reference must match the pool property on one or more</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>answers defined in the answer list for the policy.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>LIMIT</td>
<td>• No cases are allowed.</td>
<td></td>
</tr>
</tbody>
</table>

Example of a POST /steeringPolicies request body using the ROUTE_BY_IP template:

```json
{
  "compartmentId": "ocid1...",
  "displayName": "IP subnets mapped to answer pools",
  "ttl": 30,
  "template": "ROUTE_BY_IP",
  "answers": [
    {
      "name": "ABC Server",
      "rtype": "A",
      "rdata": "192.168.0.2",
      "pool": "ABC"
    }
  ]
}```
{
    "name": "DEF Server",
    "rtype": "A",
    "rdata": "192.168.0.3",
    "pool": "DEF"
},
{
    "name": "Other",
    "rtype": "A",
    "rdata": "203.0.113.2",
    "pool": "Other"
}
],
"rules": [
{
    "ruleType": "FILTER",
    "defaultAnswerData": [
    {
        "answerCondition": "answer.isDisabled != true",
        "shouldKeep": true
    }
    ],
},
{
    "ruleType": "PRIORITY",
    "cases": [
    {
        "caseCondition": "query.client.address in (subnet '10.0.3.0/24')",
        "answerData": [
        {
            "answerCondition": "answer.pool == 'ABC'",
            "value": 1
        },
        {
            "answerCondition": "answer.pool == 'DEF'",
            "value": 2
        },
        {
            "answerCondition": "answer.pool == 'Other'",
            "value": 3
        }
    ]
    },
    {
        "caseCondition": "query.client.address in (subnet '192.0.2.2/24')",
        "answerData": [
        {
            "answerCondition": "answer.pool == 'DEF'",
            "value": 1
        },
        {
            "answerCondition": "answer.pool == 'ABC'",
            "value": 2
        },
        {
            "answerCondition": "answer.pool == 'Other'",
            "value": 3
        }
    ]
    }
],
"answerData": [}
{  "answerCondition": "answer.pool == 'Other'",
   "value": 1
},
{  "answerCondition": "answer.pool == 'ABC'",
   "value": 2
},
{  "answerCondition": "answer.pool == 'DEF'",
   "value": 3
}
]
]
",
{  "ruleType": "LIMIT",
   "defaultCount": 1
}
]
}  

CUSTOM

Custom policies allow you to create complex policies combining the capabilities of failover, load balancing, geolocation, ASN and IP prefix steering. Custom templates do not require a regimented sequence of rules and it is recommended to contact Oracle Cloud Infrastructure support before creating a custom policy.

Rule Types

FILTER

Uses boolean data associated with answers, keeping answers only if the rule's shouldKeep value is true.

HEALTH

Utilizes Oracle Cloud Health Check monitors to determine the health of your endpoints and add and remove answers from your policy as needed. A health check monitor must be referenced in a health rule to have an effect on the policy. For more information about Health Checks, see Health Checks.

WEIGHTED

Uses a number between 0 and 255 used to determine how often an answer will be served in relation to other answers. Answers with higher values are more likely to be returned.

PRIORITY

Uses an integer associated with each answer to sort answers from lowest to highest value. Example: An answer with a priority value of 1 would be returned before an answer with a priority value of 10 in the list of answers. Answers that do not have a priority value assigned to them will be moved to the end of the list of answers.

LIMIT

Uses a count property to filter away all but the first answers in the list.

Traffic Management Steering Policy geokeys

Use these keys as values for the geokey fields of caseConditions in ROUTE_BY_GEO steering policies.
## Continent geokeys

<table>
<thead>
<tr>
<th>Continent Name</th>
<th>geoKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>6255146</td>
</tr>
<tr>
<td>Antarctica</td>
<td>6255152</td>
</tr>
<tr>
<td>Asia</td>
<td>6255147</td>
</tr>
<tr>
<td>Europe</td>
<td>6255148</td>
</tr>
<tr>
<td>North America</td>
<td>6255149</td>
</tr>
<tr>
<td>Oceania</td>
<td>6255151</td>
</tr>
<tr>
<td>South America</td>
<td>6255150</td>
</tr>
</tbody>
</table>

## Country geokeys

<table>
<thead>
<tr>
<th>Country Name</th>
<th>geoKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan(AF)</td>
<td>1149361</td>
</tr>
<tr>
<td>Aland Islands(AX)</td>
<td>661882</td>
</tr>
<tr>
<td>Albania(AL)</td>
<td>783754</td>
</tr>
<tr>
<td>Algeria(DZ)</td>
<td>2589581</td>
</tr>
<tr>
<td>American Samoa(AS)</td>
<td>5880801</td>
</tr>
<tr>
<td>Andorra(AD)</td>
<td>3041565</td>
</tr>
<tr>
<td>Angola(AO)</td>
<td>3351879</td>
</tr>
<tr>
<td>Anguilla(AI)</td>
<td>3573511</td>
</tr>
<tr>
<td>Antarctica(AQ)</td>
<td>6697173</td>
</tr>
<tr>
<td>Antigua and Barbuda(AG)</td>
<td>3576396</td>
</tr>
<tr>
<td>Argentina(AR)</td>
<td>3865483</td>
</tr>
<tr>
<td>Armenia(AM)</td>
<td>174982</td>
</tr>
<tr>
<td>Aruba(AW)</td>
<td>3577279</td>
</tr>
<tr>
<td>Australia(AU)</td>
<td>2077456</td>
</tr>
<tr>
<td>Austria(AT)</td>
<td>2782113</td>
</tr>
<tr>
<td>Azerbaijan(AZ)</td>
<td>587116</td>
</tr>
<tr>
<td>Bahamas(BS)</td>
<td>3572887</td>
</tr>
<tr>
<td>Bahrain(BH)</td>
<td>290291</td>
</tr>
<tr>
<td>Bangladesh(BD)</td>
<td>1210997</td>
</tr>
<tr>
<td>Barbados(BB)</td>
<td>3374084</td>
</tr>
<tr>
<td>Belarus(BY)</td>
<td>630336</td>
</tr>
<tr>
<td>Belgium(BE)</td>
<td>2802361</td>
</tr>
<tr>
<td>Belize(BZ)</td>
<td>3582678</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Benin(BJ)</td>
<td>2395170</td>
</tr>
<tr>
<td>Bermuda(BM)</td>
<td>3573345</td>
</tr>
<tr>
<td>Bhutan(BT)</td>
<td>1252634</td>
</tr>
<tr>
<td>Bolivia(BO)</td>
<td>3923057</td>
</tr>
<tr>
<td>Bonaire, Saint Eustatius and Saba(BQ)</td>
<td>7626844</td>
</tr>
<tr>
<td>Bosnia and Herzegovina(BA)</td>
<td>3277605</td>
</tr>
<tr>
<td>Botswana(BW)</td>
<td>933860</td>
</tr>
<tr>
<td>Bouvet Island(BV)</td>
<td>3371123</td>
</tr>
<tr>
<td>Brazil(BR)</td>
<td>3469034</td>
</tr>
<tr>
<td>British Indian Ocean Territory(IO)</td>
<td>1282588</td>
</tr>
<tr>
<td>British Virgin Islands(VG)</td>
<td>3577718</td>
</tr>
<tr>
<td>Brunei(BN)</td>
<td>1820814</td>
</tr>
<tr>
<td>Bulgaria(BG)</td>
<td>732800</td>
</tr>
<tr>
<td>Burkina Faso(BF)</td>
<td>2361809</td>
</tr>
<tr>
<td>Burundi(BI)</td>
<td>433561</td>
</tr>
<tr>
<td>Cambodia(KH)</td>
<td>1831722</td>
</tr>
<tr>
<td>Cameroon(CM)</td>
<td>2233387</td>
</tr>
<tr>
<td>Canada(CA)</td>
<td>6251999</td>
</tr>
<tr>
<td>Cape Verde(CV)</td>
<td>3374766</td>
</tr>
<tr>
<td>Cayman Islands(KY)</td>
<td>3580718</td>
</tr>
<tr>
<td>Central African Republic(CF)</td>
<td>239880</td>
</tr>
<tr>
<td>Chad(TD)</td>
<td>2434508</td>
</tr>
<tr>
<td>Chile(CL)</td>
<td>3895114</td>
</tr>
<tr>
<td>China(CN)</td>
<td>1814991</td>
</tr>
<tr>
<td>Christmas Island(CX)</td>
<td>2078138</td>
</tr>
<tr>
<td>Cocos (Keeling) Islands(CC)</td>
<td>1547376</td>
</tr>
<tr>
<td>Colombia(CO)</td>
<td>3686110</td>
</tr>
<tr>
<td>Comoros(KM)</td>
<td>921929</td>
</tr>
<tr>
<td>Congo(CG)</td>
<td>2260494</td>
</tr>
<tr>
<td>Cook Islands(CK)</td>
<td>1899402</td>
</tr>
<tr>
<td>Costa Rica(CR)</td>
<td>3624060</td>
</tr>
<tr>
<td>Croatia(HR)</td>
<td>3202326</td>
</tr>
<tr>
<td>Cuba(CU)</td>
<td>3562981</td>
</tr>
<tr>
<td>Curacao(CW)</td>
<td>7626836</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Cyprus (CY)</td>
<td>146669</td>
</tr>
<tr>
<td>Czech Republic (CZ)</td>
<td>3077311</td>
</tr>
<tr>
<td>Democratic Republic of the Congo (CD)</td>
<td>203312</td>
</tr>
<tr>
<td>Denmark (DK)</td>
<td>2623032</td>
</tr>
<tr>
<td>Djibouti (DJ)</td>
<td>223816</td>
</tr>
<tr>
<td>Dominica (DM)</td>
<td>3575830</td>
</tr>
<tr>
<td>Dominican Republic (DO)</td>
<td>3508796</td>
</tr>
<tr>
<td>East Timor (TL)</td>
<td>1966436</td>
</tr>
<tr>
<td>Ecuador (EC)</td>
<td>3658394</td>
</tr>
<tr>
<td>Egypt (EG)</td>
<td>357994</td>
</tr>
<tr>
<td>El Salvador (SV)</td>
<td>3585968</td>
</tr>
<tr>
<td>Equatorial Guinea (GQ)</td>
<td>2309096</td>
</tr>
<tr>
<td>Eritrea (ER)</td>
<td>338010</td>
</tr>
<tr>
<td>Estonia (EE)</td>
<td>453733</td>
</tr>
<tr>
<td>Ethiopia (ET)</td>
<td>337996</td>
</tr>
<tr>
<td>Falkland Islands (FK)</td>
<td>3474414</td>
</tr>
<tr>
<td>Faroe Islands (FO)</td>
<td>2622320</td>
</tr>
<tr>
<td>Fiji (FJ)</td>
<td>2205218</td>
</tr>
<tr>
<td>Finland (FI)</td>
<td>660013</td>
</tr>
<tr>
<td>France (FR)</td>
<td>3017382</td>
</tr>
<tr>
<td>French Guiana (GF)</td>
<td>3381670</td>
</tr>
<tr>
<td>French Polynesia (PF)</td>
<td>4030656</td>
</tr>
<tr>
<td>French Southern Territories (TF)</td>
<td>1546748</td>
</tr>
<tr>
<td>Gabon (GA)</td>
<td>2400553</td>
</tr>
<tr>
<td>Gambia (GM)</td>
<td>2413451</td>
</tr>
<tr>
<td>Georgia (GE)</td>
<td>614540</td>
</tr>
<tr>
<td>Germany (DE)</td>
<td>2921044</td>
</tr>
<tr>
<td>Ghana (GH)</td>
<td>2300660</td>
</tr>
<tr>
<td>Gibraltar (GI)</td>
<td>2411586</td>
</tr>
<tr>
<td>Greece (GR)</td>
<td>390903</td>
</tr>
<tr>
<td>Greenland (GL)</td>
<td>3425505</td>
</tr>
<tr>
<td>Grenada (GD)</td>
<td>3580239</td>
</tr>
<tr>
<td>Guadeloupe (GP)</td>
<td>3579143</td>
</tr>
<tr>
<td>Guam (GU)</td>
<td>4043988</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
</tr>
<tr>
<td>Guatemala(GT)</td>
<td>3595528</td>
</tr>
<tr>
<td>Guernsey(GG)</td>
<td>3042362</td>
</tr>
<tr>
<td>Guinea(GN)</td>
<td>2420477</td>
</tr>
<tr>
<td>Guinea-Bissau(GW)</td>
<td>2372248</td>
</tr>
<tr>
<td>Guyana(GY)</td>
<td>3378535</td>
</tr>
<tr>
<td>Haiti(HT)</td>
<td>3723988</td>
</tr>
<tr>
<td>Heard Island and McDonald Islands(HM)</td>
<td>1547314</td>
</tr>
<tr>
<td>Honduras(HN)</td>
<td>3608932</td>
</tr>
<tr>
<td>Hong Kong(HK)</td>
<td>1819730</td>
</tr>
<tr>
<td>Hungary(HU)</td>
<td>719819</td>
</tr>
<tr>
<td>Iceland(IS)</td>
<td>2629691</td>
</tr>
<tr>
<td>India(IN)</td>
<td>1269750</td>
</tr>
<tr>
<td>Indonesia(ID)</td>
<td>1643084</td>
</tr>
<tr>
<td>Iran(IR)</td>
<td>130758</td>
</tr>
<tr>
<td>Iraq(IQ)</td>
<td>99237</td>
</tr>
<tr>
<td>Ireland(IE)</td>
<td>2963597</td>
</tr>
<tr>
<td>Isle of Man(IM)</td>
<td>3042225</td>
</tr>
<tr>
<td>Israel(IL)</td>
<td>294640</td>
</tr>
<tr>
<td>Italy(IT)</td>
<td>3175395</td>
</tr>
<tr>
<td>Ivory Coast(CI)</td>
<td>2287781</td>
</tr>
<tr>
<td>Jamaica(JM)</td>
<td>3489940</td>
</tr>
<tr>
<td>Japan(JP)</td>
<td>1861060</td>
</tr>
<tr>
<td>Jersey(JE)</td>
<td>3042142</td>
</tr>
<tr>
<td>Jordan(JO)</td>
<td>248816</td>
</tr>
<tr>
<td>Kazakhstan(KZ)</td>
<td>1522867</td>
</tr>
<tr>
<td>Kenya(KE)</td>
<td>192950</td>
</tr>
<tr>
<td>Kiribati(KI)</td>
<td>4030945</td>
</tr>
<tr>
<td>Kuwait(KW)</td>
<td>285570</td>
</tr>
<tr>
<td>Kyrgyzstan(KG)</td>
<td>1527747</td>
</tr>
<tr>
<td>Laos(LA)</td>
<td>1655842</td>
</tr>
<tr>
<td>Latvia(LV)</td>
<td>458258</td>
</tr>
<tr>
<td>Lebanon(LB)</td>
<td>272103</td>
</tr>
<tr>
<td>Lesotho(LS)</td>
<td>932692</td>
</tr>
<tr>
<td>Liberia(LR)</td>
<td>2275384</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td>Libya(LY)</td>
<td>2215636</td>
</tr>
<tr>
<td>Liechtenstein(LI)</td>
<td>3042058</td>
</tr>
<tr>
<td>Lithuania(LT)</td>
<td>597427</td>
</tr>
<tr>
<td>Luxembourg(LU)</td>
<td>2960313</td>
</tr>
<tr>
<td>Macau(MO)</td>
<td>1821275</td>
</tr>
<tr>
<td>Macedonia(MK)</td>
<td>718075</td>
</tr>
<tr>
<td>Madagascar(MG)</td>
<td>1062947</td>
</tr>
<tr>
<td>Malawi(MW)</td>
<td>927384</td>
</tr>
<tr>
<td>Malaysia(MY)</td>
<td>1733045</td>
</tr>
<tr>
<td>Maldives(MV)</td>
<td>1282028</td>
</tr>
<tr>
<td>Mali(ML)</td>
<td>2453866</td>
</tr>
<tr>
<td>Malta(MT)</td>
<td>2562770</td>
</tr>
<tr>
<td>Marshall Islands(MH)</td>
<td>2080185</td>
</tr>
<tr>
<td>Martinique(MQ)</td>
<td>3570311</td>
</tr>
<tr>
<td>Mauritania(MR)</td>
<td>2378080</td>
</tr>
<tr>
<td>Mauritius(MU)</td>
<td>934292</td>
</tr>
<tr>
<td>Mayotte(YT)</td>
<td>1024031</td>
</tr>
<tr>
<td>Mexico(MX)</td>
<td>3996063</td>
</tr>
<tr>
<td>Micronesia(FM)</td>
<td>2081918</td>
</tr>
<tr>
<td>Moldova(MD)</td>
<td>617790</td>
</tr>
<tr>
<td>Monaco(MC)</td>
<td>2993457</td>
</tr>
<tr>
<td>Mongolia(MN)</td>
<td>2029969</td>
</tr>
<tr>
<td>Montenegro(ME)</td>
<td>3194884</td>
</tr>
<tr>
<td>Montserrat(MS)</td>
<td>3578097</td>
</tr>
<tr>
<td>Morocco(MA)</td>
<td>2542007</td>
</tr>
<tr>
<td>Mozambique(MZ)</td>
<td>1036973</td>
</tr>
<tr>
<td>Myanmar(MM)</td>
<td>1327865</td>
</tr>
<tr>
<td>Namibia(NA)</td>
<td>3355338</td>
</tr>
<tr>
<td>Nauru(NR)</td>
<td>2110425</td>
</tr>
<tr>
<td>Nepal(NP)</td>
<td>1282988</td>
</tr>
<tr>
<td>Netherlands(NL)</td>
<td>2750405</td>
</tr>
<tr>
<td>New Caledonia(NC)</td>
<td>2139685</td>
</tr>
<tr>
<td>New Zealand(NZ)</td>
<td>2186224</td>
</tr>
<tr>
<td>Nicaragua(NI)</td>
<td>3617476</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Niger(NE)</td>
<td>2440476</td>
</tr>
<tr>
<td>Nigeria(NG)</td>
<td>2328926</td>
</tr>
<tr>
<td>Niue(NU)</td>
<td>4036232</td>
</tr>
<tr>
<td>Norfolk Island(NF)</td>
<td>2155115</td>
</tr>
<tr>
<td>North Korea(KP)</td>
<td>1873107</td>
</tr>
<tr>
<td>Northern Mariana Islands(MP)</td>
<td>4041468</td>
</tr>
<tr>
<td>Norway(NO)</td>
<td>3144096</td>
</tr>
<tr>
<td>Oman(OM)</td>
<td>286963</td>
</tr>
<tr>
<td>Pakistan(PK)</td>
<td>1168579</td>
</tr>
<tr>
<td>Palau(PW)</td>
<td>1559582</td>
</tr>
<tr>
<td>Palestinian territories(PS)</td>
<td>6254930</td>
</tr>
<tr>
<td>Panama(PA)</td>
<td>3703430</td>
</tr>
<tr>
<td>Papua New Guinea(PG)</td>
<td>2088628</td>
</tr>
<tr>
<td>Paraguay(PY)</td>
<td>3437598</td>
</tr>
<tr>
<td>Peru(PE)</td>
<td>3932488</td>
</tr>
<tr>
<td>Philippines(PH)</td>
<td>1694008</td>
</tr>
<tr>
<td>Pitcairn(PN)</td>
<td>4030699</td>
</tr>
<tr>
<td>Poland(PL)</td>
<td>798544</td>
</tr>
<tr>
<td>Portugal(PT)</td>
<td>2264397</td>
</tr>
<tr>
<td>Puerto Rico(PR)</td>
<td>4566966</td>
</tr>
<tr>
<td>Qatar(QA)</td>
<td>289688</td>
</tr>
<tr>
<td>Reunion(RE)</td>
<td>935317</td>
</tr>
<tr>
<td>Romania(RO)</td>
<td>798549</td>
</tr>
<tr>
<td>Russia(RU)</td>
<td>2017370</td>
</tr>
<tr>
<td>Rwanda(RW)</td>
<td>49518</td>
</tr>
<tr>
<td>Saint Barthelemy(BL)</td>
<td>3578476</td>
</tr>
<tr>
<td>Saint Helena(SH)</td>
<td>3370751</td>
</tr>
<tr>
<td>Saint Kitts and Nevis(KN)</td>
<td>3575174</td>
</tr>
<tr>
<td>Saint Lucia(LC)</td>
<td>3576468</td>
</tr>
<tr>
<td>Saint Martin(MF)</td>
<td>3578421</td>
</tr>
<tr>
<td>Saint Pierre and Miquelon(PM)</td>
<td>3424932</td>
</tr>
<tr>
<td>Saint Vincent and the Grenadines(VC)</td>
<td>3577815</td>
</tr>
<tr>
<td>Samoa(WS)</td>
<td>4034894</td>
</tr>
<tr>
<td>San Marino(SM)</td>
<td>3168068</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Sao Tome and Principe(ST)</td>
<td>2410758</td>
</tr>
<tr>
<td>Saudi Arabia(SA)</td>
<td>102358</td>
</tr>
<tr>
<td>Senegal(SN)</td>
<td>2245662</td>
</tr>
<tr>
<td>Serbia(RS)</td>
<td>6290252</td>
</tr>
<tr>
<td>Seychelles(SC)</td>
<td>241170</td>
</tr>
<tr>
<td>Sierra Leone(SL)</td>
<td>2403846</td>
</tr>
<tr>
<td>Singapore(SG)</td>
<td>1880251</td>
</tr>
<tr>
<td>Sint Maarten(SX)</td>
<td>7609695</td>
</tr>
<tr>
<td>Slovakia(SK)</td>
<td>3057568</td>
</tr>
<tr>
<td>Slovenia(SI)</td>
<td>3190538</td>
</tr>
<tr>
<td>Solomon Islands(SB)</td>
<td>2103350</td>
</tr>
<tr>
<td>Somalia(SO)</td>
<td>51537</td>
</tr>
<tr>
<td>South Africa(ZA)</td>
<td>953987</td>
</tr>
<tr>
<td>South Georgia and the South Sandwich Islands(GS)</td>
<td>3474415</td>
</tr>
<tr>
<td>South Korea(KR)</td>
<td>1835841</td>
</tr>
<tr>
<td>South Sudan(SS)</td>
<td>7909807</td>
</tr>
<tr>
<td>Spain(ES)</td>
<td>2510769</td>
</tr>
<tr>
<td>Sri Lanka(LK)</td>
<td>1227603</td>
</tr>
<tr>
<td>Sudan(SD)</td>
<td>366755</td>
</tr>
<tr>
<td>Suriname(SR)</td>
<td>3382998</td>
</tr>
<tr>
<td>Svalbard and Jan Mayen(SJ)</td>
<td>607072</td>
</tr>
<tr>
<td>Swaziland(SZ)</td>
<td>934841</td>
</tr>
<tr>
<td>Sweden(SE)</td>
<td>2661886</td>
</tr>
<tr>
<td>Switzerland(CH)</td>
<td>2658434</td>
</tr>
<tr>
<td>Syria(SY)</td>
<td>163843</td>
</tr>
<tr>
<td>Taiwan(TW)</td>
<td>1668284</td>
</tr>
<tr>
<td>Tajikistan(TJ)</td>
<td>1220409</td>
</tr>
<tr>
<td>Tanzania(TZ)</td>
<td>149590</td>
</tr>
<tr>
<td>Thailand(TH)</td>
<td>1605651</td>
</tr>
<tr>
<td>Togo(TG)</td>
<td>2363686</td>
</tr>
<tr>
<td>Tokelau(TK)</td>
<td>4031074</td>
</tr>
<tr>
<td>Tonga(TO)</td>
<td>4032283</td>
</tr>
<tr>
<td>Trinidad and Tobago(TT)</td>
<td>3573591</td>
</tr>
<tr>
<td>Tunisia(TN)</td>
<td>2464461</td>
</tr>
<tr>
<td>Country Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Turkey (TR)</td>
<td>298795</td>
</tr>
<tr>
<td>Turkmenistan (TM)</td>
<td>1218197</td>
</tr>
<tr>
<td>Turks and Caicos Islands (TC)</td>
<td>3576916</td>
</tr>
<tr>
<td>Tuvalu (TV)</td>
<td>2110297</td>
</tr>
<tr>
<td>U.S. Virgin Islands (VI)</td>
<td>4796775</td>
</tr>
<tr>
<td>Uganda (UG)</td>
<td>226074</td>
</tr>
<tr>
<td>Ukraine (UA)</td>
<td>690791</td>
</tr>
<tr>
<td>United Arab Emirates (AE)</td>
<td>290557</td>
</tr>
<tr>
<td>United Kingdom (GB)</td>
<td>2635167</td>
</tr>
<tr>
<td>United States (US)</td>
<td>6252001</td>
</tr>
<tr>
<td>United States Minor Outlying Islands (UM)</td>
<td>5854968</td>
</tr>
<tr>
<td>Uruguay (UY)</td>
<td>3439705</td>
</tr>
<tr>
<td>Uzbekistan (UZ)</td>
<td>1512440</td>
</tr>
<tr>
<td>Vanuatu (VU)</td>
<td>2134431</td>
</tr>
<tr>
<td>Vatican City (VA)</td>
<td>3164670</td>
</tr>
<tr>
<td>Venezuela (VE)</td>
<td>3625428</td>
</tr>
<tr>
<td>Vietnam (VN)</td>
<td>1562822</td>
</tr>
<tr>
<td>Wallis and Futuna (WF)</td>
<td>4034749</td>
</tr>
<tr>
<td>Western Sahara (EH)</td>
<td>2461445</td>
</tr>
<tr>
<td>Yemen (YE)</td>
<td>69543</td>
</tr>
<tr>
<td>Zambia (ZM)</td>
<td>895949</td>
</tr>
<tr>
<td>Zimbabwe (ZW)</td>
<td>878675</td>
</tr>
</tbody>
</table>

**United States geokeys**

<table>
<thead>
<tr>
<th>State Name</th>
<th>geoKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>4829764</td>
</tr>
<tr>
<td>Alaska</td>
<td>5879092</td>
</tr>
<tr>
<td>Arizona</td>
<td>5551752</td>
</tr>
<tr>
<td>Arkansas</td>
<td>4099753</td>
</tr>
<tr>
<td>California</td>
<td>5332921</td>
</tr>
<tr>
<td>Colorado</td>
<td>5417618</td>
</tr>
<tr>
<td>Connecticut</td>
<td>4831725</td>
</tr>
<tr>
<td>Delaware</td>
<td>4142224</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>4138106</td>
</tr>
<tr>
<td>State Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>Florida</td>
<td>4155751</td>
</tr>
<tr>
<td>Georgia</td>
<td>4197000</td>
</tr>
<tr>
<td>Hawaii</td>
<td>5855797</td>
</tr>
<tr>
<td>Idaho</td>
<td>5596512</td>
</tr>
<tr>
<td>Illinois</td>
<td>4896861</td>
</tr>
<tr>
<td>Indiana</td>
<td>4921868</td>
</tr>
<tr>
<td>Iowa</td>
<td>4862182</td>
</tr>
<tr>
<td>Kansas</td>
<td>4273857</td>
</tr>
<tr>
<td>Kentucky</td>
<td>6254925</td>
</tr>
<tr>
<td>Louisiana</td>
<td>4331987</td>
</tr>
<tr>
<td>Maine</td>
<td>4971068</td>
</tr>
<tr>
<td>Maryland</td>
<td>4361885</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>6254926</td>
</tr>
<tr>
<td>Michigan</td>
<td>5001836</td>
</tr>
<tr>
<td>Minnesota</td>
<td>5037779</td>
</tr>
<tr>
<td>Mississippi</td>
<td>4436296</td>
</tr>
<tr>
<td>Missouri</td>
<td>4398678</td>
</tr>
<tr>
<td>Montana</td>
<td>5667009</td>
</tr>
<tr>
<td>Nebraska</td>
<td>5073708</td>
</tr>
<tr>
<td>Nevada</td>
<td>5509151</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>5090174</td>
</tr>
<tr>
<td>New Jersey</td>
<td>5101760</td>
</tr>
<tr>
<td>New Mexico</td>
<td>5481136</td>
</tr>
<tr>
<td>New York</td>
<td>5128638</td>
</tr>
<tr>
<td>North Carolina</td>
<td>4482348</td>
</tr>
<tr>
<td>North Dakota</td>
<td>5690763</td>
</tr>
<tr>
<td>Ohio</td>
<td>5165418</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>4544379</td>
</tr>
<tr>
<td>Oregon</td>
<td>5744337</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>6254927</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>5224323</td>
</tr>
<tr>
<td>South Carolina</td>
<td>4597040</td>
</tr>
<tr>
<td>South Dakota</td>
<td>5769223</td>
</tr>
<tr>
<td>Tennessee</td>
<td>4662168</td>
</tr>
<tr>
<td>State Name</td>
<td>geoKey</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Texas</td>
<td>4736286</td>
</tr>
<tr>
<td>Utah</td>
<td>5549030</td>
</tr>
<tr>
<td>Vermont</td>
<td>5242283</td>
</tr>
<tr>
<td>Virginia</td>
<td>6254928</td>
</tr>
<tr>
<td>Washington</td>
<td>5815135</td>
</tr>
<tr>
<td>West Virginia</td>
<td>4826850</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>5279468</td>
</tr>
<tr>
<td>Wyoming</td>
<td>5843591</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Canada Provinces geokeys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Province Name</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>Alberta</td>
</tr>
<tr>
<td>British Columbia</td>
</tr>
<tr>
<td>Manitoba</td>
</tr>
<tr>
<td>New Brunswick</td>
</tr>
<tr>
<td>Newfoundland and Labrador</td>
</tr>
<tr>
<td>Northwest Territories</td>
</tr>
<tr>
<td>Nova Scotia</td>
</tr>
<tr>
<td>Nunavut</td>
</tr>
<tr>
<td>Ontario</td>
</tr>
<tr>
<td>Prince Edward Island</td>
</tr>
<tr>
<td>Quebec</td>
</tr>
<tr>
<td>Saskatchewan</td>
</tr>
<tr>
<td>Yukon</td>
</tr>
</tbody>
</table>
This chapter explains how to send large volume email.

Overview of the Email Delivery Service

Oracle Cloud Infrastructure Email Delivery is an email sending service that provides a fast and reliable managed solution for sending high-volume emails that need to reach your recipients' inbox. Email Delivery provides the tools necessary to send application-generated email for mission-critical communications such as receipts, fraud detection alerts, multi-factor identity verification, and password resets.

Oracle Cloud Infrastructure's Email Deliverability team manages the platform using key deliverability metrics to ensure the best sending reputation possible for your emails.

The following items are provided to you when you send email using the Email Delivery service:

- Unique mailbox provider SMTP configurations on our Mail Transfer Agents (MTA)
- Bounce collection
- User complaint collection
- Email authentication standards
- Deliverability performance

Email Delivery Service Components

Email Delivery uses the components described in this section.

APPROVED SENDERs

An Approved Sender is a resource that equates to the "From" address. An approved sender is associated with a compartment and only exists in the region where the approved sender was configured. If you need to have the same approved sender in another region, it must be created in the other region. For example, if you create an approved sender in the US West (Phoenix) region, you cannot send email through the US East (Ashburn) region.

SUPPRESSION LIST

The Suppression List is included on your Email Delivery console user interface and from the API. Email Delivery automatically adds email addresses with bounce codes showing permanent failures or user complaints to the suppression list to protect your sender reputation. Email Delivery will not send any messages to these recipients in the future.

Reasons for suppression currently include:

- Complaints
- Hard bounces
- Repetitive soft bounces
- Manual entries
- List-unsubscribe requests
SPF AUTHENTICATION

Sender Policy Framework (SPF) is used by email receivers to detect email spoofing. Using SPF, an email receiver can check if the Internet Protocol (IP) is explicitly authorized to send for that domain. SPF is implemented by publishing a special TXT record to a domain's DNS records. The TXT record declares which hosts are allowed to send mail on behalf of this domain. Receiving mail servers check the SPF records of sending domains to verify that the email's source IP address is authorized to send from that domain. Without SPF, a spam or phishing email can be “spoofed” to appear that the email comes from a legitimate domain. Domains that implement SPF are much more likely to block emails attempting to spoof your domain. For an overview of how SPF works, see Sender Policy Framework. For details on SPF record syntax, see SPF Record Syntax.

Regions and Availability Domains

SMTP credentials can be used for any region, as identities are global assets. However, approved senders (your "From" address) must be configured within each region you plan to use for Email Delivery. To configure approved senders within each region, select a region from the Region menu in the Console and create an approved sender. Configure your application to send email to the endpoint of that region where you created the approved sender, using the global SMTP credentials. The sending application is not required to be located in the region where email is sent from, however, we recommend that it is local or as close as possible for performance reasons.

For more information, see Regions and Availability Domains on page 180.

Configuring a New Region

If you want to start sending email from a new region, keep the following in mind:

- An approved sender must be created in the new region.
- SMTP credentials are global, however, it is recommended that you generate SMTP credentials for a new user (without console access) in the new region so that the credentials are not shared with other regions. Ensure that the user has the correct privileges.
- Email must be sent to the new regional SMTP connection endpoint.
- The suppression list and approved senders are regional Email Delivery assets.

For example, if an email sent from the US West (Phoenix) region bounces, the recipient email address will be added to the US West (Phoenix) region suppression list. This recipient would not be added to other region suppression lists. If you are sending email from different regions, approved senders must be created in each region.

- SPF must be set up on each subdomain. For example, in your DNS setup, create a TXT record for notification.eu-frankfurt-1.oraclecloud.com and paste the following information from the dialog box into the record: v=spf1 include:eu.rp.oracleemaildelivery.com ~all

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see SDKs and Other Tools.

To access the Console, you must use a supported browser. You can use the Console link at the top of this page to go to the sign-in page. You are prompted to enter your cloud tenant, your user name, and your password. For general information about using the API, see About the API.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more
information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Email Delivery supports the following authentication types for control plane operations (management endpoint):

- **Instance Authorization:** The IAM service feature that enables instances to be authorized actors (or principals) to perform actions on service resources. Each compute instance has its own identity, and it authenticates using the certificates that are added to it. These certificates are automatically created, assigned to instances and rotated, preventing the need for you to distribute credentials to your hosts and rotate them.

- **Cross-Tenancy:** Cross-tenancy authorization allows customers to share resources between tenancies. To authorize a cross-tenancy request, the request must be endorsed by the requester’s tenancy and permitted by the target tenancy.

- **Federated:** Federated authentication enables an administrator to configure a relationship between an identity provider and a service provider. When you federate Oracle Cloud Infrastructure with an identity provider, you manage users and groups in the identity provider. You manage authorization in Oracle Cloud Infrastructure’s IAM service. Oracle Cloud Infrastructure tenancies are federated with Oracle Identity Cloud Service by default.

**Note:** Instance authorization, cross-tenancy, and federated authentication types do not apply to SMTP email sending. An approved sender and SMTP credentials are required and must be associated with the same tenancy for SMTP email sending.

**SMTP Authentication and Connection Endpoints**

Email Delivery only supports the AUTH PLAIN command when using SMTP authentication. If the sending application is not flexible with the AUTH command, an SMTP proxy/relay can be used. For more information about the AUTH command, see AUTH Command and its Mechanisms.

Use the following regional endpoints for establishing SMTP connections for sending.

- South Korea North (Chuncheon): smtp.email.ap-chuncheon-1.oci.oraclecloud.com
- India South (Hyderabad): smtp.email.ap-hyderabad-1.oci.oraclecloud.com
- Australia Southeast (Melbourne): smtp.email.ap-melbourne-1.oci.oraclecloud.com
- India West (Mumbai): smtp.email.ap-mumbai-1.oci.oraclecloud.com
- Japan Central (Osaka): smtp.email.ap-osaka-1.oci.oraclecloud.com
- South Korea Central (Seoul): smtp.email.ap-seoul-1.oci.oraclecloud.com
- Australia East (Sydney): smtp.email.ap-sydney-1.oci.oraclecloud.com
- Japan East (Tokyo): smtp.email.ap-tokyo-1.oci.oraclecloud.com
- Canada Southeast (Montreal): smtp.email.ca-montreal-1.oci.oraclecloud.com
- Canada Southeast (Toronto): smtp.email.ca-toronto-1.oci.oraclecloud.com
- Netherlands Northwest (Amsterdam): smtp.email.eu-amsterdam-1.oci.oraclecloud.com
- Germany Central (Frankfurt): smtp.email.eu-frankfurt-1.oci.oraclecloud.com
- Switzerland North (Zurich): smtp.email.eu-zurich-1.oci.oraclecloud.com
- UAE East (Dubai): smtp.email.me-dubai-1.oci.oraclecloud.com
- Saudi Arabia West (Jeddah): smtp.email.me-jeddah-1.oci.oraclecloud.com
- Chile (Santiago): smtp.email.sa-santiago-1.oci.oraclecloud.com
- Brazil East (Sao Paulo): smtp.email.sa-saopaulo-1.oci.oraclecloud.com
- UK West (Newport): smtp.email.uk-cardiff-1.oci.oraclecloud.com
- UK South (London): smtp.email.uk-london-1.oci.oraclecloud.com
- US East (Ashburn): smtp.email.us-ashburn-1.oci.oraclecloud.com
- US West (Phoenix): smtp.email.us-phoenix-1.oci.oraclecloud.com
• US West (San Jose): smtp.email.us-sanjose-1.oci.oraclecloud.com

Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about available Email Delivery service metrics and how to view them, see Email Delivery Metrics on page 1756.

Email Delivery Service Capabilities and Limits

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Customers that sign up for a free Oracle Cloud trial are limited to:

• A volume of 200 unique recipients among all emails sent per day.

  Note:
  
  This limit applies to unique recipients among all emails sent. For example, a single email sent to 100 recipients would count the same as 100 individual emails each sent to a single recipient.

• 2,000 approved senders.
• Each user is limited to a maximum of two SMTP credentials.
• Sending rates are limited to 10 emails per minute.
• Inline attachments.

  Note:
  
  Customers that start with a Free Trial and transition to a paid account must request a limit increase.

Enterprise accounts are limited to:

• A volume of 50,000 unique recipients among all emails sent per day.

  Note:
  
  This limit applies to unique recipients among all emails sent. For example, a single email sent to 100 recipients would count the same as 100 individual emails each sent to a single recipient.

• 10,000 approved senders.
• Sending rates are limited to 18,000 emails per minute.
• Inline attachments.

Email Delivery, by default, supports messages up to 2 MB, inclusive of message headers, body, and attachments. Based on requirement, you can request a limit increase up to a maximum of 60 MB. To open a service request to increase the limit, see Requesting a Service Limit Increase on page 217. Your increase request is evaluated by the following information you provide:

• What are your current sending domains?
• Do your sending practices meet the requirements of CAN-SPAM and CASL?
• Briefly describe the type of email you will be sending. For example, are the emails marketing/bulk/newsletters, transactional, notifications, and so on?
• Do you send emails related to payday loans or credit card offers?
• Do you send email on behalf of other companies?
• How do the recipients sign up to receive these emails? Specify any domains they might sign up on.
• Are there any other methods that are used to collect email addresses?
• How many emails do you want to send per month?
• Which ESP supplier are you currently using to send your emails?
• What is the maximum number of messages you need to send in a burst capacity (within a specific timeframe)?
• What is the maximum size of your messages?
• What is the number of emails sent per day that is over 2 MB?
• Are your recipients Oracle email addresses (for example, test.user@oracle.com)?
• Which email delivery region do you intend to use to send email through?

**Note:**
The Email Delivery platform supports higher volumes. Limits are set as a safeguard for our customers' reputation. To open a service request to increase the email sending limit, see Requesting a Service Limit Increase on page 217.

### Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies. For more details about policies for Email Delivery, see Details for the Email Service.

Permissions are required for managing and using approved senders and the suppression list. For example:

• To enable all operations on approved senders for a specific user group:
  
  Allow group <Your Group Name> to manage approved-senders in tenancy

• To enable all operations on suppressions for a specific user group:
  
  Allow group <Your Group Name> to manage suppressions in tenancy

### Dedicated IP Addresses

When you create an Email Delivery service account, by default, your emails are sent from IP addresses shared with other Oracle customers.

Email Delivery supports IPs addresses dedicated to you, for complete control over your reputation. Both a shared IP or dedicated IP strategy can provide excellent delivery depending on your needs and mail stream characteristics.

When using a dedicated pool of Oracle owned IP addresses, only your mail is sent from them.

**Note:**
Our deliverability experts review all dedicated IP requests to ensure the best deliverability for your situation. Dedicated IP addresses may not be advised for lower volume or more sporadic email sending, as this does not support a good sending reputation and therefore can cause an impact to your email deliverability.

Dedicated IP addresses are ideal for senders who:

• **Send large volumes of mail on a consistent basis to sustain their own IP reputation.** Sending a large volume of mail consistently is what Internet Service Providers (ISPs) automated filters use to assign a reputation to your IP address. This is one of the key inputs into whether your messages are delivered into the inbox, spam folder, or temporarily rejected.

• **Want complete control of their sending reputation AND understand email delivery best practices.** When you are the only sender on an IP, it insulates your reputation from other senders. This can be good or bad depending on your sending practices and consistent hygiene.
• **Have large volumes, different mail streams, and want to build unique reputations for each.** Dedicated IPs enable you to build separate IP reputations based on different types of mail streams like transactional messages versus bulk marketing mail. If you have the volume to support it, isolating these mail streams can reduce the risk of delivery challenges for more critical message types.

Dedicated IP addresses are likely not a good fit for senders who:

• **Send mail inconsistently at low volumes preventing an ISP reputation from being assigned.** To build an IP reputation, ISPs prefer a predictable mail cadence with enough email volume to assign a reputation. Failing to meet this requirement could lead to delivery challenges. Sending in a shared IP pool with many smaller senders will provide the ISP with a large volume of consistent mail.

• **Do not understand email best practices, which could lead to poor-reputation delivery challenges.** Sending in a shared IP pool with other customers that is managed by Oracle can be less risky for an email novice.

Your mail characteristics (volume, burst rates, reputation, and so on) will vary your dedicated IP strategy. Our teams are trained on dedicated IP strategies and ready to support your needs. If you need help with your configuration, you can go to My Oracle Support and create a service request.

### Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Email Delivery supports applying tags to approved senders.

### Integration with Oracle Cloud Infrastructure Services

Email Delivery audits the following events:

- Creating a sender (CreateSender)
- Deleting a sender (DeleteSender)
- Retrieving details about a sender (ListSenders)

To view logs for events in the Email Delivery service, your user must be in a group with the ability to view all of the Audit event logs in the tenancy. For more information, see Viewing Audit Log Events on page 494.

### Getting Started with Email Delivery

You can set up the Email Delivery service within the Console. To begin sending email with Email Delivery, complete the following steps:

1. Generate SMTP credentials for a user.
2. Set up permissions.
3. Create an approved sender.
4. Configure SPF on the approved sender domain.
5. Configure the SMTP connection.

For more information, see Getting Started with Email Delivery on page 1743.

### Getting Started with Email Delivery

Email Delivery provides a highly scalable, cost effective, and reliable way to send email from your applications. Email Delivery includes developer-friendly tools to quickly send application-generated email for mission-critical communications such as receipts, programmatic notifications, or password reset emails.
Email Delivery Basics

When you use Email Delivery, we become your outbound email server. If you have an existing email server, you can keep it and configure it to send through Email Delivery. The Email Delivery service will take care of the feedback loops and platform reputation automatically.

Getting Started

This topic gives guidance on how to get started with Email Delivery. For complete details about the service and its components, see Overview of the Email Delivery Service on page 1738.

Email Configuration Options

You can configure Oracle Cloud Infrastructure using the Console (a browser-based interface), REST API, SDKs, CLI or Terraform.

Using the Email Delivery SDK

The Email Delivery SDK is available in several programming languages. For information on installing and configuring the Oracle Cloud Infrastructure SDKs, see Developer Resources on page 4178.

Examples of SDK usage can be found on GitHub, including:

- Example: Email Delivery SDK for Java
- Example: Email Delivery SDK for Python
- Example: Email Delivery SDK for Ruby
- Example: Email Delivery SDK for Go

Configuring Third-Party Applications

The following information describes how you can configure third-party applications to send email through Email Delivery:

- Integrating Oracle Application Express with Email Delivery on page 1758
- Integrating Postfix with Email Delivery on page 1759
- Integrating Oracle Enterprise Manager with Email Delivery on page 1760
- Integrating Mailx with Email Delivery on page 1761
- Integrating Swaks with Email Delivery on page 1763
Email Delivery

- Integrating Sendmail with Email Delivery on page 1767
- Integrating JavaMail with Email Delivery on page 1764
- Integrating PeopleSoft with Email Delivery on page 1770
- Integrating Python with Email Delivery on page 1773

Sending Email

To begin sending email with Email Delivery, complete the following steps:

**Generate SMTP credentials for a user.**

Simple Mail Transfer Protocol (SMTP) credentials are necessary to send email through Email Delivery. Each user is limited to a maximum of two SMTP credentials. If more than two are required, SMTP credentials must be generated that are associated with another existing user or more users must be created.

**Best Practice:** A security best practice is to generate SMTP credentials for a new user instead of your Console user that already has permissions assigned to it. For detailed instructions on creating a user, see Adding Users.

**To generate SMTP credentials for a user.**

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list that has permissions to manage email, and then click the user's name to view the details.

   **Tip:** If your user does not have permissions to view or create users, you can create SMTP credentials under your user.

   Open the Profile menu and click User Settings.

2. Click SMTP Credentials.
3. Click Generate SMTP Credentials.
4. Enter a Description of the SMTP Credentials in the dialog box.
5. Click Generate SMTP Credentials. A user name and password is displayed.
6. Copy the user name and password for your records and click Close.

**Set up permissions.**

The new user must be assigned to a group with permissions to manage approved-senders and suppressions.

**To create a policy to allow a group to manage approved senders and suppressions**

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed.
2. If you want to attach the policy to a compartment other than the one you're viewing, select the desired compartment from the list on the left. Where the policy is attached controls who can later modify or delete it (see Overview of Policies on page 2136).
3. Click Create Policy.
4. Enter the following:
   - **Name:** A unique name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later.
   - **Description:** A friendly description. You can change this later if you want to.
   - **Policy Versioning:** Select Keep Policy Current if you'd like the policy to stay current with any future changes to the service's definitions of verbs and resources. Or if you'd prefer to limit access according to the
Email Delivery

definitions that were current on a specific date, select **Use Version Date** and enter that date in format YYYY-MM-DD format. For more information, see **Advanced Policy Features** on page 2160.

- **Statement**: Enter the following policy statement:

  ```
  Allow group <group name> to use approved-senders in compartment <compartment name>
  ```

  For more information about policies and policy syntax, see **Policy Basics** on page 2137.

- **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Create**.

The new policy will go into effect typically within 10 seconds.

**To add the new user to the group**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. A list of the users in your tenancy is displayed.

2. Locate the user in the list.

3. Click the user. Its details are displayed.

4. Click **Groups**.

5. Click **Add User to Group**.

6. Select the group from the drop-down list, and then click **Add**.

Make sure to let the user know which compartment(s) they have access to.

**Create an approved sender.**

You must set up an approved sender for all “From:” addresses sending mail via Oracle Cloud Infrastructure or mail will be rejected. An approved sender is associated with a compartment and only exists in the region where the approved sender was configured. That is, if you create an approved sender in the Phoenix (PHX) region, you cannot send email through the Ashburn (IAD) region.

**Best Practice**: Approved senders should not be created in the root compartment. If approved senders exist in the root compartment, you are required to create a policy to manage approved senders in the entire tenant. Creating approved senders in a compartment other than the root allows the policy to be specific to that compartment.

**To create an approved sender using the Console**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Email Delivery** and click **Email Approved Senders**. Ensure that you are in the correct compartment. Your user must be in a group with permissions to manage approved-senders in this compartment.

2. Click **Create Approved Sender** within the **Approved Senders** view.

3. Enter the email address you want to list as an approved sender in the **Add Sender** dialog box.

4. Click **Add**. The email address is added to your Approved Senders list.

**Tip:**

Approved senders are unique to tenancies. If an attempt is made to create a duplicate approved sender within a tenancy, the service will return a 409 Conflict error.

**To create an approved sender using the API**

The following example shows how to create an approved sender. For more information about creating an approved sender, see **CreateSender**.

```bash
POST /20170907/senders
```
Configure SPF on the approved sender domain.

Sender Policy Framework (SPF) is used by email receivers to detect email spoofing. Using SPF, an email receiver can check if the Internet Protocol (IP) is explicitly authorized to send for that domain. SPF is implemented by publishing a special TXT record to a domain's DNS records. The TXT record declares which hosts are allowed to send mail on behalf of this domain. Receiving mail servers check the SPF records of sending domains to verify that the email's source IP address is authorized to send from that domain. Without SPF, a spam or phishing email can be "spoofed" to appear that the email comes from a legitimate domain. Domains that implement SPF are much more likely to block emails attempting to spoof your domain. For an overview of how SPF works, see Sender Policy Framework. For details on SPF record syntax, see SPF Record Syntax.

The Approved Senders section within the Console provides validation of an SPF record for each of your approved senders.

To configure SPF

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Approved Senders.
2. Select the checkbox for the approved sender you want to view SPF details for and click View SPF.
3. The Manage SPF dialog box appears indicating whether an SPF record for the approved sender exists.

- If your domain does not currently have an SPF record, the information necessary to add an SPF record in your DNS setup is displayed. See Managing DNS Service Zones for instructions on adding a zone record in Oracle Cloud Infrastructure. If your DNS setup resides with another provider, please reference their documentation for adding a TXT record to your domain.
- In your DNS setup, create a TXT record and paste the following information into the record based on the sending location:

<table>
<thead>
<tr>
<th>Sending Location</th>
<th>SPF Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
<tr>
<td>Asia/Pacific</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:ap.rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
<tr>
<td>Europe</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:eu.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
<tr>
<td>All Commercial Regions</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:ap.rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>include:eu.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
</tbody>
</table>
Configure the SMTP connection.

Set up and test your SMTP connection using an SMTP library or product such as Postfix or Sendmail, to send email through Oracle Cloud Infrastructure Email Delivery.

SMTP Connection Endpoints

Use the following regional endpoints for establishing SMTP connections for sending.

- YNY: smtp.email.ap-chuncheon-1.oci.oraclecloud.com
- HYD: smtp.email.ap-hyderabad-1.oci.oraclecloud.com
- MEL: smtp.email.ap-melbourne-1.oci.oraclecloud.com
- BOM: smtp.email.ap-mumbai-1.oci.oraclecloud.com
- KIX: smtp.email.ap-osaka-1.oci.oraclecloud.com
- ICN: smtp.email.ap-seoul-1.oci.oraclecloud.com
- SYD: smtp.email.ap-sydney-1.oci.oraclecloud.com
- NRT: smtp.email.ap-tokyo-1.oci.oraclecloud.com
- YUL: smtp.email.ca-montreal-1.oci.oraclecloud.com
- YYZ: smtp.email.ca-toronto-1.oci.oraclecloud.com
- AMS: smtp.email.eu-amsterdam-1.oci.oraclecloud.com
- FRA: smtp.email.eu-frankfurt-1.oci.oraclecloud.com
- ZRH: smtp.email.eu-zurich-1.oci.oraclecloud.com
- DXB: smtp.email.me-dubai-1.oci.oraclecloud.com
- JED: smtp.email.me-jeddah-1.oci.oraclecloud.com
- SCL: smtp.email.sa-santiago-1.oci.oraclecloud.com
- GRU: smtp.email.sa-saopaulo-1.oci.oraclecloud.com
- CWL: smtp.email.uk-cardiff-1.oci.oraclecloud.com
- LHR: smtp.email.uk-london-1.oci.oraclecloud.com
- IAD: smtp.email.us-ashburn-1.oci.oraclecloud.com
- PHX: smtp.email.us-phoenix-1.oci.oraclecloud.com
- SJC: smtp.email.us-sanjose-1.oci.oraclecloud.com

TLS Requirements

Oracle maintains strict security policies and only accepts email traffic using Transport Layer Security (TLS). Use of TLS 1.2 is mandatory to send email using Oracle Cloud Infrastructure.

The approved TLS 1.2 ciphers are:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

To access SMTP sending information to configure the connection in your system

Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Configuration.

The following information is displayed:

- **Public Endpoint**: The public endpoint used to send email to for this region.
- **SMTP Ports**: The SMTP ports used to accept email. Email Delivery supports TLS on port 25 or 587.
• **Security:** This field indicates if TLS, the standard means of performing encryption in transit for email, is being used. Customers must encrypt email while it is in transit to the Oracle Cloud Infrastructure Email Delivery service. Encrypted emails are protected from being read during transit.

  **Tip:**

  Java applications (including JavaMail) must be updated to the latest version to ensure the latest protocols, ciphers, and security patches are in compliance with Oracle’s supported security policies and ciphers.

**Begin sending email.**

Use Email Delivery to begin sending email.

**Suppression List**

As you begin to send email, Email Delivery automatically adds email addresses with bounce codes showing permanent failures or user complaints to the suppression list to protect your sender reputation. Email Delivery will not send any messages to these recipients in the future. Reasons for suppression currently include:

- Complaints
- Hard bounces
- Repetitive soft bounces
- Manual entries
- List-unsubscribe requests

**To manually add an email address to the suppression list using the Console**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Email Delivery** and click **Email Suppression List**.
2. Click **Add Suppression**.
3. In the Add Suppression dialog box, enter the email address.
4. Click **Add**. The email address is added to the suppression list.

For more information, see **Managing the Suppression List** on page 1755.

**To manually add an email address to the suppression list using the API**

The following example shows how to add an email address to the suppression list. For more information about managing the suppressions list, see **GetSuppression** and **DeleteSuppression**.

```
POST /20170907/suppressions
{
    "compartmentId": "ocid1.compartment.oc1..aaaaaaaat7uqcb6zoxvzoga4d4vh4dtweciauepcacd3skz56atf3qp73d7fx",
    "emailAddress": "user@example.com",
}
```

**Using the API**

You can access Oracle Cloud Infrastructure using the **REST API**. Instructions for the API are included in topics throughout this guide. For a list of available SDKs, see **SDKs and Other Tools**.

**Regions**

See **Regions and Availability Domains** on page 1739 for more information.

**Limits**

See **Email Delivery Service Capabilities and Limits** for information on new account and enterprise account limits.
Best Practices

This section describes best practices for using Email Delivery.

Volume Testing - In order to maintain our sender reputation and yours, testing at volume needs to be done using the following best practice.

- Use a recipient address at the email-blackhole.com domain, such as example@email-blackhole.com. Email Delivery will accept the mail but will not deliver it to an inbox.
- If large volume emails are sent to valid email addresses, these will get rejected by receivers and will result in a large amount of hard bounces. This will negatively affect IP reputation. For testing bounce processing, send small amounts of emails to a domain that does not have an MX record, in other words, the domain does not exist.

Deliverability - To help you learn and manage the habits that affect your sending reputation, see Deliverability Best Practices on page 1780.

Sending to Email Aliases - When sending email to an alias, the alias is considered one recipient. When sending email to a distribution group or list set up in an email client such as Apple Mail or Outlook, a separate email is sent for each recipient in the group.

Generate SMTP Credentials for a User

Simple Mail Transfer Protocol (SMTP) credentials are necessary to send email through Email Delivery. Each user is limited to a maximum of two SMTP credentials. If more than two are required, SMTP credentials must be generated on other existing users or more users must be created.

A security best practice is to generate SMTP credentials for a new user instead of your Console user that already has permissions assigned to it. For detailed instructions on creating a user, see Adding Users. The new user must be assigned to a group with permissions to manage approved-senders and suppressions. For example:

```
Allow group <group name> to use approved-senders in compartment <compartment name>
```

Using the Console

To generate SMTP credentials for a user

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list that has permissions to manage email, and then click the user's name to view the details.

   **Tip:**
   If your user does not have permissions to view or create users, you can create SMTP credentials under your user.

   Open the **Profile** menu () and click **User Settings**.

2. Click SMTP Credentials.
3. Click Generate SMTP Credentials.
4. Enter a Description of the SMTP Credentials in the dialog box.
5. Click Generate SMTP Credentials. A user name and password is displayed.
6. Copy the user name and password for your records and click Close.

Managing Approved Senders

An approved sender must be set up for all “From:” addresses sending mail through Oracle Cloud Infrastructure, or mail will be rejected. An approved sender is associated with a compartment and only exists in the region where the approved sender was configured. That is, if you create an approved sender in the US West (Phoenix) region, you cannot send email through the US East (Ashburn) region with that sender.

The approved senders that you add must use a domain name that you own and control. The following sending domains cannot be used to create approved senders:
Email Delivery

- @oracle.com - This sending domain name is reserved for Oracle employee and corporate system use.
- @*.oraclevcn.com - This domain name is reserved for private use within an Oracle Cloud Infrastructure VCN. Email sending domains must have SPF and DKIM records that can be resolved on the public internet, and oraclevcn.com is only reachable within private Oracle Cloud Infrastructure networks. Use of this sending domain results in delivery delays, failures, and a possible blocklist addition.
- @gmail.com, @hotmail.com, @yahoo.com, and other public mailbox service providers - You cannot use a sending domain from a public mailbox service provider such as gmail, hotmail, icloud, yahoo, and so on. These providers tend to have restrictive DMARC records and will not delegate permission to third-party Email Delivery services (through SPF and DKIM records). Use of these sending domains results in delivery delays, failures, and a possible blocklist addition.

The following sending domain is problematic for use as an approved sender:
- @oraclecloud.com - This sending domain name is reserved for Oracle Cloud system use.

Approved senders should not be created in the root compartment. If approved senders exist in the root compartment, you are required to create a policy to manage approved senders in the entire tenant. Creating approved senders in a compartment other than the root allows the policy to be specific to that compartment.

Moving Approved Senders to a Different Compartment

You can move approved senders from one compartment to another. To manage approved senders and use approved senders to send mail, user groups must have an associated identity policy in the new compartment. For more information, see Managing Compartments on page 2431.

Using the Console

To create an approved sender

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Approved Senders. Ensure that you are in the correct compartment. Your user must be in a group with permissions to manage approved senders in this compartment.
2. Click Create Approved Sender within the Approved Senders view.
3. Enter the email address you want to list as an approved sender in the Create Approved Sender dialog box.

   Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
4. Click Create Approved Sender. The email address is added to your Approved Senders list.

   Tip:
   Approved senders are unique to tenancies. If an attempt is made to create a duplicate approved sender within a tenancy, the service will return a 409 Conflict error.

To delete an approved sender

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Approved Senders.
2. Find the approved sender you're interested in, click the Actions icon (three dots), and then click Delete.
3. In the confirmation dialog box, click Confirm. The email address is removed from the Approved Senders list.

To move an approved sender to a different compartment

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Approved Senders.
2. In the List Scope section, select a compartment.
3. Find the approved sender in the list, click the the Actions icon (three dots), and then click Choose New Compartment.
4. Choose the destination compartment from the list.
5. Click Move Approved Sender.

   For more information, see Managing Compartments on page 2431.

To manage tags for an approved sender

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Approved Senders.
2. Find the approved sender you're interested in, click the Actions icon (three dots), and then click View Tags to view or edit existing tags. Or click Apply tag(s) to add new ones.

   For more information, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225. Use the following operations to manage your approved senders:

- CreateSender
- GetSender
- ListSenders
- DeleteSender

Configure SPF

Sender Policy Framework (SPF) is used by email receivers to detect email spoofing. Using SPF, an email receiver can check if the Internet Protocol (IP) is explicitly authorized to send for that domain. SPF is implemented by publishing a special TXT record to a domain's DNS records. The TXT record declares which hosts are allowed to send mail on behalf of this domain. Receiving mail servers check the SPF records of sending domains to verify that the email's source IP address is authorized to send from that domain. Without SPF, a spam or phishing email can be “spoofed” to appear that the email comes from a legitimate domain. Domains that implement SPF are much more likely to block emails attempting to spoof your domain. For an overview of how SPF works, see Sender Policy Framework. For details on SPF record syntax, see SPF Record Syntax.

The Approved Senders section within the Console provides validation of an SPF record for each of your approved senders. SPF is required for subdomains of oraclegovcloud.com and recommended in other cases.

Using the Console

To configure SPF:

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Approved Senders.
2. Select the checkbox for the approved sender you want to view SPF details for and click View SPF.

   Tip:

   You can search for an approved sender by using the Search field. Addresses can be sorted alphanumerically or by creation date in ascending or descending order.

3. The Manage SPF dialog box appears indicating whether an SPF record for the approved sender exists.

   If your domain does not currently have an SPF record, the information necessary to add an SPF record in your DNS setup is displayed. See Managing DNS Service Zones for instructions on adding a zone record in Oracle...
Cloud Infrastructure. If your DNS setup resides with another provider, please reference their documentation for adding a TXT record to your domain.

- In your DNS setup, create a TXT record and paste the following information into the record based on the sending region:

<table>
<thead>
<tr>
<th>Sending Region</th>
<th>SPF Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
<tr>
<td>Asia/Pacific</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:ap.rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
<tr>
<td>Europe</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:eu.rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
<tr>
<td>All Commercial Regions</td>
<td>v=spf1</td>
</tr>
<tr>
<td></td>
<td>include:rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>include:ap.rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>include:eu.rp.oracleemaildelivery.com</td>
</tr>
<tr>
<td></td>
<td>-all</td>
</tr>
</tbody>
</table>

- For US Government Cloud with FedRAMP Authorization, see SPF Record Syntax on page 161.
- For US Federal Cloud with DISA Impact Level 5, see SPF Record Syntax on page 167.
- For United Kingdom Government Cloud, see SPF Record Syntax on page 176.

- If your domain currently has an SPF DNS record, you must update your record in order to successfully use Email Delivery.
- The following is an example of a command used to view an SPF record:

```
dig -t TXT +short syd1.rp.oracleemaildelivery.com
```

Example output:

```
"v=spf1 ip4:192.168.0.25 -all"
```

- If you're using other email providers in addition to Email Delivery, you'll need to combine the include statements from your other providers with Email Delivery.

### Configure SMTP Connection

Set up and test your SMTP connection using an SMTP library or product, such as Postfix or Sendmail, to send email through Oracle Cloud Infrastructure Email Delivery.

Open Email Configuration to access SMTP sending information to configure the connection in your system. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Configuration. The following information is displayed:

- **Public Endpoint:** The public endpoint used to send email to for this region.
- **SMTP Ports:** The SMTP ports used to accept email. Email Delivery supports TLS on port 25 or 587.
• **Security:** This field indicates if TLS, the standard means of performing encryption in transit for email, is being used. Customers must encrypt email while it is in transit to the Oracle Cloud Infrastructure Email Delivery service. Encrypted emails are protected from being read during transit.

```
<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java applications (including JavaMail) must be updated to the latest version to ensure the latest protocols, ciphers, and security patches are in compliance with Oracle’s supported security policies and ciphers.</td>
</tr>
</tbody>
</table>
```

**SMTP Connection Endpoints**

Use the following regional endpoints for establishing SMTP connections for sending.

- YNY: smtp.email.ap-chuncheon-1.oci.oraclecloud.com
- HYD: smtp.email.ap-hyderabad-1.oci.oraclecloud.com
- MEL: smtp.email.ap-melbourne-1.oci.oraclecloud.com
- BOM: smtp.email.ap-mumbai-1.oci.oraclecloud.com
- KIX: smtp.email.ap-osaka-1.oci.oraclecloud.com
- ICN: smtp.email.ap-seoul-1.oci.oraclecloud.com
- SYD: smtp.email.ap-sydney-1.oci.oraclecloud.com
- NRT: smtp.email.ap-tokyo-1.oci.oraclecloud.com
- YUL: smtp.email.ca-montreal-1.oci.oraclecloud.com
- YYZ: smtp.email.ca-toronto-1.oci.oraclecloud.com
- AMS: smtp.email.eu-amsterdam-1.oci.oraclecloud.com
- FRA: smtp.email.eu-frankfurt-1.oci.oraclecloud.com
- ZRH: smtp.email.eu-zurich-1.oci.oraclecloud.com
- DXB: smtp.email.me-dubai-1.oci.oraclecloud.com
- JED: smtp.email.me-jeddah-1.oci.oraclecloud.com
- SCL: smtp.email.sa-santiago-1.oci.oraclecloud.com
- GRU: smtp.email.sa-sao paulo-1.oci.oraclecloud.com
- CWL: smtp.email.uk-cardiff-1.oci.oraclecloud.com
- LHR: smtp.email.uk-london-1.oci.oraclecloud.com
- IAD: smtp.email.us-ashburn-1.oci.oraclecloud.com
- PHX: smtp.email.us-phoenix-1.oci.oraclecloud.com
- SJC: smtp.email.us-sanjose-1.oci.oraclecloud.com

**TLS Requirements**

Oracle maintains strict security policies and only accepts email traffic using Transport Layer Security (TLS). Use of TLS 1.2 is mandatory to send email using Oracle Cloud Infrastructure.

The approved TLS 1.2 ciphers are:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Managing the Suppression List

Manually add an email address to the suppression list to prevent it from being part of your sending list.

Users are required to have correct permissions to manage the suppression list. Currently, identity policies for suppression must be at the tenant level (not at the compartment level). The following is an example of the permission policy statement.

```
Allow group <group name> to manage suppressions in tenancy
```

Suppressions are stored at the tenancy level. Therefore any request requiring a `compartmentId` must provide the `tenancyId` as the `compartmentId`. For example:

```
Allow group <ordinary users> to inspect approved-senders in tenancy
Allow group <power users> to read approved-senders in tenancy
Allow group <sender admins> to manage approved-senders in tenancy
Allow user <mail user> to use approved-senders in tenancy where target.approved-sender.senderId = <senderId>
```

```
Allow group <ordinary users> to inspect suppressions in tenancy
Allow group <power users> to read suppressions in tenancy
Allow group <sender admins> to manage suppressions in tenancy
```

Using the Console

To manually add an email address to the suppression list

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Suppression List.
2. Click Add Suppression.
3. In the Add Suppression dialog box, enter the email address.
4. Click Add. The email address is added to the Suppression List.

To delete an email address from the suppression list

1. Open the navigation menu. Under Solutions and Platform, go to Email Delivery and click Email Suppression List.
2. Select the checkbox for the email address you want to delete and then click Delete.
3. In the confirmation dialog box, click OK. The email address is removed from the Suppression List.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225. Use the following operations to manage your suppressions:

- CreateSuppression
- GetSuppression
- ListSuppressions
- DeleteSuppression
Email Delivery Metrics

You can monitor the health, capacity, and performance of your Email Delivery by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace `oci_emaildelivery` (the Email Delivery service).

Overview of the Email Delivery Service Metrics

Oracle Cloud Infrastructure Email Delivery (Email Delivery) is an email sending service that provides a fast and reliable managed solution for sending high-volume emails that need to reach your recipients' inbox. The Email Delivery service metrics help you measure counts for accepted mail, email complaints, emails hard bounced, and emails soft bounced. Accepted mail consists of the unique emails accepted by the Email Delivery service to send. Emails are defined by the number of unique emails, as well as the number of unique recipients per message attempted to be delivered, resulting in successful delivery and blocked email. For example, sending an email with 10 recipients means 10 emails accepted. Email complaints consists of the number of email complaints for a sender by the Email Delivery service. Emails hard bounced consists of the number of emails hard bounced (permanent failure) for a sender by the recipient domain's email service. Emails soft bounced consists of the number of emails soft bounced (persistent transient failure) by the recipient domain's email service or due to an inability to reach that service.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Delivery is billed for every 1,000 emails accepted.</td>
</tr>
</tbody>
</table>

For more information, see Overview of the Email Delivery Service on page 1738.

Prerequisites

- IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_emaildelivery

The metrics listed in the following table are automatically available for any policies you create. You do not need to enable monitoring on the resource to get these metrics. However, your tenancy must have Email Delivery configured and must send mail to make the `oci_emaildelivery` metric space available in the Metrics Explorer feature.

Each metric includes the following dimensions:

- **RESOURCEID**
  
  The OCID of the policy to which the metric applies.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailsAccepted</td>
<td>Emails Accepted</td>
<td>count</td>
<td>The number of unique emails accepted by the Email Delivery service.</td>
<td>resourceID (The OCID of the approved sender to which the metric applies.)</td>
</tr>
<tr>
<td>EmailComplaints</td>
<td>Email Complaints</td>
<td>count</td>
<td>The number of email complaints for a sender by the Email Delivery service.</td>
<td>resourceDomain (The domain name of the approved sender email address to which the metric applies.)</td>
</tr>
<tr>
<td>EmailsHardBounced</td>
<td>Emails Hard Bounced</td>
<td>count</td>
<td>The number of emails hard bounced (permanent failure) for a sender by the recipient domain's email service.</td>
<td></td>
</tr>
<tr>
<td>EmailsSoftBounced</td>
<td>Emails Soft Bounced</td>
<td>count</td>
<td>The number of emails soft bounced (persistent transient failure) by the recipient domain's email service or due to an inability to reach that service.</td>
<td></td>
</tr>
</tbody>
</table>

**Using the Console**

Email Delivery service metrics are currently only available using the Metrics Explorer feature in the Console. For more information about metrics, see Viewing Metric Charts.

**To view Email Delivery metric charts**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
   For Metric Namespace, select `oci_emaildelivery`.
2. Select a metric to view from the Metric Name field.
3. Select a qualifier specified in the Dimension Name field. For example, the dimension `resourceId` is specified in the metric definition for `EmailsAccepted`.
4. Select the value you want to use for the specified dimension in the Dimension Value field. For example, the resource identifier for your instance of interest.
5. Click Update Chart.
   The chart will be updated with the metrics that have been requested.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**Using the API**

Use the following APIs for monitoring:
- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)
Integrating Oracle Application Express with Email Delivery

Configure Oracle Application Express to Send Email Through Email Delivery

You can use the APEX_MAIL package to send emails from Oracle Application Express applications deployed in Autonomous Transaction Processing. See Creating an Autonomous Database on Shared Exadata Infrastructure on page 1157 and Autonomous Transaction Processing for more information.

Before you use APEX_MAIL you must configure Oracle Cloud Infrastructure Email Delivery in your Application Express instance.

To enable APEX_MAIL functionality in your Application Express instance in Autonomous Transaction Processing:

1. Identify the SMTP connection endpoint for Email Delivery. You configure the endpoint as the SMTP Host in your Application Express instance in Step 4. See Configure SMTP Connection on page 1753 for more information.

2. Generate SMTP credentials for Email Delivery. Your Application Express instance uses credentials to authenticate with Email Delivery servers when you send email. See Generate SMTP Credentials for a User on page 1750 for more information.

3. Create an approved sender for Email Delivery. You need to complete this step for all email addresses you use as the "From" with APEX_MAIL.SEND calls, as the Application Email From Address in your apps, or in the SMTP_FROM instance parameter. See Managing Approved Senders on page 1750 for more information.

4. Connect to your Autonomous Transaction Processing as ADMIN user using a SQL client and configure the following SMTP parameters using APEX_INSTANCE_ADMIN.SET_PARAMETER:
   - **SMTP_HOST_ADDRESS**: Specifies the SMTP connection endpoint from Step 1.
   - **SMTP_USERNAME** Specifies the SMTP credential user name from Step 2.
   - **SMTP_PASSWORD** Specifies the SMTP credential password from Step 2.

   For example:

   ```sql
   BEGIN
   APEX_INSTANCE_ADMIN.SET_PARAMETER('SMTP_HOST_ADDRESS', 'smtp.us-phoenix-1.oraclecloud.com');
   APEX_INSTANCE_ADMIN.SET_PARAMETER('SMTP_USERNAME', 'ocid1.user.oc1.username');
   APEX_INSTANCE_ADMIN.SET_PARAMETER('SMTP_PASSWORD', 'password');
   COMMIT;
   END;
   /
   ```

5. Send a test email using APEX SQL Workshop, SQL Commands specifying one of the approved senders from Step 3 as "From". For example:

   ```sql
   BEGIN
   APEX_MAIL.SEND(p_from => 'alice@example.com',
   p_to   => 'bob@example.com',
   p_subj => 'Email from Oracle Autonomous Database',
   p_body => 'Sent using APEX_MAIL');
   END;
   /
   ```

6. To monitor email delivery in your Application Express instance:
   a. Sign in to APEX Administration Services.
   b. Open the Manage Instance page.
   c. Click the Mail Queue link in the Manage Meta Data section.

   Alternatively, query APEX_MAIL_QUEUE and APEX_MAIL_LOG views using a SQL client.

More Information

- Creating Applications with Oracle Application Express in Autonomous Database
Integrating Postfix with Email Delivery

Configure Postfix to Send Email Through Email Delivery

You can use Postfix to send emails through Email Delivery. Before you use Postfix you must configure Oracle Cloud Infrastructure Email Delivery in your Postfix application.

**Note:**
The paths and commands used below for specifying file locations are specific to Ubuntu/Debian; your file paths or editing commands may differ depending on the operating system you are using. The changes to the configuration files are the same.

To enable Postfix to integrate with Email Delivery:

1. Make sure Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

   **Note:**
The SMTP credentials are required to configure Postfix to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.

2. To open the `main.cf` file, run the following command:

   ```
sudo vi /etc/postfix/main.cf
   ```

   Add the following information to the end of the file:

   ```
smtp_tls_security_level = may
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options =
   ```

3. Update the Postfix `main.cf` file.

   If the following line is present, either remove the line or turn it off:

   ```
smtpd_use_tls = yes
   ```

4. Update `relayhost` to include your SMTP connection endpoint and port. For example:

   ```
relayhost = smtp.us-ashburn-1.oraclecloud.com:587
   ```

5. Create the `sasl_passwd` file in the same directory as `main.cf`.

   Run the following command:

   ```
sudo vi /etc/postfix/sasl_passwd
   ```

6. Add your relay host and port by entering:

   ```
server:port user:pass
   ```

   where:

   - `server` is your relay host and `port` is 25 or 587.
   - `user` is the user name and `pass` is the password you received when you generated your SMTP credentials.
7. Enter the permissions in the password file.
   Run the following command:
   ```bash
   sudo chown root:root /etc/postfix/sasl_passwd & & sudo chmod 600 /etc/postfix/sasl_passwd
   ```

8. Generate the password hash.
   Run the following command:
   ```bash
   sudo postmap hash:/etc/postfix/sasl_passwd
   ```

   Run the following command:
   ```bash
   sudo postfix reload
   ```

10. Test the configuration by sending a test email.
    Run the following command:
    ```bash
    echo "This is a test message" | mail -s "Test" -r "<approved sender email address>" <recipient email address>
    ```
    If you want to monitor the log while you send the test email, open a separate Terminal window and run the following command before running the test command:
    ```bash
    log stream --predicate ' (process == "smtpd") || (process == "smtp")' --info
    ```
    A status=sent (250 Ok) message in the log indicates the email was sent successfully.

    **Note:**
    If you are using SASL authentication, you must use the following RPM package: cyrus-sasl-plain. See the PostFix website for further documentation on configuring SASL authentication.

**More Information**
- See the Postfix website for more information on Postfix configuration.
- See TLS errors when integrating with Postfix on page 1776 for troubleshooting techniques related to Email Delivery.

**Integrating Oracle Enterprise Manager with Email Delivery**

**Configure Oracle Enterprise Manager to Send Email Through Email Delivery**

You can use Oracle Enterprise Manager to send emails through Email Delivery. Before you use Oracle Enterprise Manager, you must configure Oracle Cloud Infrastructure Email Delivery in your Oracle Enterprise Manager application.

**Note:**
For information on installing Oracle Enterprise Manager, see Setting Up Oracle Enterprise Manager on Oracle Cloud Infrastructure.

To enable Oracle Enterprise Manager to integrate with Email Delivery:
1. Make sure Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

   Note:

   The SMTP credentials are required to configure Oracle Enterprise Manager to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.

2. In Oracle Enterprise Manager, go to the Setup menu and click Initial Setup Console.
3. In the Initial Setup Console section, click Configure Mail Servers in the navigation pane.
4. In the Sender Identify section, click Edit.
5. Enter the name of the administrator or system that should send the email notifications and the email address from which the notifications should be sent, and then click OK.
6. In the Outgoing Mail (SMTP) Servers section, click Create.
7. Enter the mail server host name, the mail server credentials, and the encryption method to be used, and then click OK.
8. Select the outgoing mail server you wish to test and select Test Mail Server. Note the confirmation message in the console and verify that you received the test email in your inbox.

   Note:

   If you configure multiple outgoing mail servers, automatic failover and load balancing is performed in round robin fashion.

Integrating Mailx with Email Delivery

Configure Mailx to Send Email Through Email Delivery

You can use Mailx to send emails through Email Delivery. Before you use Mailx, you must configure Oracle Cloud Infrastructure Email Delivery in your Mailx application.

Use these instructions only if no mail transfer agent (MTA), such as Postfix or Sendmail, is in use on the system. If you are configuring an MTA, follow the configuration instructions for that program and leave the Mailx settings at their defaults. This makes Mailx use the local MTA program to send outbound mail.

   Note:

   These steps assume you are logged into an Oracle Linux instance. Other distributions of Linux might have different commands and file locations.

To enable Mailx to integrate with Email Delivery:

1. Ensure that Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

   Note:

   The SMTP credentials are required to configure Mailx to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.

2. Update the Mailx mail.rc file.

   To open the mail.rc file, run the following command:

   ```
   sudo vi ~/etc/mail.rc
   ```

   Add the following information to the end of the file:

   ```
   #smtp config
   set nss-config-dir=/etc/pki/nssdb/
   set smtp-use-starttls
   ```
set smtp-auth=plain
set smtp=<SMTP_connection_endpoint>:25
set from=<from_email_address>
set smtp-auth-user=<OCID from smtp credentials>
set smtp-auth-password=<password from smtp credentials>

#write and quit file
:wq!

3. Test the configuration by sending a test email.

Run the following command:

```bash
echo "Test Email" | mail -v -s "Send an email via mailx" -r "from_name<from_email_address>" -S replyto="from_name<from_email_address>" -S smtp="SMTP_connection endpoint:25" -S smtp-use-starttls -S smtp-auth=plain -S smtp-auth-user='"<ocid from smtp credentials>"' -S smtp-auth-password='"<password from smtp credentials>"' -S ssl-verify=ignore <recipient_email_address>
```

**Troubleshooting**

"Error in certificate: Peer's certificate issuer has been marked as not trusted" occurs when sending email

To troubleshoot this issue, complete the following steps:

1. Run the following command to view the certificate chain:

   ```bash
echo | openssl s_client -starttls smtp -crlf -connect <SMTP-endpoint>:587
```

Example output:

```
[root@ociuvddatg01 ~]# echo | openssl s_client -starttls smtp -crlf -connect smtp.email.us-ashburn-1.oci.oraclecloud.com:587
CONNECTED(00000003)
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
  verify return:1
depth=1 C = US, O = DigiCert Inc, CN = DigiCert Global CA G2
  verify return:1
depth=0 C = US, ST = California, L = Redwood City, O = Oracle Corporation, OU = Oracle OCI-PROD ASHBURN, CN = smtp.email.us-ashburn-1.oci.oraclecloud.com
  verify return:1
  ---
Certificate chain
0 s:/C=US/ST=California/L=Redwood City/O=Oracle Corporation/OU=Oracle OCI-PROD ASHBURN/CN=smtp.email.us-ashburn-1.oci.oraclecloud.com
  i:/C=US/O=DigiCert Inc/CN=DigiCert Global CA G2
1 s:/C=US/O=DigiCert Inc/CN=DigiCert Global CA G2
  i:/C=US/O=DigiCert Inc/CN=www.digicert.com/CN=DigiCert Global Root G2
2 s:/C=US/O=DigiCert Inc/CN=www.digicert.com/CN=DigiCert Global Root G2
  i:/C=US/O=DigiCert Inc/CN=www.digicert.com/CN=DigiCert Global Root G2
  ---
Server certificate
-----BEGIN CERTIFICATE-----
.......-----END CERTIFICATE-----
.......```

2. Extract the certificate that signed your domain. In this example, this is the last certificate (2 s:/C=US/O=DigiCert Inc/CN=www.digicert.com/CN=DigiCert Global Root G2). Copy and paste the
certificate into a separate DigiCert.pem file, including the BEGIN CERTIFICATE and END CERTIFICATE fields.

3. Install the certificate into the Centos NSSDB database. Replace "DigiCert Global Root G2" in the following example with your certificate:

```bash
sudo certutil -A -t "C,r," -n "DigiCert Global Root G2" -d /etc/pki/nssdb/ -i DigiCert.pem
```

To view the certificate, use the following command:

```bash
sudo certutil -L -d /etc/pki/nssdb/
```

More Information

- For network security services, see the Mailx documentation.

Integrating Swaks with Email Delivery

Swaks (Swiss Army Knife SMTP) is a transaction-based tool you can use to test SMTP configurations in Email Delivery. Before you use Swaks, you must configure Email Delivery and take note of your SMTP sending information and SMTP credentials.

**Note:**
Many options and parameters can be used to test various scenarios with Swaks. When Swaks evaluates an option (that is, a flag with parameters), it does so in three steps:
- First, it looks for a configuration file (default location or specified with --config).
- Next, it looks for options in environment variables.
- Finally, it looks at command line options. At each step, any options set earlier are overridden.

Assumptions

The following procedures assume the following:
- The following example supplies options to Swaks via the command line in long form, for example, --server as opposed to the short form, -s.
- The following example assumes the default behavior to connect through network sockets.
- A local certificate is not required for a TLS connection to be negotiated. The following example assumes the default behavior where Swaks does not attempt certificate verification.
- Swaks is primarily intended for use on UNIX-like operating systems with functionality based on known standards so it should work on most modern mail servers.

Configure Swaks to Send Email Through Email Delivery

To enable Swaks to test the configuration of Email Delivery:

1. Ensure Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

**Note:**
The SMTP credentials are required to configure Swaks to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.
2. Ensure Swaks is installed. The installation process differs depending on which operating system you are using. For example, run the following command to install Swaks on Oracle Linux:

```
sudo yum install swaks -y
```

3. To send a test email with Swaks, run the following command:

```
swaks --pipeline -tls --server <smtp.region.oraclecloud.com> --port <587 or 25> --auth-user '<username OCID from SMTP credentials>' --auth-pass '<password>' --from '<sender email address>' --to '<recipient email address>' --data '<email message>'
```

For example:

```
swaks --pipeline -tls --server smtp.us-ashburn-1.oraclecloud.com --port 25 --auth-user 'ocid1.user.oc1..<unique_ID>' --auth-pass '<password>' --from 'sender@example.com' --to 'recipient@example.com' --data 'From: sender@example.com
Date: Thu, 13 Sep 2019
Subject: Test Send

Test email'
```

Note the following when sending email with Swaks:

- The `-tls` parameter is required.
- The `--pipeline` parameter is supported to make use of SMTP pipelining.
- The `--port <number>` parameter or `:<port number>` syntax can be used to specify the port.

**More Information**

- See the Swaks documentation for more information.

**Integrating JavaMail with Email Delivery**

JavaMail provides a platform-independent and protocol-independent framework to build mail and messaging applications. Before you use JavaMail, you must configure Email Delivery and take note of your SMTP sending information and SMTP credentials. This guide uses the Eclipse IDE and the JavaMail API to send email through Email Delivery.

**Important:**

Java applications (including JavaMail) must be updated to the latest version to ensure that the latest protocols, ciphers, and security patches are in compliance with Oracle's supported security policies and ciphers.

**Configure JavaMail to Send Email Through Email Delivery**

To enable JavaMail to test the configuration of Email Delivery:

1. Ensure Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

```
Note:

The SMTP credentials are required to configure JavaMail to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.
```

2. Open a browser and go to https://github.com/javaee/javamail/releases.

3. Under Downloads, select `javax.mail.jar` to download the latest version of JavaMail.
4. Create a project in Eclipse by performing the following steps:
   
   a. In Eclipse, open the **File** menu. Select **New**, and then click **Java Project**.
   
   b. In the Create a Java Project dialog box, enter a project name, and then click **Next**.
   
   c. In the Java Settings dialog box, select the **Libraries** tab.
   
   d. Click **Add External JARs**.
   
   e. In the JAR Selection dialog box, browse to the folder in which you downloaded JavaMail. Select the `javax.mail.jar` file, and then click **Open**.
   
   f. In the Java Settings dialog box, click **Finish**.
   
5. In Eclipse, in the Package Explorer window, expand your project.

6. Under your project, right-click the src directory, select **New**, and then click **Class**.

7. In the New Java Class dialog box, enter "OCIemail" in the **Name** field and then click **Finish**.

8. Enter the following code in **OCIemail.java** to send a test email with JavaMail:

```java
import java.util.Properties;
import javax.mail.Message;
import javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;

public class OCIemail {

    public static void main(String[] args) throws Exception {

    // Replace FROM with your "From" address.
    // This address must be added to Approved Senders in the console.
    static final String FROM = "<sender email address>";
    static final String FROMNAME = "<sender name>";

    // Replace TO with a recipient address.
    static final String TO = "<recipient email address>";

    // Replace smtp_username with your Oracle Cloud Infrastructure SMTP username generated in console.
    static final String SMTP_USERNAME = "<username OCID from SMTP credentials>";

    // Replace smtp_password with your Oracle Cloud Infrastructure SMTP password generated in console.
    static final String SMTP_PASSWORD = "<SMTP password>";

    // Oracle Cloud Infrastructure Email Delivery hostname.
    static final String HOST = "<SMTP endpoint>";

    // The port you will connect to on the SMTP endpoint. Port 25 or 587 is allowed.
    static final int PORT = 587;

    static final String SUBJECT = "<subject of your email>";
    static final String BODY = String.join(
        System.getProperty("line.separator"),
        "<h1>OCI Email Delivery test</h1>",
        "<p>This email was sent with OCI Email Delivery using the ",
        "<a href='javamail'>https://github.com/javaee/javamail</a>'s Javamail Package</a>",
    )

    }

```
Properties props = System.getProperties();
props.put("mail.transport.protocol", "smtp");
props.put("mail.smtp.port", PORT);
//props.put("mail.smtp.ssl.enable", "true"); //the default value is
false if not set
props.put("mail.smtp.auth", "true");
props.put("mail.smtp.auth.login.disable", "true"); //the default
authorization order is "LOGIN PLAIN DIGEST-MD5 NTLM". 'LOGIN' must be
disabled since Email Delivery authorizes as 'PLAIN'
props.put("mail.smtp.starttls.enable", "true"); //TLSv1.2 is
required
props.put("mail.smtp.starttls.required", "true"); //Oracle Cloud
Infrastructure required

// Create a Session object to represent a mail session with the
specified properties.
Session session = Session.getDefaultInstance(props);

// Create a message with the specified information.
MimeMessage msg = new MimeMessage(session);
msg.setFrom(new InternetAddress(FROM,FROMNAME));
msg.setRecipient(Message.RecipientType.TO, new
InternetAddress(TO));
msg.setSubject(SUBJECT);
msg.setContent(BODY,"text/html");

// Create a transport.
Transport transport = session.getTransport();

// Send the message.
try {
    System.out.println("Sending Email now...standby...");

    // Connect to OCI Email Delivery using the SMTP credentials
    specified.
    transport.connect(HOST, SMTP_USERNAME, SMTP_PASSWORD);
    // Send email.
    transport.sendMessage(msg, msg.getAllRecipients());
    System.out.println("Email sent!");
}
catch (Exception ex) {
    System.out.println("The email was not sent.");
    System.out.println("Error message: " + ex.getMessage());
}
finally
{
    // Close & terminate the connection.
9. In the OCIemail.java file, replace the following with your own values:

```
transport.close();
}
}
}
```

**Note:**

Email addresses are case-sensitive. Ensure that the addresses are the same as the ones you entered in Approved Senders in the console.

- **FROM** - Replace with your sender email address. This email address must be added to the Approved Senders list in Email Delivery first.
- **TO** - Replace with your recipient email address.
- **SMTP credentials** - Replace smtp_username and smtp_password with your Oracle Cloud Infrastructure SMTP username and password generated in the console.
- **HOST** - Replace with the Email Delivery SMTP endpoint. For example, smtp.us-ashburn-1.oraclecloud.com.

10. Refer to the requirements for configuring an SMTP connection with Email Delivery. TLSv1.2 is required for Email Delivery. Some default settings of Javamail need to be disabled. For example, JavaMail authorizes in a certain order. The default authorization order is "LOGIN PLAIN DIGEST-MD5 NTLM". Since Email Delivery authorizes as "PLAIN", "LOGIN" needs to be disabled. For example, the following code is entered in OCIemail.java file to configure the SMTP connection:

```
//props.put("mail.smtp.ssl.enable", "true"); //default is false if not set
props.put("mail.smtp.auth", "true");
props.put("mail.smtp.auth.login.disable", "true");
props.put("mail.smtp.starttls.enable", "true");
props.put("mail.smtp.starttls.required", "true");
```

11. Open the File menu and click **Save**.
12. To build the project, open the **Project** menu and then select **Build Project**. If this option is disabled, you may have automatic building enabled.
13. To start the program and send the email, open the **Run** menu and then click **Run**.
14. Review the output. If the email was successfully sent, the console displays "Email sent successfully!" Otherwise, it displays an error message.
15. Log into the recipient inbox to verify receipt of the email.

**More Information**

- See the JavaMail documentation for more information.
- There is a known issue that can cause an error. See **JavaMail issues occur when multiple recipients are set in an email and one or more of the email addresses are suppressed.**

**Integrating Sendmail with Email Delivery**

**Configure Sendmail to Send Email Through Email Delivery**

You can use Sendmail to send emails through Email Delivery. Before you use Sendmail you must configure Oracle Cloud Infrastructure Email Delivery in your Sendmail application.
To enable Sendmail to integrate with Email Delivery:

1. Make sure Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

2. Run the following update and install commands:

   ```
   sudo apt update
   sudo apt install sendmail
   sudo apt install m4
   ```

3. In a file editor such as vi, update `/etc/mail/authinfo`. Run the following command:

   ```
   sudo vi /etc/mail/authinfo
   ```

   Add the following line:

   ```
   AuthInfo:<SMTP connection endpoint> "U:root" "I:<username from smtp credentials>" "P:<password from smtp credentials>" "M:PLAIN"
   #write and quit file
   :wq!
   ```

4. Generate the `/etc/mail/authinfo.db` file.

   Run the following command:

   ```
   sudo sh -c 'makemap hash /etc/mail/authinfo.db < /etc/mail/authinfo'
   ```

5. Add support for relaying to the Oracle Cloud Infrastructure Email Delivery SMTP endpoint.

   Run the following command:

   ```
   sudo sh -c 'echo "Connect:<SMTP connection endpoint> RELAY" >> /etc/mail/access'
   ```

6. Regenerate `/etc/mail/access.db`.

   Run the following command:

   ```
   sudo sh -c 'makemap hash /etc/mail/access.db < /etc/mail/access'
   ```

7. Create a backup of the `sendmail.cf` and `sendmail.mc` files.

   Run the following command:

   ```
   sudo sh -c 'cp /etc/mail/sendmail.cf /etc/mail/sendmail_cf.backup && cp /etc/mail/sendmail.mc /etc/mail/sendmail_mc.backup'
   ```
8. Update the `/etc/mail/sendmail.mc` file.

   Run the following command:

   ```sh
sudo vi /etc/mail/sendmail.mc
   ```

   Find the MAILER() definitions.

   Type `/MAILER` and press ENTER.

   In Insert mode, add the following settings before any MAILER() definitions:

   ```
   define(`SMART_HOST', `<SMTP connection endpoint>')
   define(`RELAY_MAILER_ARGS', `TCP $h 25')
   define(`confAUTH_MECHANISMS', `LOGIN PLAIN')
   FEATURE(`authinfo', `hash -o /etc/mail/authinfo.db')
   MASQUERADE_AS(`<sending_domain>')
   FEATURE(`masquerade_envelope')
   FEATURE(`masquerade_entire_domain')
   ```

   Disable Insert mode.

   Run the following command:

   ```sh
   #write and quit file
   :wq!
   ```


   Run the following command:

   ```sh
   sudo chmod 666 /etc/mail/sendmail.cf
   ```

10. Regenerate `sendmail.cf`.

    Run the following command:

    ```sh
    sudo sh -c 'm4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf'
    ```

    **Note:**

    If you receive an error, such as "Command not found" or "No such file or directory," confirm that the `m4` and `sendmail` packages are installed on your system.

11. Reset permissions for `sendmail.cf` to read only.

    Run the following command:

    ```sh
    sudo chmod 644 /etc/mail/sendmail.cf
    ```

12. Restart Sendmail.

    Run the following command:

    ```sh
    sudo /etc/init.d/sendmail restart
    ```
13. Test the configuration by sending a test email.
   Run the following command:
   
   ```
   /usr/sbin/sendmail -vf <from_email_address> <recipient_email_address>
   ```
   
Enter the details of the email. After each line press `Enter`.
   For example:
   
   ```
   From: <from_email_address>
   To: <recipient_email_address>
   Subject: OCI Email Delivery test email
   This is a test message sent from OCI Email Delivery using Sendmail.
   ```
   
   Press `Ctrl + D` to send the email.

14. Verify receipt of the test email.

   **Note:**
   You can troubleshoot an issue by reviewing the Sendmail log on your mail server, located at `/var/log/mail.log`.

**More Information**

- For more information, see the [Sendmail Installation and Operation Guide](#).

### Integrating PeopleSoft with Email Delivery

#### Configure PeopleSoft to Send Email Through Email Delivery

You can use PeopleSoft to send emails through Email Delivery. Before you use PeopleSoft, you must configure Oracle Cloud Infrastructure Email Delivery in your PeopleSoft application.

**Note:**

The following steps require familiarity with人民Soft documentation. (This link points to PeopleTools 8.57, which is the latest version at the time this article was published. Please refer to the documentation for your specific PeopleTools version.)

To enable PeopleSoft to integrate with Email Delivery:

1. Make sure Email Delivery is configured to send email. See [Getting Started with Email Delivery](#) on page 1743.

   **Note:**
   SMTP credentials are required to configure PeopleSoft to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.

2. Run the following command to view the certificate chain:

   ```
   echo | openssl s_client -starttls smtp -crlf -connect <SMTP-endpoint>:587
   ```

   Example output:

   ```
   [root@ociuvddatg01 ~]# echo | openssl s_client -starttls smtp -crlf -connect smtp.email.us-ashburn-1.oci.oraclecloud.com:587
   CONNECTED(00000003)
   depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
   verify return:1
   ```
3. Extract the certificate that signed your domain. In this example, this is the last certificate (2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2). Copy and paste the certificate into a separate DigiCert.pem file, including the BEGIN CERTIFICATE and END CERTIFICATE fields.

4. Add the certificates to the PeopleSoft application.
   Log into the Pure Internet Architecture (PIA) as user "PS" and import the certificates into the target environment. See Installing Application Server-Based Digital Certificates and refer to the Adding CA Authorities and Installing Root Certificates section.

5. Encrypt the SMTP password in the config file.
   You can encrypt the SMTP password using the PIA or the PSCipher utility.

   **Using the PIA**
   a. Open the navigation menu on the PeopleSoft dashboard. Go to PeopleTools, and then select Integration Broker.
   b. Select Configuration, and then click Gateways. Select the default LOCAL gateway.
   c. Click Gateway Setup Properties. The default user ID is administrator and the default password is the password selected during setup.
   d. Click the Advanced Properties Page link.
   e. Click Password Encryption at the bottom of the page. This is where you will encrypt your password.

   **Using PSCipher**
   The PSCipher utility can be found under $PS_CFG_HOME/webserv/<DOMAIN>/piabin where <DOMAIN> is your web server domain.
   Run the following command:

   ```bash
   ./PSCipher.sh <password>
   ```

   **Note:**
   The password can have special characters so you will need to enclose the password in single quotes. For example: ./PSCipher.sh
   ```bash
   '#rpassword$){'
   ```
6. Update the SMTP settings on the PeopleSoft Application server. For more information, see SMTP Settings in the PeopleSoft documentation.

Establish an ssh connection to the PeopleSoft Application server machine (as username "opc") and do the following:

a. Switch user to psadm2 (for example, sudo su - psadm2).

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>psadm2 is the PeopleTools domain user who creates and configures the Application Server domain.</td>
</tr>
</tbody>
</table>

b. Navigate to the Appserver configuration directory.

Run the following command:

```
$ cd $PS_CFG_HOME/appserv/APPDOM
```

c. Back up the original psappsrv.cfg file.

d. Add the following information to the psappsrv.cfg file:

```
SMTPServer=<SMTP connection endpoint>
SMTPUserName=<username from SMTP credentials>
SMTPUserPassword=<encrypted SMTP password>
SMTPPort=587
SMTPUseSSL=N
SMTPSSLPort=587
SMTPTLSEnable=true
SMTPTLSRequired=true
```

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not include a space between the &quot;=&quot; and the values because the space could be counted in the value for the password, causing an authentication failure.</td>
</tr>
</tbody>
</table>

7. Add the primary email address for the PeopleSoft application user who is trying to send notification from within the application. In this example, the user is "PS".

Log in as "PS" and do the following:

a. Open the navigation menu on the PeopleSoft dashboard. Go to PeopleTools, and then select Security.

b. Select User Profiles, and then click user Profiles. Find the profile for "PS".

c. On the General tab, click Edit Email Addresses.

d. Enter the approved sender email address as the primary email address.

8. Log out of the PeopleSoft application.

9. Reboot the application server using the PSADMIN utility. See Using the Application Server Administration Menu.

10. Test the email notification delivery.

Log into the PIA as "PS", and select Notify anywhere in the console. For example, you can do the following:

a. Go to Peopletools, and then select Web Profile.

b. Select Web Profile Configuration.

c. Click Search, and then click PROD in the search results.

d. Click Notify, enter the notification details, and then click OK.

Confirm receipt of the test email.

To debug SMTP errors (optional):
1. You can add the following parameter to help with SMTP debugging: `SMTPTrace=1`
   
   LogFence should be set to 5 to use this parameter. The system writes the log information to SMTP<DDMM>.log in `%PS_SERVDIR%/LOGS` by default, or the custom value set for Log Directory.
   
   For example:
   ```
   $PS_CFG_HOME\APPSERV\domain\LOGS\SMTP6_27.log
   ```

2. After you set this parameter, you will need to reboot the Application server. Once this parameter is set, you can monitor the SMTP log.

3. Type `ls` and find the SMTP file for the date you sent the email.

4. Run the following command:
   ```
   tail -f <smtp log file and date>
   ```
   
   For example,
   ```
   tail -f SMTP9_17.log
   ```
   
   Search for any errors in the output.

**Troubleshooting**

*535 authentication required error occurs when sending email*

To troubleshoot this issue, complete the following steps:

1. Use the following method to re-encrypt the SMTP user password, and enter it in the PeopleSoft application server or process scheduler configuration file's SMTP settings.
   
   a. Open any Integration Broker node by navigating to **PeopleTools, Integration Broker, Integration Setup**, and then click **Nodes**.
   
   b. Click on the **Connectors** tab. Ensure it is using the HTTPTARGET Connector.
   
   c. Expand the encryption section and encrypt the SMTP user password again.
   
   d. Enter the new encrypted password in the SMTPUserPassword settings.

2. Verify that the optional parameters below are set in the SMTP settings section of the configuration file even if they are not being used.
   ```
   SMTPUseSSL1=N
   SMTPSSLPor1t1=587
   SMTPTLSEnable1=true
   SMTPTLSRequired1=true
   SMTPClientCertAlias1=
   ```

**More Information**

- **SMTP Settings (PeopleSoft)**
- **Encrypting Passwords in the PeopleSoft Pure Internet Architecture**
- **My Oracle Support: Is There a Way to Both Authenticate And Secure Emails From PeopleSoft?**

**Integrating Python with Email Delivery**

You can use Python to send emails through Email Delivery. Before you can send email you must configure Email Delivery in Python.

**Note:**

These steps assume you are logged into an Oracle Linux instance. Other distributions of Linux may have different commands and file locations.
Configure Python to Send Email Through Email Delivery

To enable Python to test the configuration of Email Delivery:

1. Ensure Email Delivery is configured to send email. See Getting Started with Email Delivery on page 1743.

   **Note:**
   The SMTP credentials are required to configure Python to use Email Delivery. Be sure to note the user name and password when you generate the SMTP credentials.

2. Ensure Python is installed. The installation process differs depending on which operating system you are using. For example, run the following command to install Python on Oracle Linux:

   ```bash
   sudo yum install python3 -y
   ```

3. In a file editor such as vi, create a python script to test Email Delivery.

   Run the following command:

   ```bash
   sudo vi ociemail.py
   ```

4. In the `ociemail.py` file, replace the variables with your own values.

   For example:

   ```python
   # python script for sending SMTP configuration with Oracle Cloud Infrastructure Email Delivery
   import smtplib
   import email.utils
   from email.message import EmailMessage
   import ssl

   # Replace sender@example.com with your "From" address.
   # This address must be verified.
   # this is the approved sender email
   SENDER = 'sender@example.com'
   SENDERNAME = 'Sender Name'

   # Replace recipient@example.com with a "To" address. If your account
   # is still in the sandbox, this address must be verified.
   RECIPIENT = 'recipient@example.com'

   # Replace the USERNAME_SMTP value with your Email Delivery SMTP username.
   USERNAME_SMTP = '
ocid1.user.oc1..<unique_ID>@ocid1.tenancy.oc1..<unique_ID>.vf.com'

   # Put the PASSWORD value from your Email Delivery SMTP password into the
   # following file.
   PASSWORD_SMTP_FILE = 'ociemail.config'

   # If you're using Email Delivery in a different region, replace the HOST
   # value with an appropriate SMTP endpoint.
   # Use port 25 or 587 to connect to the SMTP endpoint.
   HOST = "smtp.us-ashburn-1.oraclecloud.com"
   PORT = 587

   # The subject line of the email.
   SUBJECT = 'Email Delivery Test (Python smtplib)'

   # The email body for recipients with non-HTML email clients.
   BODY_TEXT = "Email Delivery Test\r\n" "This email was sent through the Email Delivery SMTP " "Interface using the Python smtplib package."
   ```
Email Delivery

# The HTML body of the email.
BODY_HTML = """"<html>
<head></head>
<body>
<h1>Email Delivery SMTP Email Test</h1>
<p>This email was sent with Email Delivery using the
<a href='https://www.python.org/'>Python</a>
<a href='https://docs.python.org/3/library/smtplib.html'>smtplib</a> library.</p>
</body>
</html>"

# get the password from a named config file ociemail.config
with open(PASSWORD_SMTP_FILE) as f:
    password_smtp = f.readline().strip()

# create message container
msg = EmailMessage()
msg['Subject'] = SUBJECT
msg['From'] = email.utils.formataddr((SENDERNAME, SENDER))
msg['To'] = RECIPIENT

# make the message multi-part alternative, making the content the first part
msg.add_alternative(BODY_TEXT, subtype='text')
# this adds the additional part to the message
# According to RFC 2046, the last part of a multipart message, in this case
# the HTML message, is best and preferred.
msg.add_alternative(BODY_HTML, subtype='html')

# Try to send the message.
try:
    server = smtplib.SMTP(HOST, PORT)
    server.ehlo()
    # most python runtimes default to a set of trusted public CAs that will include the CA used by OCI Email Delivery.
    # However, on platforms lacking that default (or with an outdated set of CAs), customers may need to provide a capath that includes our public CA.
    server.starttls(context=ssl.create_default_context(purpose=ssl.Purpose.SERVER_AUTH, cafile=None, capath=None))
    # smtplib docs recommend calling ehlo() before & after starttls()
    server.ehlo()
    server.login(USERNAME_SMTP, password_smtp)
    # our requirement is that SENDER is the same as From address set previously
    server.sendmail(SENDER, RECIPIENT, msg.as_string())
    server.close()
except Exception as e:
    print(f"Error: {e}")
else:
    print("Email successfully sent!")

Note:
Python 2 and legacy email APIs should not be used with Email Delivery.
5. In a file editor such as vi, create a file that contains the SMTP password. Run the following command and replace the contents with your SMTP password:

```bash
sudo vi ociemail.config
```

6. To send a test email with Python, run the following command from the directory the script is located in:

```bash
python3 ociemail.py
```

**More Information**

- More Python script examples can be found on [GitHub](https://github.com).

**Troubleshooting Email Delivery**

This topic provides troubleshooting solutions for problems you might encounter using Email Delivery.

**TLS errors when integrating with Postfix**

- If you are encountering TLS errors when attempting to integrate Postfix with Email Delivery, ensure that the following setting is removed from the Postfix `main.cf` file, as it has been deprecated:

  ```
  smtp_use_tls = yes
  ```

- Use the following setting instead to turn on TLS:

  ```
  smtp_tls_security_level = may
  ```

  Using this setting, the Postfix SMTP server announces STARTTLS support to remote SMTP clients, but does not require that clients use TLS encryption.

- If you want to enforce the use of TLS, so that the Postfix SMTP server announces STARTTLS and accepts no mail without TLS encryption, use the following setting:

  ```
  smtp_tls_security_level = encrypt
  ```

  For more information, see [Postfix TLS Support](https://www.postfix.org/tls.html).

**Connectivity Issues**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Delivery does not prohibit connectivity from any source IP range. Any IP that attempts to connect to Email Delivery will be accepted.</td>
</tr>
</tbody>
</table>

Refer to [Configure SMTP Connection](https://docs.oracle.com/en-us/iaas/Content/Email FAMILY/Concepts/ociemail.htm#ociemail_connection) on page 1753 for a list of regional endpoints to establish SMTP connections for sending.

**To troubleshoot a problem connecting to endpoint network ports**

- Ensure that you have the correct endpoint DNS name or IP address for the region and that you have been allowlisted to use the endpoint.
Email Delivery

- Test connectivity to the endpoint using port 25 or 587. Use a utility such as Telnet or netcat to attempt to connect to the port manually.
  
  1. Open a command prompt.
  2. Use the following command to test the network connection.

```
telnet <SMTP endpoint> <port>
```

For example:

```
telnet smtp.us-ashburn-1.oraclecloud.com 25
```

The port is open and the test is successful if a blank screen appears. If you are unable to connect to the ports using telnet, you are experiencing a network connectivity issue.

**To troubleshoot a problem connecting to an external mail transfer agent (MTA)**

Use the following steps to determine whether you are able to communicate with an external service on the required ports 25 or 587. If you are unable to connect successfully, you are experiencing a network connectivity issue. If you are able to connect to an external MTA, the network connectivity issue is within Oracle Cloud Infrastructure.

- Connect to an external MTA such as Google's mail exchangers.
  
  1. Open a command prompt.
  2. Use the following command to retrieve one of Google's MX server records.

```
dig MX google.com
```

3. Use the following command to test connectivity to the endpoint port 25 or 587 against Google's MX servers.

```
telnet <IP address> <port>
```

If you are unable to connect to Google's MX servers, this confirms that you are having issues connecting to mail servers (port 25 or 587). It is possible that your egress rules are filtering traffic at the VCN.

If you can connect to an external MTA (that is, you are able to communicate with a public SMTP endpoint on the correct ports) but you cannot connect to Email Delivery public SMTP endpoints on those ports, create a service request with My Oracle Support with this information.

**Common Errors Returned by Email Delivery**

**API Errors**

For a complete list of common errors returned by all the services for Oracle Cloud Infrastructure, see API Errors.

**Common SMTP Errors Returned by Email Delivery**

The following table lists the common errors returned by the Email Delivery SMTP service.

<table>
<thead>
<tr>
<th>SMTP Status Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>254</td>
<td>4.7.1</td>
<td>Message has been accepted but a status code was returned indicating suppression. Enhanced Status Code 4.7.1 indicated a persistent transient failure (RFC3463).</td>
</tr>
<tr>
<td></td>
<td>Suppression for user &lt;user ocid&gt; to &lt;recpt&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 1777
<table>
<thead>
<tr>
<th>SMTP Status Code</th>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>421</td>
<td>421</td>
<td>Timeout waiting for data from client</td>
</tr>
<tr>
<td>421</td>
<td>4.4.0</td>
<td>Problem attempting to execute commands. Please try again later</td>
</tr>
<tr>
<td>421</td>
<td></td>
<td>Too many connections, try again later</td>
</tr>
<tr>
<td>421</td>
<td>4.3.0</td>
<td>Mail system failure, closing transmission channel</td>
</tr>
<tr>
<td>451</td>
<td></td>
<td>Server error An unexpected error has occurred during the SMTP conversation.</td>
</tr>
<tr>
<td>451</td>
<td></td>
<td>Error in Processing An unexpected error has occurred during the SMTP conversation.</td>
</tr>
<tr>
<td>452</td>
<td></td>
<td>System storage error The server is unable to persist the message in its delivery queue.</td>
</tr>
<tr>
<td>455</td>
<td>Maximum messages sent per minute reached : limit is &lt;limit&gt;</td>
<td>The SMTP send burst rate (of messages accepted per minute period) has been exceeded.</td>
</tr>
<tr>
<td>455</td>
<td>Maximum messages sent per day reached : limit is &lt;limit&gt;</td>
<td>The SMTP daily send rate (of messages accepted per 24 hour period) has been exceeded.</td>
</tr>
<tr>
<td>471</td>
<td>Authorization failed: address &lt;address&gt; not authorized</td>
<td>Authorization of the address (either in the envelope or message) has failed for the SMTP user.</td>
</tr>
<tr>
<td>SMTP Status Code</td>
<td>Error Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>501</td>
<td>501</td>
<td>Invalid command argument, not a valid Base64 string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The base64 encoded AUTH (PLAIN) secret is invalid.</td>
</tr>
<tr>
<td>501</td>
<td>501</td>
<td>Invalid command argument, does not contain NUL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The base64 encoded AUTH (PLAIN) secret does not contain NUL field separator(s).</td>
</tr>
<tr>
<td>501</td>
<td>501</td>
<td>Invalid command argument, does not contain the second NUL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The base64 encoded AUTH (PLAIN) secret does not contain NUL field separator(s).</td>
</tr>
<tr>
<td>504</td>
<td></td>
<td>Method not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client has attempted to use an unsupported AUTH mechanism with our service.</td>
</tr>
<tr>
<td>504</td>
<td></td>
<td>AUTH mechanism mismatch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client has sent an invalid AUTH command to our service.</td>
</tr>
<tr>
<td>523</td>
<td></td>
<td>Exceeds byte limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The message has exceeded the size limit enforced by the service (see server response to EHLO for size restriction).</td>
</tr>
<tr>
<td>535</td>
<td></td>
<td>Authentication credentials invalid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication of the SMTP user has failed.</td>
</tr>
<tr>
<td>535</td>
<td></td>
<td>Authentication required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client has sent commands that require SMTP authentication succeeded before the service is able to process (that is, commands are being sent out of order).</td>
</tr>
<tr>
<td>553</td>
<td></td>
<td>&lt;address&gt; Invalid email address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The RFC-822 Internet Address sent by the client is invalid.</td>
</tr>
<tr>
<td>554</td>
<td></td>
<td>Message parse error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The RFC-2822 Internet Message is invalid (and unable to be parsed by the server).</td>
</tr>
</tbody>
</table>

**Service Limits**

For Email Delivery limits issues, see Email Delivery Service Capabilities and Limits and Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

**Troubleshooting Undelivered Emails**

The following issues can cause an email to be undelivered:

- The recipient is on the Suppression List.
- An authentication failure or an issue with the format of the email message occurred. For example, if the SMTP "From" address is not the same as the "From" address in the email body, the email is rejected. The addresses must match and be an Approved Sender. Refer to your sending application’s logs to review any issues.
Refer to Deliverability Best Practices to learn about recommendations that can help lower your email bounce rate, stay off blocklists, lower your complaint rate, and improve your email sender reputation.

If you are unable to resolve the issue, you can go to My Oracle Support and create a service request. See 4. Open a support service request on page 126 for more information.

Deliverability Best Practices

Deliverability Best Practices help you to learn and manage the habits that affect your sending reputation. These recommendations can help lower your email bounce rate, stay off blocklists, lower your complaint rate, and improve your email sender reputation.

Implement an Opt-in Process

An opt-in process is a method for your users to subscribe to your mailing list, which gives you permission to send messages. Only send messages to subscribers who have opted-in to your mailing list. There are two types of opt-in procedures.

- **Single opt-in (unconfirmed):** A user provides their email address and gives permission to receive relevant messages. Once the address is provided, messages can be sent without confirming the email address belongs to the user who provided it.

- **Double opt-in (confirmed):** A user provides their email address, but before the first mailing, a confirmation email is sent to the account owner. The email requires action from the account owner to confirm that future messages are wanted. An account can be verified by having the owner click a link for reply to the email. The confirmation email ensures that the address was not added to a third-party mailing list without consent.

Purge Unengaged Users

Remove unengaged users by implementing a process. If a recipient is not engaging with your mail by either opening or clicking the email, this might be an indication that the email account is not in use or that the recipient is no longer interested in your content. If the recipient does not use the email account, eventually the mailbox provider terminates the account or transforms the account into a spam trap. Remove recipients who have not engaged with your email in a time frame defined by your business model. Purging unengaged users helps your deliverability by increasing your user engagement rate.

Review Your Subscriber List

When reviewing your subscriber list, keep these things in mind:

- Eliminate duplicate addresses before sending. If addresses that do not exist are mailed to multiple times, your hard bounce rate could be inflated.
- Ensure that a previous suppression list (possibly from another email service provider) was not accidentally included.
- Verify that subscribers have opted-in. Do not send to an old list that you found.
- Restrict users from uploading their email client’s contact list in a “select all” fashion. Forcing users to select addresses individually prevents users from accidentally including potentially out of date or expired addresses.

Evaluate Your Sending Frequency

Sending too many emails in a short time might aggravate recipients, causing the recipients to mark your messages as spam. This is called list fatigue. Ensure that your message cadence aligns with the expected frequency of your content. Reducing frequency might reduce spam complaints. Ensure that your content is relevant to your subscribers. Keep your email messages consistent to your audience. A person who subscribed to a list for coupon updates might not want regular emails about auto loan finance rates. These unexpected messages are likely to be marked as spam, which decreases your sender reputation.
Easily Accessible Unsubscribe URL

Unsubscribing helps your inbox success by sending only to recipients that engage by opening or clicking. When people complain, your sending reputation is harmed. Make it easy for recipients to be removed from the list. Do not hide the unsubscribe URL at the bottom of the message. A small percentage of users scroll to the bottom of the email and search for a small URL. Most users mark the email as spam.

Canadian Anti-Spam Law (CASL) Guide

Canada's Anti-Spam Law (CASL) is one of the best guides to ensuring your compliance with the law, users’ desire, and the intended filtering that most mailbox providers use. If you are a Canadian email sender or you send email to Canadian residents, you must comply with CASL. The following information is intended to help provide you with some guidance for complying with CASL. This article does not constitute legal advice, nor is it intended supplement or otherwise affect your rights or obligations under your service agreement with Oracle, including your obligations under Oracle’s Acceptable Use Policy. If you have questions about CASL or the legality of your sending practices, we encourage you to speak with an attorney who specializes in that subject matter.

What is covered by CASL?

CASL and its related regulations apply to any “commercial electronic message” sent from or to Canadian computers and devices in Canada. Electronic messages that are merely routed through Canadian computer systems are not subject to CASL.

A “commercial electronic message” is any message that:

- Is in an electronic format, including emails, instant messages, text messages, and some social media communications.
- Is sent to an electronic address, including email addresses, instant message accounts, phone accounts, and social media accounts; and
- Contains a message encouraging recipients to take part in some type of commercial activity, including the promotion of products, services, people/personas, companies, or organizations.

Are there any types of messages that are exempt from CASL?

These types of electronic messages are exempt from CASL for various reasons.

- Messages to family or a person with established personal relationship.
- Messages to an employee, consultant, or person associated with your business.
- Responses to a current customer, or someone who has inquired in the last six months.
- Messages that will be opened or accessed in a foreign country, including the U.S., China, and most of Europe.
- Messages sent on behalf of a charity or political organization for the purposes of raising funds or soliciting contributions.
- Messages attempting to enforce a legal right or court order.
- Messages that provide warranty, recall, safety, or security information about a product or service purchased by the recipient.
- Messages that provide information about a purchase, subscription, membership, account, loan, or other ongoing relationship, including delivery of product updates or upgrades.
- A single message to a recipient without an existing relationship based on a referral. The full name of the referring person must be disclosed in the message. The referrer might be family or have another relationship with the person to whom you are sending.

If your message does not meet one of these criteria, consent is required under CASL. Not all of the previous messages listed are permitted under the Oracle Cloud Hosting and Delivery Policy.

What is “express consent”?

Under CASL, “express consent” means a written or oral agreement to receive specific types of messages. For example, “You want to receive monthly newsletters and weekly discount notifications from Oracle”.

Express consent is only valid if your request for consent clearly and simply describes the following information:
Email Delivery

- Your purpose in obtaining consent.
- A description of messages you will be sending.
- The name and contact information (physical mailing address and telephone number, email address, or website URL) of the requestor.
- A statement that the recipient can unsubscribe at any time.

The requestor can be you or someone for whom you are asking. If you are requesting consent on behalf of a client, the name and contact information of the client must be included with the consent request.

What is “implied consent”?
Under CASL, you can only obtain implied consent when certain circumstances exist, including when:

- A recipient has purchased a product, service or made another business deal, contract, or membership with your organization in the last 24 months.
- You are a registered charity or political organization, and the recipient has made a donation or gift, has volunteered, or attended a meeting organized by you.
- A professional message is sent to someone whose email address was given to you, or is conspicuously published, and who has not published or told you that unsolicited messages are not wanted.

What type of consent is required?
After July 1, 2017, you can only send to recipients with express consent or whose implied consent is valid under CASL.

Some additional requirements
In addition to understanding what qualifies as CASL-regulated message, and what type of consent is needed, there are a few other details to keep in mind.

- Retention of a record of consent confirmations is required.
- When requesting consent, checkboxes cannot be pre-filled to suggest consent. Each subscriber must check the box themselves for consent to be valid.
- All messages sent must include the following:
  - your name
  - the person on whose behalf you are sending (if any)
  - your physical mailing address and telephone number
  - your email address or website URL
- All messages sent after consent must also include an unsubscribe mechanism, and unsubscribes must be processed within ten days.

Where can I find more information on CASL?
The full text of the law can be found on the website for the Canadian Justice Department. The Canadian Radio and Telecommunications Commission has also set up an FAQ page and some guidelines for obtaining consent. If you have any questions, we encourage you to contact an attorney who is familiar with the law.

Oracle Cloud Hosting and Delivery Policy
Often, the Oracle Cloud Hosting and Delivery Policy is more stringent than CASL requirements. It is important that you review Oracle policies before using the service.

Troubleshooting Undelivered Emails
The following issues can cause an email to be undelivered:

- The recipient is on the Suppression List.
- An authentication failure or an issue with the format of the email message occurred. For example, if the SMTP "From" address is not the same as the "From" address in the email body, the email is rejected. The addresses must match and be an Approved Sender. Refer to your sending application’s logs to review any issues.
If you are unable to resolve the issue, you can go to My Oracle Support and create a service request. See Creating a Service Request Using the Console for more information.
Chapter 17

Events

This chapter explains how to create automation in your tenancy.

Overview of Events

Oracle Cloud Infrastructure Events enables you to create automation based on the state changes of resources throughout your tenancy. Use Events to allow your development teams to automatically respond when a resource changes its state.

Here are some examples of how you might use Events:

- Send a notification to a DevOps team when a database backup completes.
- Convert files of one format to another when files are uploaded to an Object Storage bucket.

How Events Works

Oracle Cloud Infrastructure services emit events, which are structured messages that indicate changes in resources. Events (the messages, not the service) follow the CloudEvents industry standard format hosted by the Cloud Native Computing Foundation (CNCF). This standard allows for interoperability between various cloud providers or on-premises systems and cloud providers. An event could be a create, read, update, or delete (CRUD) operation, a resource lifecycle state change, or a system event impacting a resource. For example, an event can be emitted when a backup completes or fails, or a file in an Object Storage bucket is added, updated, or deleted.

Services emit events for resources or data. For example, Object Storage emits events for buckets and objects. Services emit different types of events for resources, which are distinguished as event types. Buckets and objects have event types of create, update, and delete, for example. Event types are the changes that produce events by a given resource. For a list of services that produce events and the event types that those services track, see Services that Produce Events on page 1817.

You work with events by creating rules. Rules include a filter you define to specify events produced by the resources in your tenancy. The filter is flexible:

- You can define filters that match only certain events or all events.
- You can define filters based on the way resources are tagged or the presence of specific values in attributes from the event itself.

Rules must also specify an action to trigger when the filter finds a matching event. Actions are responses you define for event matches. You set up select Oracle Cloud Infrastructure services that the Events service has established as actions (more on these select services follows). The resources for these services act as destinations for matching events. When the filter in the rule finds a match, the Events service delivers the matching event to one or more of the destinations you identified in the rule. The destination service that receives the event then processes the event in whatever manner you defined. This delivery provides the automation in your environment.

You can only deliver events to certain Oracle Cloud Infrastructure services with a rule. Use the following services to create actions:

- Notifications
- Streaming
Events Concepts

The following concepts are essential to working with Events.

**EVENTS**

An automatic notification of a state change as reported by an event-emitting Oracle Cloud Infrastructure resource. For example, an database resource emits a `backup.begin` event when a backup begins.

**EVENT TYPES**

A distinction between the different types of events. For more information, see Services that Produce Events on page 1817.

**RULES**

A JSON object you create to subscribe to an event type and trigger an action should that event occur. For example, a rule might specify that `backup.end` event types from databases trigger the Notifications service to send an email to a particular DevOps engineer. For more information, see Matching Events with Filters on page 1796.

**ACTIONS**

Rules must also specify an action to trigger when the filter finds a matching event. Actions are responses you define for event matches. You set up select Oracle Cloud Infrastructure services that the Events service has established as actions. The resources for these services act as destinations for matching events. When the filter in the rule finds a match, the Events service delivers the matching event to one or more of the destinations you identified in the rule. The destination service that receives the event then processes the event in whatever manner you defined. This delivery provides the automation in your environment.

You can only deliver events to certain Oracle Cloud Infrastructure services with a rule. Use the following services to create actions:

- Notifications
- Streaming
- Functions
Events

Region Availability

Events is currently available in all regions of the commercial realm. Events is currently not available in regions within the Government Cloud realm.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Administrators: You must write IAM policy that authorize users to work with rules. For more information, see Events and IAM Policies on page 1801.

Limits on Events Resources

The Events service has a limitation of 50 rules per tenancy.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Service Gateway and Events

The Events service also supports private access from Oracle Cloud Infrastructure resources in a VCN through a service gateway. A service gateway allows connectivity to the Events public endpoints from private IP addresses in private subnets. For example, you can manage rules over the Oracle Cloud Infrastructure backbone instead of over the internet. You can optionally use IAM policies to control which VCNs or ranges of IP addresses can access Events. See Access to Oracle Services: Service Gateway on page 3256 for details.

Getting Started with Events

This topic introduces you to creating automation with Events. You create a simple rule that sends a notification whenever someone creates a bucket in a particular compartment in your tenancy.

Setting Up for Events

To try out the Events service for this tutorial, you must have these things set up first:

- Create IAM policy for Events
Events

- Create a topic and subscription to use as an action

**Important:**

A tenancy administrator must configure your tenancy for Events. These configurations give you access to an Oracle Cloud Infrastructure tenancy with the necessary IAM policy and a resource to use as an action.

Create Users, Groups, and Compartments

You can use existing users, groups, and compartments or make new ones.

**To create groups and users**

If suitable users and groups for assigning users permissions to work with rules don't already exist, log in to the Console as a tenancy administrator and create them.

1. Log in to the Console as a tenancy administrator.
2. If you need a group for Events, perform these steps:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups. A list of the groups in your tenancy is displayed.
   b. Click Create Group and create a new group (see To create a group on page 2420). Give the group a meaningful name and description. Avoid entering confidential information.
3. If you need user accounts for Events, perform these steps:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of
      the users in your tenancy is displayed.
   b. Click Create User and create one or more new users (see To create a user on page 2417).

4. If users haven't been added to groups already, perform these steps:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups. A list
      of the groups in your tenancy is displayed.
   b. Click the group you want to use for Events.
   c. Click Add User to Group.
   d. Select the users from the drop-down list, and then click Add.

To create a compartment

If suitable compartment for rules and the resources that emit events doesn't already exist, log in to the Console as a
tenancy administrator and create it.

1. Log in to the Console as a tenancy administrator.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A
   list of the compartments in your tenancy is displayed.
3. Click **Create Compartment** and create a new compartment (see To create a compartment on page 2442). Give the compartment a meaningful name and description. Avoid entering confidential information.

### Create IAM Policy for Events

Before users can start using Events to create automation, as a tenancy administrator you must create IAM policy:

**To create a policy that allows users to create and manage rules**

1. Log in to the Console as a tenancy administrator.
2. In the Console, open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**. A list of the policies in the compartment you're viewing is displayed.
3. Select the root compartment.
4. Click **Create Policy**.
5. Enter the following:
   - **Name**: A meaningful name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
   - **Description**: A meaningful description. You can change this later if you want to.
   - **Statement**: Enter the following policy statements to give users in the group the ability to manage and create rules:
     - This line gives the user inspect access to resources in compartments to select actions.
     ```plaintext
     allow group <RuleAdmins> to inspect compartments in tenancy
     ```
     - This line gives the user access to defined tags to apply filter tags to rules.
     ```plaintext
     allow group <RuleAdmins> to use tag-namespaces in tenancy
     ```
     - These lines give the user access to Streaming resources for actions
     ```plaintext
     allow group <RuleAdmins> to inspect streams in tenancy
     allow group <RuleAdmins> to use stream-push in tenancy
     allow group <RuleAdmins> to use stream-pull in tenancy
     ```
     - These lines give the user access to Functions resources for actions.
     ```plaintext
     allow group <RuleAdmins> to use virtual-network-family in tenancy
     ```
allow group <RuleAdmins> to manage function-family in tenancy

This line gives the user access to Notifications topics for actions.

allow group <RuleAdmins> to use ons-topic in tenancy

This line gives the user manage access to rules for Events.

allow group <RuleAdmins> to manage cloudevents-rules in tenancy

6. Click Create.

Create Notifications Topic and Subscription

If a suitable Notifications topic doesn't already exist, then you must log in to the Console as a tenancy administrator and create it. Whether you use an existing topic or create a new one, add an email address as a subscription so that you can monitor that email account for notifications.

To create a topic

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Click Create Topic at the top of the topic list.

3. In the Create Topic dialog box, configure your topic.
   - Name: Required. Specify a friendly name for the topic. It must be unique; validation is case-sensitive. Avoid entering confidential information.
   - Description: Optional. Enter a description for the topic.
4. Click Create.

To create a subscription

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Click the name of the topic that you created in the previous step or the topic you intend to use for this tutorial.
3. On the topic detail page, click **Create Subscription**.

![Create Subscription Dialog Box](image)

4. In the **Create Subscription** dialog box, select **Email**, and then type an email address.

5. Click **Create**.

The subscription has been created and a subscription confirmation URL will be sent. The subscription remains in "Pending" status until it has been confirmed.

To confirm a subscription

- In the confirmation email sent to the address you specified in the previous procedure, click the confirmation URL.

Using the Console to Create a Rule

Use the Console to create a rule with a pattern that matches bucket creation events emitted by Object Storage. Specify the Notifications topic you created as an action to deliver matching events. To test your rule, create a bucket. Object Storage emits an event which triggers the action. Check the email specified in the subscription to receive your notification.

To create a rule

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click **Create Rule**.
   
   Events compares the rules you create in this compartment to event messages emitted from resources in this compartment and any child compartments.

3. Enter the following.
   
   - **Display Name**: Specify a friendly name for the rule. You can change this name later. Avoid entering confidential information.
   - **Description**: Specify a description of what the rule does. You can change this description later.

4. In **Event Matching**, select **Event Type**.
   
   a. In **Service Name**, select **Object Storage**.
   b. In **Event Type**, select **Object Storage - Create Bucket**.

5. In **Actions**, specify the actions to trigger when the filter finds a match:
   
   a. In **Action Type**, select **Notifications**.
   b. In **Notifications Compartment**, select the compartment that contains the topic.
   c. In **Topic**, select the topic.

6. Click **Create Rule**.

**To create a bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Select the compartment where you created your rule (or any of its subordinate compartments).
3. Click **Create Bucket**.

4. In the **Create Bucket** dialog, specify the attributes of the bucket:
   
   - **Name**: Required. A user-friendly name or description. Avoid entering confidential information.
   - **Storage Tier**: Select the tier in which you want to store your data. Available tiers include:
     
     - **Standard** is the primary default Object Storage tier for storing data that is accessed frequently and requires fast and immediate access.
     - **Archive** is a special tier for storing data that is accessed infrequently and requires long retention periods. Access to data in the **Archive** tier is not immediate. You must restore archived data before it’s accessible.

5. Click **Create Bucket**.
To receive your notification

- Log in to the email account you specified in the previous procedure to receive the notification about the bucket being created.

Tip:
You will receive notifications each time a bucket is created in the compartment (or any of its sub compartments) until you disable the rule.

Using the CLI to Create a Rule

When you use the CLI to create a rule, you work a little differently than using the Console.

- To specify the actions for your rule, use a JSON formatted file. You create this file before you create the rule, and the file simplifies the amount of information you must type at the command line.
- To specify an event to match, use a JSON formatted string. You type this right into the console as you create the rule.

To create an action file

1. Create a file and add the following content.

```json
{
   "actions": [
   {
      "actionType": "ONS",
```
Tip: You can specify functions, streams, or topics as an action.

Example action file template

```
{
  "actions": [
    {
      "actionType": "FAAS",
      "description": "string",
      "functionId": "<function_OCID>",
      "isEnabled": true
    },
    {
      "actionType": "ONS",
      "description": "string",
      "isEnabled": true,
      "topicId": "<topic_OCID>
    },
    {
      "actionType": "OSS",
      "description": "string",
      "isEnabled": true,
      "streamId": "<stream_OCID>
    }
  ]
}
```

2. Fill in `<topic_OCID>` with actual topic OCID value from your tenancy.

3. Add a description.

4. Save the file with `action.json` as the file name.

To create a rule

Open a command prompt and run `oci events rule create` to create a rule.

Use the following options:

- `display-name` indicates the name of the rule in the Console
- `is-enabled` indicates whether the rule is evaluated.
- `condition` a JSON formatted string used to indicate a pattern for event matching (see Examples for usage).

**Examples**

- `compartment-id` indicates the compartment where the rule applies. Events evaluates messages from resources in this compartment and any child compartments.
- `actions` indicates the location in the local file system of the JSON formatted file you created to specify the actions for a rule.
- `wait-for-state=` when used with ACTIVE indicates that the CLI should wait for the service to create the rule, do another GET operation, and then display the rule in the active state. Without the option, the CLI displays the rule immediately in the creating state.

For example:

```
oci events rule create --display-name CLI-created_rule
--is-enabled true --condition "{"eventType": ["com.oraclecloud.objectstorage.createbucket"]}"
--compartment-
```
id <compartment_OCID> --actions <path_to_json_formatted_actions_file> --
wait-for-state=ACTIVE

Note:
Replace the values in <compartment_OCID> and
<path_to_json_formatted_actions_file> with the actual values from your
tenancy and local file system.

When you run the preceding command, the CLI prompts you about the rule and its display:

```
Action completed. Waiting until the resource has entered state: ACTIVE
{
    "data": {
        "actions": [
            {
                "action-type": "ONS",
                "description": "Notifications action",
                "id": "ocid1.eventaction.oc1.phx.<unique_ID>",
                "lifecycle-message": null,
                "lifecycle-state": "ACTIVE",
                "topic-id": "ocid1.onstopic.oc1.phx.<unique_ID>"
            }
        ],
        "compartment-id": "ocid1.compartment.oc1..<unique_ID>",
        "condition": "{"eventType": ["com.oraclecloud.objectstorage.createbucket"]}",
        "defined-tags": {},
        "description": null,
        "display-name": "CLI-created_rule",
        "freeform-tags": {},
        "id": "ocid1.eventrule.oc1.phx.<unique_ID>",
        "is-enabled": true,
        "lifecycle-message": null,
        "lifecycle-state": "ACTIVE",
        "time-created": "2019-04-25T01:32:56.855000+00:00"
    },
    "etag": "<unique_ID>--gzip"
}
```

To create a bucket

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Select the compartment where you created your rule (or any of its subordinate compartments).
3. Click Create Bucket.
4. In the Create Bucket dialog, specify the attributes of the bucket:
   - **Name**: Required. A user-friendly name or description. Avoid entering confidential information.
   - **Storage Tier**: Select the tier in which you want to store your data. Available tiers include:
     - **Standard** is the primary default Object Storage tier for storing data that is accessed frequently and requires fast and immediate access.
     - **Archive** is a special tier for storing data that is accessed infrequently and requires long retention periods. Access to data in the Archive tier is not immediate. You must restore archived data before it’s accessible.
5. Click Create Bucket.
To receive your notification

- Log in to the email account you specified in the previous procedure to receive the notification about the bucket being created.

Tip:

You receive notifications each time a bucket is created in the compartment (or any of its sub compartments) until you disable the rule.

Matching Events with Filters

This topic describes how to match events with pattern filters in rules to build automation.

Background

To understand filtering, it’s helpful to review the structure of an actual event message. Events uses JSON objects to represent events. This is an event:

```
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.objectstorage.deletebucket",
  "source": "objectstorage",
  "eventTypeVersion": "1.0",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceId": "my_bucket",
    "resourceId": "ocid1.compartment.oc1..<unique_ID>",
    "availabilityDomain": "NfHZ:PHX-AD-2",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "namespace": "example_namespace",
      "publicAccessType": "NoPublicAccess",
      "eTag": "f8ffb6e9-f602-460f-a6c0-00b5abfa24c7"
    }
  }
}
```

Two key points to remember about all events:

- Events all have the same set of top-level attributes, which are known as the event envelope. With one exception, most of these top-level attributes are not that useful for creating filters. The exception is eventType, which identifies the type of event included in the payload.

- The payload of the event appears within the data attribute. The information in this field depends on which service produced the event and the event type requested. The information in the payload is useful for isolating one event from another with a filter.
For more information about the envelope, see Contents of an Event Message on page 1814. For a list of all the services that produce events, see Services that Produce Events on page 1817.

**Event Matching with Filters**

Rules use filters to select events and route them for delivery to action resources. A rule is represented as a JSON object, similar to an event. The filter is an attribute of the rule, and the attribute is named `condition`. A filter either matches an event or it does not.

A few important things to remember about filters:

- Fields not mentioned in a filter are ignored. You can create a valid filter that matches all event messages with two curly brackets.
- For a filter to match an event, the event must contain all the field names listed in the filter. Field names must appear in the filter with the same nesting structure used in the event.
- Rules apply to events in the compartment in which you create them and any child compartments. This means that a filter specified by a rule only matches events emitted from resources in the same compartment or any child compartments.
- Wildcard matching is supported with the asterisk (*) character. See Examples of Wildcard Matching in Filters on page 1799.

**Examples of Simple Filters**

The following filter matches every event in the compartment and any child compartments where you create the rule.

```json
{
  ...
  "condition": "{ }"
}
```

When you add fields to the filter, you limit the events that the filter can match. For example, the following filter matches only `deletebucket` events.

```json
{
  ...
  "condition": "{
    "eventType": "com.oraclecloud.objectstorage.deletebucket"
  }"
}
```

To create a filter for more than one event type, use an array in `eventType`. The following filter matches `deletebucket` and `createbucket` events.

```json
{
  ...
  "condition": "{
    "eventType": [
      "com.oraclecloud.objectstorage.deletebucket",
      "com.oraclecloud.objectstorage.createbucket"
    ]
  }"
}
```
Examples of Filters with Event Payload Attributes

Both of the following filters would match the event at the top of the page. The first because filter specifies two fields and both fields appear in the event, the second because the "NoPublicAccess" type appears in the event.

The important thing to note is how the field names in the filter match the nesting structure of the event.

```json
{
...
"condition": "{
"data": {
  "compartmentName": "example_name",
  "resourceName": "my_bucket"
}
}""
}
```

Neither of the following filters would match the event at the top of this page. The first because the filter specifies a PublicAccessType not found in the event. The second because the event specifies a name for different bucket.

```json
{
...
"condition": "{
"data": {
  "additionalDetails": {
    "publicAccessType": "NoPublicAccess"
  }
}
}""
}
```

```json
{
...
"condition": "{
"data": {
  "compartmentName": "example_name",
  "resourceName": "my_bucket",
  "additionalDetails": {
    "publicAccessType": "PublicAccess"
  }
}
}""
}
```

```json
{
...
"condition": "{
"data": {
  "additionalDetails": {
    "publicAccessType": "NoPublicAccess"
  }
}
}""
}
```
Examples of Arrays in Filters

Arrays in filters match events if any of the values in the filter match a value in an event. The following filter would match the event at the top of the page because the name of the bucket in the event is included in an array in the filter.

```json
{
  ...
  "condition": 
  "data": 
  "resourceName": [
    "my_bucket_2",
    "my_bucket_1",
    "my_bucket"
  ],
  "additionalDetails": 
  "namespace": "example_namespace",
  "publicAccessType": "NoPublicAccess"
}
```

You can use an array in `eventType` (or any of the top-level fields), the event payload as shown in the preceding example, or both the event payload and a top-level field.

```json
{
  ...
  "condition": 
  "eventType": [
    "com.oraclecloud.objectstorage.deletebucket",
    "com.oraclecloud.objectstorage.createbucket"
  ],
  "data": 
  "resourceName": [
    "my_bucket_2",
    "my_bucket_1",
    "my_bucket"
  ],
  "additionalDetails": 
  "namespace": "example_namespace",
  "publicAccessType": "NoPublicAccess"
}
```

Examples of Wildcard Matching in Filters

The following are a few things to consider about wildcard matching with filters.

- Use the wildcard only in attribute values. You cannot use the asterisk for matching in keys.
- An attribute value with only an asterisk matches all values for the associated attribute name, but not null.
- The period character has no special meaning in a filter.

You can add the asterisk at the start of a string, in the middle, or at the end. All of the filters that follow match the event at the top of the page.

- The first matches because the wildcard in `displayName` matches the bucket naming pattern.
- The second one matches because the `publicAccessType` uses a wildcard. Because of the use of the wildcard, these first two filters would also match events from buckets with a similar naming pattern and would include events from buckets with or without public access.
- The third one matches because the event type includes all types of bucket events.

```json
{
...
"condition": "{
    "data": {
        "resourceName": "my_bucket*",
        "additionalDetails": {
            "namespace": "example_namespace",
            "publicAccessType": "NoPublicAccess"
        }
    }
}
}
```

```json
{
...
"condition": "{
    "data": {
        "resourceName": ["my_bucket_2", "my_bucket_1", "my_bucket"],
        "additionalDetails": {
            "namespace": "example_namespace",
            "publicAccessType": "*
        }
    }
}
}
```

```json
{
...
"condition": "{
    "eventType": "com.oraclecloud.objectstorage.*bucket",
    "data": {
        "resourceName": ["my_bucket_2", "my_bucket_1", "my_bucket"],
        "additionalDetails": {
            "namespace": "example_namespace",
            "publicAccessType": "NoPublicAccess"
        }
    }
}
}
```
Events and IAM Policies

This topic describes how an administrator must write IAM policy for the Events service. If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more details about how to write IAM policy for Events, see Details for the Events Service on page 2272.

Allow Users to Work with Rules

These IAM policies allow users to manage or list rules.

**Let users list rules in a compartment**

*Type of access:* Ability to list Events rules.

*Where to create the policy:* In the tenancy.

Allow group RuleReaders to read cloudevents-rules in tenancy

The preceding policy allows RuleReaders to list rules in the tenancy.

**Let admins manage rules in a compartment**

*Type of access:* Ability to manage Events rules, including creating, deleting, updating or moving rules to a different compartment.

*Where to create the policy:* In the tenancy.

This line gives the user inspect access to resources in compartments to select actions.

allow group <RuleAdmins> to inspect compartments in tenancy

This line gives the user access to defined tags to apply filter tags to rules.

allow group <RuleAdmins> to use tag-namespaces in tenancy

These lines give the user access to Streaming resources for actions.

allow group <RuleAdmins> to inspect streams in tenancy
allow group <RuleAdmins> to use stream-push in tenancy
allow group <RuleAdmins> to use stream-pull in tenancy

These lines give the user access to Functions resources for actions.

allow group <RuleAdmins> to use virtual-network-family in tenancy
allow group <RuleAdmins> to manage function-family in tenancy

This line gives the user access to Notifications topics for actions.

allow group <RuleAdmins> to use ons-topic in tenancy

This line gives the user manage access to rules for Events.

allow group <RuleAdmins> to manage cloudevents-rules in tenancy

Managing Rules for Events

This topic describes how to manage rules for the Events service. For more information about Events, see Overview of Events on page 1784.
Prerequisites for Creating Rules

- Action resources: You must have resources already set up to specify as an action. The Events service invokes the action specified in the rule by delivering the event message to action resources, which can include topics, streams, or functions. Every rule must have at least one action. The Events service can invoke any of the following services by delivering an event message for processing:
  - Notifications
  - Streaming
  - Functions
- IAM policies: To manage or list rules, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform a task and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information, see Events and IAM Policies on page 1801.
- Event messages: To create rules, the resources you want to monitor with the rule must emit events. For more information, see Services that Produce Events on page 1817.

Working with Rules

**Note:** Each rule can have a maximum of 10 actions.

A typical workflow for setting up rule might follow this pattern:

1. **Identify action resources**
   
   Set up or identify whatever action resources you intend to use with the rule. For example, you might set up a Notifications topic and create subscriptions for the DevOps team so that they are notified when backups complete. If a topic already exists, you can use it instead of creating a topic. The resources you specify for actions do not have to be in the same compartment as the rule.

2. **Plan filtering**
   
   Ensure the resources that you want to monitor emit events to the Events service and plan your pattern matching strategy. For example, you might want to monitor backups on Autonomous Data Warehouse instances in the ABC compartment. Ensure Autonomous Data Warehouse instances emit an event type you can use to create the automation you require. Review the example JSON event to determine the best way to identify those resources in filters. See Matching Events with Filters on page 1796 and Services that Produce Events on page 1817.

3. **Create the rule**
   
   Rules apply to events in the compartment in which you create them and any child compartments. Create a rule in the compartment with the resource you want to monitor and specify where to deliver matching events. For example, in the ABC compartment, you might create a rule that filters for Autonomous Data Warehouse backup events. Since Events has no requirement about the location of action resources, you could specify a topic in the XYZ compartment as the resource to deliver any matching events.

Managing Tags for Rules

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

Tags and Event Filtering

With Events, you can also use tags to target resources in your tenancy. You target resources by adding the tag to a filter in a rule. A filter tag helps you hone automation by targeting only resources that contain a particular tag. For example, let's say you have dozens of Database instances in your tenancy, but only a few of the most critical of these instances have the tag "Operations." You could create a rule that triggers a particular action for resources that only contain the "Operations" tag.
Policy for working with filter tags is no different from policy for working with tags.

To manage filter tags

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click rule's name.
3. In the Resources menu, click Event Matching.
4. In the Filter Tags section, you can view or edit existing filter tags, or click Add Filter Tag to add new ones.

To manage tags for rules

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click rule's name.
3. Click the Tags tab to view or edit existing tags, or click Add Tags to add new ones.

For more information, see Resource Tags on page 211.

Move Rules to a Different Compartment

You can move rules from one compartment to another. When you move a rule to a new compartment, you stop monitoring events from resources in the current compartment and begin monitoring events in the new compartment (and any child compartments). After you move the rule to the new compartment, inherent policies apply immediately and affect access to the rules through the Console. Moving rules doesn't affect access by the Events service to actions defined in rules. For more information, see Working with Compartments on page 2432.

Monitoring Rules

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For more information about monitoring the rules you create, see Events Metrics on page 1917.

Object Events and the Events Service

Events for objects are handled differently than other resources. Objects do not emit events by default. Use the Console, CLI, or API to enable a bucket to emit events for object state changes. You can enable events for object state changes during or after bucket creation.

Using the Console

To create a rule

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click Create Rule.
   
   Events compares the rules you create in this compartment to event messages emitted from resources in this compartment and any child compartments.
3. Enter the following.
   
   - Display Name: Specify a friendly name for the rule. You can change this name later. Avoid entering confidential information.
   - Description: Specify a description of what the rule does. You can change this description later.
4. In **Rule Conditions**, create a filter:

**To add an event type**

a. Select **Event Type**.

b. Select a **Service Name**.

c. In **Event type**, select one or more event types for this service.

d. Click **+ Another Condition** and select **Event Type** to add event types for a different service.

This filter will match events of the event types you specify.

**To add an attribute**

You must first select an event type to add an attribute.

a. Select **Attribute**.

b. Select an **Attribute Name**. Attribute values are optional.

c. Enter an **Attribute Value**. Attribute values are optional.

d. Click **+ Another Condition** and select **Attribute** to add another attribute.

This filter will match events of the event types with the attributes you specify.

**To add a filter tag**

a. Select **Filter Tag**

b. Select a **Tag Namespace**.

To specify a free-form tag, select **None (apply a free-form tag)**.

c. Select a **Tag Key**.

d. Enter a **Tag Value**. Tag values are optional.

e. Click **+ Another Condition** and select **Filter Tag** to add another filter tag.

This filter will match events with the tags you specify.

Filter tags help you to hone automation by targeting only resources that contain a particular tag. If you want to use tags to organize your rules, use resource tags instead. For more information, see [Managing Tags for Rules](#) on page 1802.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can leave this field entirely blank to match all events. See <a href="#">Matching Events with Filters</a> on page 1796.</td>
</tr>
</tbody>
</table>

**To validate this rule**

You can only evaluate a rule against one event type at a time. To test different event types, repeat these steps as necessary.

a. Click **Validate Rule**. The **Test Rule** panel opens.

b. In **Service Name**, select a service if necessary.

c. In **Event Type**, select an event type, if necessary. A example event appears based on the selections you made. Edit the values in the event to match the values for any attributes and tags you added to your rule. For more information, see [Contents of an Event Message](#) on page 1814.

d. Click **Check if Example Event Matches Rule**. If the rule doesn't match, use the rule editor to modify any of the following:

   - Add or remove event types
   - Add or remove values or attributes
   - Add or remove tags
   - Insert wildcards

   For more information, see [Matching Events with Filters](#) on page 1796.

e. Click **Close**.
To view reference events

a. Click View example events (JSON). The View Example Events panel opens.
b. In Service Name, select a service if necessary.
c. In Event Type, select an event type, if necessary. An example event appears based on the selections you made. Use the events viewer to browse reference events.
d. Click Done.

For more information, see Contents of an Event Message on page 1814 and Matching Events with Filters on page 1796.

To add an attribute

5. In Actions, specify the actions resources to trigger when the filter finds a match:

To select a topic

a. Select Notifications.
b. Select the Notifications Compartment.
c. Select the Topic.
d. Click + Another Action and select Notifications to add another topic.

To select a stream

a. Select Streaming.
b. Select the Stream Compartment.
c. Select the Stream.
d. Click + Another Action and select Streaming to add another stream.

To select a function

a. Select Functions.
b. Select the Function Compartment.
c. Select a Function Application.
d. Select the Function.
e. Click + Another Action and select Functions to add another function.

6. Click Create Rule.

To edit a rule

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment that has the rule you want to edit.
3. For the rule you want to edit, click the Actions icon (three dots), and then click Edit.
4. Make your changes and click Save Changes.

To disable or enable a rule

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment that has the rule you want to work with.
3. For the rule, you want change, click the Actions icon (three dots), and then take one of the following actions:
   a. Click Disable
   b. Click Enable
4. Confirm when prompted.

To move a rule to a different compartment

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. In the Scope section, select a compartment.
3. Find the rule in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To validate a rule**

You can only evaluate a rule against one event type at a time. Repeat as necessary to test different event types.

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to test.
3. Click **Validate Rule**.
4. Take one or more of the following actions:
   - If there are no event types in the rule, select the service and event type you want to test.
   - If you want to test a different event type than the one selected by default, select the service and event type you want to test.
   - If you added attribute values or filter tags to the rule, edit the example data in the event to match the values in your rule.
5. Click **Check if Example Event Matches Rule**.

For more information, see **Matching Events with Filters** on page 1796 and **Contents of an Event Message** on page 1814.

**To delete a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose the **Compartment** that has rule you want to delete.
3. For the rule you want to delete, click the Actions icon (three dots) , and then click **Delete**.
4. Confirm when prompted.

**To add an action to a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Actions**.
4. Click **Add**.
   - The **Add Action** box appears. Configure the action resources:
     - **To select a topic**
       a. Select **Notifications**.
       b. Select the **Notifications Compartment**.
       c. Select the **Topic**.
     - **To select a stream**
       a. Select **Streaming**.
       b. Select the **Stream Compartment**.
       c. Select the **Stream**.
     - **To select a function**
       a. Select **Functions**.
       b. Select the **Function Compartment**.
       c. Select a **Function Application**.
       d. Select the **Function**.
   - **Action State**: Select to enable the action. Clear to disable.
5. Click Add Action.

To edit an action
1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click the Name of the rule you want to update.
3. In the Resources menu, click Actions.
4. Select an action.
5. Go to Actions and click Edit. The Edit Action box appears.
6. Make your changes and click Save Changes.

To enable or disable an action
1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click the Name of the rule you want to update.
3. In the Resources menu, click Actions.
4. Select an action.
5. Go to Actions and specify Enable or Disable.
6. Confirm when prompted.

To remove an action
1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click the Name of the rule you want to update.
3. In the Resources menu, click Actions.
4. Select an action.
5. Go to Actions and click Remove.
6. Confirm when prompted.

Each rule must have one action.

To add event types to a rule
1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click the Name of the rule you want to update.
3. In the Resources menu, click Event Matching.
4. Click Add Event Type.
5. In Service Name, select a service.
6. In Event Type, select an event type for this service.
7. Click Add Event Type.

To edit event types for a rule
1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click the Name of the rule you want to update.
3. In the Resources menu, click Event Matching.
4. Select an event type.
5. Click Edit. The Edit Event Type box appears.
6. Make your changes and click Save Changes.

To remove event types for a rule
1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Select the check box next to the event types you want to remove.

   **Tip:**
   To select the entire list, select the check box in the header row.
5. Click **Remove**.
6. Confirm when prompted.

### To add attributes to a rule

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Click **Add Attribute**. The **Add Attribute** box appears. Configure the attribute:

   - **Attribute Name**: Specify an attribute or tag to narrow matching results.
     - Select an attribute name. The list of attribute names is based on the event types you selected. If you select no event types, you cannot add an attribute.
     - If you specify an attribute here, you limit the events that match this rule.
   - **Attribute Values**: Specify one or more values for the attribute name.
     a. Enter a value. As you type, the value appears under the field with (New) appended. Select the value with (New) appended to add the value to **Attribute Values**.

![ATTRIBUTE VALUES](image)

b. Enter more values for attribute name in the same manner as before.

![ATTRIBUTE VALUES](image)

Here are some things to consider about attribute values:

- Use an asterisk to create a wildcard. See Examples of Wildcard Matching in Filters on page 1799.
- Multiple values for an attribute name broaden your results. If any of the values you enter here match a value in an event, the rule matches. See Examples of Arrays in Filters on page 1799.
5. Click **Add attribute**.
**To edit attributes for a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Select an attribute.
5. Click **Edit**. The **Edit Attribute** box appears.
6. Make your changes and click **Save Changes**.

**To remove attributes for a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Select the check box next to the attributes you want to remove.
5. Click **Remove**.
6. Confirm when prompted.

**To add filter tags to a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Click **Add Filter Tag**.
5. In **Tag Namespace**, do one of the following:
   - Select a namespace to add a defined tag as a filter.
   - Select **None (apply a free-form tag)** to add a free-form tag as a filter.
6. In **Tag Key**, do one of the following:
   - Select the tag key for the defined tag.
   - Enter the tag key for the free-form tag.
7. Enter a **Value**.
8. Click **Add Filter Tag**.

**To edit filter tags for a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Select a filter tag.
5. Click **Edit**. The **Edit Attribute** box appears.
6. Make your changes and click **Save Changes**.

**To remove filter tags for a rule**

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose a **Compartment** you have permission to work in, and then click the **Name** of the rule you want to update.
3. In the **Resources** menu, click **Event Matching**.
4. Select the check box next to the filter tags you want to remove.

   Tip:
   To select the entire list, select the check box in the header row.

5. Click Remove.
6. Confirm when prompted.

**Using the Command Line Interface (CLI)**

When you use the CLI to create a rule, you work a little differently than using the Console.

- To specify the actions for your rule, use a JSON formatted file. You create this file before you create the rule, and the file simplifies the amount of information you must type at the command line.
- To specify an event to match, use a JSON formatted string. You type this right into the console as you create the rule.

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see CLI Help.

**To create an action JSON file**

To specify the actions for your rule, use a JSON formatted file. For more information, see Advanced JSON Options on page 4214.

1. Create a file and add the following content. This content doesn't have to be escaped or on a single line, it just has to contain valid JSON.

   ```json
   {
   "actions": [
   {
   "actionType": "FAAS",
   "description": "string",
   "functionId": "<function_OCID>",
   "isEnabled": true
   },
   {
   "actionType": "ONS",
   "description": "string",
   "isEnabled": true,
   "topicId": "<topic_OCID>"
   },
   {
   "actionType": "OSS",
   "description": "string",
   "isEnabled": true,
   "streamId": "<stream_OCID>"
   }
   ]
   }
   ```

2. Edit the file and remove any objects you don't want to use as an action. For example, if you wanted to only use Notifications as an action, then you would delete all the other objects.

   ```json
   { 
   "actions": [
   {
   "actionType": "ONS",
   "description": "string",
   "isEnabled": true,
   "topicId": "<topic_OCID>"
   }
   ]
   }
3. Edit the file and fill in any variables with actual values from your tenancy, as shown in the following example.

```json
{
  "actions": [
    {
      "actionType": "ONS",
      "description": "string",
      "isEnabled": true,
      "topicId": "<topic_OCID>"
    }
  ]
}
```

4. Add a description.
5. Save the file as action.json
6. To create a rule and specify Notifications as an action, run the following command.

```bash
oci events rule create --display-name <friendly_name> --is-enabled true --condition "{}" --compartment-id <compartment_OCID> --actions file://action.json
```

**To create a rule**

Open a command prompt and run `oci events rule create` to create a rule.

Use the following options:

- `display-name` indicates the name of the rule in the Console
- `is-enabled` indicates whether Events should evaluate the rule.
- `condition` a JSON formatted string used to indicate a pattern for event matching (see Examples for usage).

**Examples**

The following example shows how to pass a simple condition that matches all events. Everything between the double quotes (" ") is a string, while the brackets { } indicate JSON:

```bash
oci events rule create --display-name <friendly_name> --is-enabled true --condition "{}" --compartment-id <compartment_OCID> --actions file://action.json --wait-for-state=ACTIVE
```

To pass complex input to the CLI as a JSON string, you must enclose the entire block in double quotes. Inside the block, each double quote for the key and value strings must be escaped with a backslash (\) character. For example:

```bash
oci events rule create --display-name <friendly_name> --is-enabled true --condition "{"eventType": ["com.oraclecloud.objectstorage.createobject"]}" --compartment-id <compartment_OCID> --actions file://action.json --wait-for-state=ACTIVE
```

In PowerShell, to escape double quotes, you must use two characters: The backslash (\) and the back tick (`). For example, in Windows PowerShell:

```bash
oci events rule create --display-name <friendly_name> --is-enabled true --condition "{"eventType": ["com.oraclecloud.objectstorage.createobject"]}" --compartment-id <compartment_OCID> --actions file://action.json
```
Tip:
The condition option does not support using a file to pass the JSON formatted string.

For information on creating filters, see Matching Events with Filters on page 1796.

- **compartment-id** indicates the compartment where the rule applies. Events evaluates messages from resources in this compartment and any subordinate compartments.
- **actions** indicates the location in the local file system of the JSON formatted file you created to specify the actions for a rule.
- **wait-for-state=** when used with ACTIVE indicates that the CLI should wait for the service to create the rule, do another GET operation, and then display the rule in the active state. Without the option, the CLI displays the rule immediately in the creating state.

For example:

```bash
oci events rule create --display-name <friendly_name> --is-enabled true --condition <json_formatted_string> --compartment-id <compartment_OCID> --actions <json_formatted_file> --wait-for-state=ACTIVE
```

**Note:**
Replace the values in `<compartment_OCID>` and `<json_formatted_file>` with the actual values from your tenancy and the local file system.

To delete a rule

Open a command prompt and run `oci events rule delete` to delete a single rule. For example:

```bash
oci events rule delete --rule-id <rule_OCID>
```

The command returns a prompt, asking for confirmation. Type y to delete the rule.

To get rule metadata

You can get rule metadata using the CLI. The Console displays this metadata in the Rule Details tab.

Open a command prompt and run `oci events rule get` to get information about a single rule. For example:

```bash
oci events rule get --rule-id <rule_OCID>
```

The command returns the following information:

```json
{
  "data": {
    "actions": {
      "actions": [
        {
          "action-type": "ONS",
          "description": null,
          "id": "ocid1.eventaction.oc1.phx.<unique_ID>",
          "lifecycle-message": null,
          "lifecycle-state": "ACTIVE",
          "topic-id": "ocid1.onstopic.oc1.phx.<unique_ID>"
        }
      ],
      "compartment-id": "ocid1.compartment.oc1..<unique_ID>",
```
To get a list of rules

Open a command prompt and run `oci events rule list` to list the rules in a compartment. For example:

```
oci events rule list --compartment-id <compartment_OCID>
```

The command returns the following information:

```json
{
  "data": [
    {
      "compartment-id": "ocid1.compartment.oc1..<unique_ID>",
      "condition": "{}",
      "description": "Example_Rule",
      "display-name": "rule_1",
      "id": "ocid1.eventrule.oc1.phx.<unique_ID>",
      "is-enabled": true,
      "lifecycle-state": "ACTIVE",
      "time-created": "2019-01-22T20:10:53.562000+00:00"
    },
    {
      "compartment-id": "ocid1.compartment.oc1..<unique_ID>",
      "condition": "{}",
      "description": null,
      "display-name": "rule_2",
      "id": "ocid1.eventrule.oc1.phx.<unique_ID>",
      "is-enabled": true,
      "lifecycle-state": "ACTIVE",
      "time-created": "2019-01-22T20:27:25.099000+00:00"
    },
    ...
  ]
}
```
To update a rule

Open a command prompt and run `oci events rule update` to update a rule.

To update the condition for a rule:

```
oci events rule update --rule-id <rule_OCID> --
condition <json_formatted_string>
```

For example:

```
oci events rule update --rule-id ocid1.eventrule.oc1.phx.<unique_ID> --
condition "{}" --wait-for-state=ACTIVE
```

The previous command would update the condition of the rule to use an empty JSON string. The CLI updates the rule, waits for the rule to update and change to the active state (only if you used the --wait-for-state option), then displays the updated rule.

Use the following options to update a rule:

- `display-name`
- `description`
- `is-enabled`
- `condition`
- `actions`
- `freeform-tags`
- `defined-tags`

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage rules:

- `ChangeRuleCompartment`
- `CreateRule`
- `DeleteRule`
- `GetRule`
- `UpdateRule`
- `ListRules`

Contents of an Event Message

This topic describes the contents of an event message. Every event message includes two main parts:

- Envelope: a container for all event messages
- Payload: the data from the resource emitting the event message

Event Envelope

These attributes for an event envelope are the same for all events. The structure of the envelope follows the CloudEvents industry standard format hosted by the Cloud Native Computing Foundation (CNCF).
### Property | Description
--- | ---
**cloudEventsVersion** | The version of the CloudEvents specification.  
  Note:  
  Events uses version 0.1 specification of the CloudEvents event envelope.
**contentType** | Set to *application/json*. The content type of the data contained in the data attribute.
**data** | The payload of the event. All of the information within data comes from the resource emitting the event. See the following table for more detail on the structure of the payload.
**eventID** | The UUID of the event. This identifier is not an OCID, but just a unique ID for the event.
**eventTime** | The time of the event, expressed in RFC 3339 timestamp format.
**eventType** | The type of event that happened. For a list of all services that produce events and the even types that those services track, see Services that Produce Events on page 1817.  
  Note:  
  The service that produces the event can also add, remove, or change the meaning of a field by publishing a new version of an eventType and revising the eventTypeVersion field.
**eventTypeVersion** | The version of the event type.
**extensions** | The OCID of the compartment from which the event originates. If the event originates from the root compartment of the tenancy, then this attribute specifies a tenancy OCID. This attribute is mandatory in the Oracle Cloud Infrastructure implementation of the CloudEvents specification.
**source** | The resource that produced the event. For example, an Autonomous Database or an Object Storage bucket.

### Payload
The data in these fields depends on which service produced the event and the event type it defines.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>compartmentId</strong></td>
<td>The OCID of the compartment of the resource emitting the event.</td>
</tr>
<tr>
<td><strong>compartmentName</strong></td>
<td>The name of the compartment of the resource emitting the event.</td>
</tr>
<tr>
<td><strong>resourceName</strong></td>
<td>The name of the resource emitting the event.</td>
</tr>
<tr>
<td><strong>resourceId</strong></td>
<td>An OCID or an ID for the resource emitting the event.</td>
</tr>
<tr>
<td><strong>availabilityDomain</strong></td>
<td>The availability domain of the resource emitting the event.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>freeFormTags</td>
<td>Free-form tags added to the resource emitting the event.</td>
</tr>
<tr>
<td>definedTags</td>
<td>Defined tags added to the resource emitting the event.</td>
</tr>
<tr>
<td>additionalDetails</td>
<td>A container for attributes unique to the resource emitting the event. In the example bucket event that follows, the payload includes three Object Storage attributes:</td>
</tr>
<tr>
<td></td>
<td>• namespace</td>
</tr>
<tr>
<td></td>
<td>• publicAccessType</td>
</tr>
<tr>
<td></td>
<td>• eTag</td>
</tr>
</tbody>
</table>
|                  | To determine what attributes are included for other resources, retrieve an event or consult the reference samples listed on Services that Produce Events on page 1817.

## Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

## An Example Event

The following is an example bucket event emitted by Object Storage.

```json
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.objectstorage.deletebucket",
  "source": "objectstorage",
  "eventTypeVersion": "1.0",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_bucket",
    "resourceId": "ocid1.compartment.oc1..<unique_ID>",
    "availabilityDomain": "NfHz:PHX-AD-2",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "namespace": "example_namespace",
      "publicAccessType": "NoPublicAccess",
      "eTag": "f8ffb6e9-f602-460f-a6c0-00b5abfa24c7"
    }
  }
}
```
Services that Produce Events

This topic lists the Oracle Cloud Infrastructure services that emit events:

- Analytics Cloud
- API Gateway
- Application Migration
- Big Data
- Block Volume
- Blockchain Platform
- Budgets
- Cloud Guard on page 1830
- Compute
- Container Engine for Kubernetes
- Content and Experience
- Database
- Data Catalog on page 1863
- Data Safe
- Data Science
- Data Transfer
- Digital Assistant
- File Storage
- Functions
- Health Checks
- IAM
- Integration
- Networking
- NoSQL Database Cloud
- Notifications
- Object Storage
- Operations Insights on page 1909
- OS Management
- Resource Manager
- WAF

About Event Types and Example Reference Events

Services emit event messages by resource type. Event messages use a combination of an event type and a data payload (from the resource) to identify state changes.

In this section:

- Event types are organized by service, then by resource type
- There is one reference example per resource type if the payload contains the same attributes for all event types

See Matching Events with Filters on page 1796 and Contents of an Event Message on page 1814.

Analytics Cloud

For details about events emitted by Analytics Cloud, see Service Events.
API Gateway

API Gateway resources that emit events:

- **API Gateway Certificate Event Types** on page 1818
- **API Deployment Event Types** on page 1819
- **API Gateway Event Types** on page 1820
- **API Event Types** on page 1821

**API Gateway Certificate Event Types**

These are the event types that API Gateway certificates emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Certificate Compartment Begin</td>
<td>com.oraclecloud.apigateway.changegatewaycertificate.begin</td>
</tr>
<tr>
<td>Change Certificate Compartment End</td>
<td>com.oraclecloud.apigateway.changegatewaycertificate.end</td>
</tr>
<tr>
<td>Create Certificate Begin</td>
<td>com.oraclecloud.apigateway.creategatewaycertificate.begin</td>
</tr>
<tr>
<td>Create Certificate End</td>
<td>com.oraclecloud.apigateway.creategatewaycertificate.end</td>
</tr>
<tr>
<td>Delete Certificate Begin</td>
<td>com.oraclecloud.apigateway.deletegatewaycertificate.begin</td>
</tr>
<tr>
<td>Delete Certificate End</td>
<td>com.oraclecloud.apigateway.deletegatewaycertificate.end</td>
</tr>
<tr>
<td>Update Certificate Begin</td>
<td>com.oraclecloud.apigateway.updategatewaycertificate.begin</td>
</tr>
<tr>
<td>Update Certificate End</td>
<td>com.oraclecloud.apigateway.updategatewaycertificate.end</td>
</tr>
</tbody>
</table>

**API Gateway Certificate Example**

This is an example event for API Gateway certificates:

```json
{
    "eventType": "com.oraclecloud.apigateway.creategatewaycertificate.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "apigateway",
    "eventTime": "2019-08-16T15:09:04.550Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "My_Certificate",
        "resourceId": "ocid1.apigatewaycertificate.oc1.phx.<unique_ID>",
        "availabilityDomain": "availability_domain"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```
API Deployment Event Types

These are the event types that API deployments emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Deployment Compartment Begin</td>
<td>com.oraclecloud.apigateway.changedeploymentcompartment.begin</td>
</tr>
<tr>
<td>Change Deployment Compartment End</td>
<td>com.oraclecloud.apigateway.changedeploymentcompartment.end</td>
</tr>
<tr>
<td>Create Deployment Begin</td>
<td>com.oraclecloud.apigateway.createdeployment.begin</td>
</tr>
<tr>
<td>Create Deployment End</td>
<td>com.oraclecloud.apigateway.createdeployment.end</td>
</tr>
<tr>
<td>Delete Deployment Begin</td>
<td>com.oraclecloud.apigateway.deletedeployment.begin</td>
</tr>
<tr>
<td>Delete Deployment End</td>
<td>com.oraclecloud.apigateway.deletedeployment.end</td>
</tr>
<tr>
<td>Update Deployment Begin</td>
<td>com.oraclecloud.apigateway.updatedeployment.begin</td>
</tr>
<tr>
<td>Update Deployment End</td>
<td>com.oraclecloud.apigateway.updatedeployment.end</td>
</tr>
</tbody>
</table>

API Deployment Example

This is an example event for API deployments:

```json
{
  "eventType": "com.oraclecloud.apigateway.createdeployment.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "apigateway",
  "eventTime": "2019-08-16T15:09:04.550Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "My_Deployment",
    "resourceId": "ocid1.apideployment.oc1.phx.<unique_ID>",
    "availabilityDomain": "availability_domain"
  },
  "eventID": "<unique_ID>",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"  
  }
}
```
**API Gateway Event Types**

These are the event types that API gateways emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Gateway Compartment Begin</td>
<td>com.oraclecloud.apigateway.changegatewaycompartment.begin</td>
</tr>
<tr>
<td>Change Gateway Compartment End</td>
<td>com.oraclecloud.apigateway.changegatewaycompartment.end</td>
</tr>
<tr>
<td>Create Gateway Begin</td>
<td>com.oraclecloud.apigateway.creategateway.begin</td>
</tr>
<tr>
<td>Create Gateway End</td>
<td>com.oraclecloud.apigateway.creategateway.end</td>
</tr>
<tr>
<td>Delete Gateway Begin</td>
<td>com.oraclecloud.apigateway.deletegateway.begin</td>
</tr>
<tr>
<td>Delete Gateway End</td>
<td>com.oraclecloud.apigateway.deletegateway.end</td>
</tr>
<tr>
<td>Update Gateway Begin</td>
<td>com.oraclecloud.apigateway.updategateway.begin</td>
</tr>
<tr>
<td>Update Gateway End</td>
<td>com.oraclecloud.apigateway.updategateway.end</td>
</tr>
</tbody>
</table>

**Gateway Example**

This is an example event for API gateways:

```json
{
    "eventType": "com.oraclecloud.apigateway.creategateway.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "apigateway",
    "eventTime": "2019-08-16T15:09:04.550Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "eventID": "<unique_ID>"
}
```
## API Event Types

These are the event types that API resources emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change API Compartment Begin</td>
<td>com.oraclecloud.apigateway.changeapicompartment.begin</td>
</tr>
<tr>
<td>Change API Compartment End</td>
<td>com.oraclecloud.apigateway.changeapicompartment.end</td>
</tr>
<tr>
<td>Create API Begin</td>
<td>com.oraclecloud.apigateway.createapi.begin</td>
</tr>
<tr>
<td>Create API End</td>
<td>com.oraclecloud.apigateway.createapi.end</td>
</tr>
<tr>
<td>Delete API Begin</td>
<td>com.oraclecloud.apigateway.deleteapi.begin</td>
</tr>
<tr>
<td>Delete API End</td>
<td>com.oraclecloud.apigateway.deleteapi.end</td>
</tr>
<tr>
<td>Update API Begin</td>
<td>com.oraclecloud.apigateway.updateapi.begin</td>
</tr>
<tr>
<td>Update API End</td>
<td>com.oraclecloud.apigateway.updateapi.end</td>
</tr>
</tbody>
</table>

### API Example

This is an example event for API resources:

```json
{
    "eventType": "com.oraclecloud.apigateway.createapi.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "apigateway",
    "eventTime": "2020-09-09T12:00:00.000Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "My_API",
        "resourceId": "ocid1.apigatewayapi.oc1.phx.<unique_ID>",
        "availabilityDomain": "availability_domain"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```

### Application Migration

For details about events emitted by Application Migration, see Service Events.
Big Data
For details about events emitted by Big Data, see Service Events.

Block Volume
Block Volume resources that emit events:
- Block Volume Event Types on page 1822 and Block Volume Backup Event Types on page 1824
- Boot Volume Event Types on page 1825 and Boot Volume Backup Event Types on page 1826
- Volume Groups and Volume Group Backups on page 1827

Block Volume Event Types
These are the event types that block volumes emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Volume Compartment Begin</td>
<td>com.oraclecloud.blockvolumes.changevolumecompartmentbegin</td>
</tr>
<tr>
<td>Change Volume Compartment End</td>
<td>com.oraclecloud.blockvolumes.changevolumecompartmentend</td>
</tr>
<tr>
<td>Create Volume Begin</td>
<td>com.oraclecloud.blockvolumes.createvolume.begin</td>
</tr>
<tr>
<td>Create Volume End</td>
<td>com.oraclecloud.blockvolumes.createvolume.end</td>
</tr>
<tr>
<td>Delete Volume Begin</td>
<td>com.oraclecloud.blockvolumes.deletevolume.begin</td>
</tr>
<tr>
<td>Delete Volume End</td>
<td>com.oraclecloud.blockvolumes.deletevolume.end</td>
</tr>
<tr>
<td>Delete Volume Kms Key Begin</td>
<td>com.oraclecloud.blockvolumes.deletevolumekmskey.begin</td>
</tr>
<tr>
<td>Update Volume</td>
<td>com.oraclecloud.blockvolumes.updatevolume</td>
</tr>
<tr>
<td>Update Volume Begin</td>
<td>com.oraclecloud.blockvolumes.updatevolumebegin</td>
</tr>
<tr>
<td>Update Volume End</td>
<td>com.oraclecloud.blockvolumes.updatevolume.end</td>
</tr>
<tr>
<td>Update Volume Kms Key Begin</td>
<td>com.oraclecloud.blockvolumes.updatevolumekmskey.begin</td>
</tr>
<tr>
<td>Update Volume Kms Key End</td>
<td>com.oraclecloud.blockvolumes.updatevolumekmskey.end</td>
</tr>
</tbody>
</table>

Block Volume Example
This is a reference event for block volumes:

```json
{
    "eventType": "com.oraclecloud.blockvolumes.createvolume.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "BlockVolumes",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_volume",
        "resourceId": "ocid1.volume.oc1..<unique_ID>",
        "availabilityDomain": "<availability_domain>"
    }
}
```


# Block Volume Backup Event Types

These are the event types that block volume backups emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Volume Backup Compartment</td>
<td>com.oraclecloud.blockvolumes.changevolumebackupcompartment</td>
</tr>
<tr>
<td>Copy Volume Backup Begin</td>
<td>com.oraclecloud.blockvolumes.copyvolumebackup.begin</td>
</tr>
<tr>
<td>Copy Volume Backup End</td>
<td>com.oraclecloud.blockvolumes.copyvolumebackup.end</td>
</tr>
<tr>
<td>Create Volume Backup Begin</td>
<td>com.oraclecloud.blockvolumes.createvolumebackup.begin</td>
</tr>
<tr>
<td>Create Volume Backup End</td>
<td>com.oraclecloud.blockvolumes.createvolumebackup.end</td>
</tr>
<tr>
<td>Create Volume Backup Policy Assignment</td>
<td>com.oraclecloud.blockvolumes.createvolumebackuppolicyassignment</td>
</tr>
<tr>
<td>Delete Volume Backup Begin</td>
<td>com.oraclecloud.blockvolumes.deletevolumebackup.begin</td>
</tr>
<tr>
<td>Delete Volume Backup End</td>
<td>com.oraclecloud.blockvolumes.deletevolumebackup.end</td>
</tr>
<tr>
<td>Delete Volume Backup Policy Assignment</td>
<td>com.oraclecloud.blockvolumes.deletevolumebackuppolicyassignment</td>
</tr>
<tr>
<td>Update Volume Backup</td>
<td>com.oraclecloud.blockvolumes.updatevolumebackup</td>
</tr>
<tr>
<td>Update Volume Backup Policy</td>
<td>com.oraclecloud.blockvolumes.updatevolumebackuppolicy</td>
</tr>
</tbody>
</table>

## Block Volume Backup Example

This is a reference event for block volume backups:

```json
{
  "eventType": "com.oraclecloud.blockvolumes.createvolumebackup.end",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "BlockVolumes",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_volumebackup via policy:gold",
    "resourceId": "ocid1.volumebackup.oc1..<unique_ID>",
    "additionalDetails": {
      "sourceType": "SCHEDULED",
      "volumeId": ""ocid1.volume.oc1..<unique_ID>"
    }
  }
}```
Boot Volume Event Types

These are the event types that boot volumes emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Boot Volume Compartment Begin</td>
<td>com.oraclecloud.blockvolumes.changebootvolumecompartment.begin</td>
</tr>
<tr>
<td>Change Boot Volume Compartment End</td>
<td>com.oraclecloud.blockvolumes.changebootvolumecompartment.end</td>
</tr>
<tr>
<td>Create Boot Volume Begin</td>
<td>com.oraclecloud.blockvolumes.createbootvolume.begin</td>
</tr>
<tr>
<td>Create Boot Volume End</td>
<td>com.oraclecloud.blockvolumes.createbootvolume.end</td>
</tr>
<tr>
<td>Delete Boot Volume Begin</td>
<td>com.oraclecloud.blockvolumes.deletebootvolume.begin</td>
</tr>
<tr>
<td>Delete Boot Volume End</td>
<td>com.oraclecloud.blockvolumes.deletebootvolume.end</td>
</tr>
<tr>
<td>Delete Boot Volume Kms Key Begin</td>
<td>com.oraclecloud.blockvolumes.deletebootvolumekmskey.begin</td>
</tr>
<tr>
<td>Update Boot Volume</td>
<td>com.oraclecloud.blockvolumes.updatebootvolume</td>
</tr>
<tr>
<td>Update Boot Volume Begin</td>
<td>com.oraclecloud.blockvolumes.updatebootvolume.begin</td>
</tr>
<tr>
<td>Update Boot Volume End</td>
<td>com.oraclecloud.blockvolumes.updatebootvolume.end</td>
</tr>
<tr>
<td>Update Boot Volume Kms Key Begin</td>
<td>com.oraclecloud.blockvolumes.updatebootvolumekmskey.begin</td>
</tr>
<tr>
<td>Update Boot Volume Kms Key End</td>
<td>com.oraclecloud.blockvolumes.updatebootvolumekmskey.end</td>
</tr>
</tbody>
</table>

Boot Volume Example

This is a reference event for boot volumes:

```json
{
    "eventType": "com.oraclecloud.blockvolumes.createbootvolume.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "BlockVolumes",
```
"eventTime": "2019-01-10T21:19:24Z",
"contentType": "application/json",
"data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"",
    "compartmentName": "example_name",
    "resourceName": "my_volume",
    "resourceId": "ocid1.volume.oc1..<unique_ID>"",
    "availabilityDomain": "<availability_domain>"
}
"eventID": ":<unique_ID>"",
"extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
}
}

Boot Volume Backup Event Types

These are the event types that boot volume backups emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Boot Volume Backup Compartment</td>
<td>com.oraclecloud.blockvolumes.changebootvolumebackup.compartment</td>
</tr>
<tr>
<td>Create Boot Volume Backup Begin</td>
<td>com.oraclecloud.blockvolumes.createbootvolumebackup.begin.</td>
</tr>
<tr>
<td>Create Boot Volume Backup End</td>
<td>com.oraclecloud.blockvolumes.createbootvolumebackup.end.</td>
</tr>
<tr>
<td>Delete Boot Volume Backup Begin</td>
<td>com.oraclecloud.blockvolumes.deletebootvolumebackup.begin.</td>
</tr>
<tr>
<td>Delete Boot Volume Backup End</td>
<td>com.oraclecloud.blockvolumes.deletebootvolumebackup.end.</td>
</tr>
<tr>
<td>Update Boot Volume Backup</td>
<td>com.oraclecloud.blockvolumes.updatebootvolumebackup.</td>
</tr>
</tbody>
</table>

Boot Volume Backup Example

This is a reference event for boot volume backups:

```json
{
    "eventType": "com.oraclecloud.blockvolumes.createbootvolume.end",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "BlockVolumes",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"",
        "compartmentName": "example_name",
        "resourceName": "my_volumebackup via policy:gold",
        "resourceId": "ocid1.volumebackup.oc1..<unique_ID>"",
        "additionalDetails": {
            "sourceType": "SCHEDULED",
            "volumeId": "ocid1.volume.oc1..<unique_ID>"
        }
    }
}
```
Volume Groups and Volume Group Backups

These are the event types that volume groups and volume group backups emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Volume Group Compartment</td>
<td>com.oraclecloud.blockvolumes.changevolumegroupcompartment</td>
</tr>
<tr>
<td>Change Volume Group Backup Compartment</td>
<td>com.oraclecloud.blockvolumes.changevolumegroupbackupcompartment</td>
</tr>
<tr>
<td>Create Volume Group</td>
<td>com.oraclecloud.blockvolumes.createvolumegroup</td>
</tr>
<tr>
<td>Create Volume Group Begin</td>
<td>com.oraclecloud.blockvolumes.createvolumegroup.begin</td>
</tr>
<tr>
<td>Create Volume Group End</td>
<td>com.oraclecloud.blockvolumes.createvolumegroup.end</td>
</tr>
<tr>
<td>Create Volume Group Backup Begin</td>
<td>com.oraclecloud.blockvolumes.createvolumegroupbackup.begin</td>
</tr>
<tr>
<td>Create Volume Group Backup End</td>
<td>com.oraclecloud.blockvolumes.createvolumegroupbackup.end</td>
</tr>
<tr>
<td>Delete Volume Group Begin</td>
<td>com.oraclecloud.blockvolumes.deletevolumegroup.begin</td>
</tr>
<tr>
<td>Delete Volume Group End</td>
<td>com.oraclecloud.blockvolumes.deletevolumegroup.end</td>
</tr>
<tr>
<td>Delete Volume Group Backup Begin</td>
<td>com.oraclecloud.blockvolumes.deletevolumegroupbackup.begin</td>
</tr>
<tr>
<td>Delete Volume Group Backup End</td>
<td>com.oraclecloud.blockvolumes.deletevolumegroupbackup.end</td>
</tr>
<tr>
<td>Update Volume Group</td>
<td>com.oraclecloud.blockvolumes.updatevolumegroup</td>
</tr>
<tr>
<td>Update Volume Group Backup</td>
<td>com.oraclecloud.blockvolumes.updatevolumegroupbackup</td>
</tr>
</tbody>
</table>

Volume Group Example

This is a reference event for volume groups:

```json
{
  "eventType": "com.oraclecloud.blockvolumes.createvolumegroup",
  "cloudEventsVersion": "0.1",
}
### Blockchain Platform

For details about events emitted by Blockchain Platform, see [Service Events](#).

### Budgets

Budgets resources that emit events:

- [Alert Rule Event Types](#) on page 1828
- [Budget Event Types](#) on page 1829
- [Create Triggered Alert Event Types](#) on page 1830

#### Alert Rule Event Types

These are the event types that alert rule emits:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Alert Rule</td>
<td>com.oraclecloud.budgets.createalertrule</td>
</tr>
<tr>
<td>Update Alert Rule</td>
<td>com.oraclecloud.budgets.updatealertrule</td>
</tr>
<tr>
<td>Delete Alert Rule</td>
<td>com.oraclecloud.budgets.deletealertrule</td>
</tr>
</tbody>
</table>

#### Alert Rule Example

This is a reference event for creating an alert:

```json
{
    "eventType": "com.oraclecloud.budgets.createalertrule",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "budgets",
    "eventID": "<unique_ID>",
    "eventTime": "2020-02-02T20:20:02.002Z",
    "contentType": "application/json",
    "data": {
        "eventName": "CreateAlertRule",
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```
Budget Event Types

These are the event types that budget emits:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Budget</td>
<td>com.oraclecloud.budgets.createbudget</td>
</tr>
<tr>
<td>Update Budget</td>
<td>com.oraclecloud.budgets.updatebudget</td>
</tr>
<tr>
<td>Delete Budget</td>
<td>com.oraclecloud.budgets.deletebudget</td>
</tr>
</tbody>
</table>

Budget Example

This is a reference event for updating a budget:

```json
{
    "eventType": "com.oraclecloud.budgets.updatebudget",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "budgets",
    "eventID": "<unique_ID>",
    "eventTime": "2020-02-02T20:20:02.002Z",
    "contentType": "application/json",
    "data": {
        "eventName": "UpdateBudget",
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "My test budget",
        "resourceId": "ocid1.budget.oc1.phx.<unique_ID>",
        "availabilityDomain": "availability_domain",
        "additionalDetails": {
            "targetCompartmentId": "ocid1.tenancy.oc1..<unique_ID>",
            "targetType": "COMPARTMENT"
        }
    },
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>
    }
}
```
Events

Create Triggered Alert Event Types
This is the event type that the create triggered alert emits:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Triggered Alert</td>
<td>com.oraclecloud.budgets.createtriggeredalert</td>
</tr>
</tbody>
</table>

Create Triggered Alert Example
This is a reference event for creating a triggered alert:

```json
{
   "eventType": "com.oraclecloud.budgets.createtriggeredalert",
   "cloudEventsVersion": "0.1",
   "eventTypeVersion": "2.0",
   "source": "budgets",
   "eventID": "<unique_ID>",
   "eventTime": "2020-02-02T20:20:02.002Z",
   "contentType": "application/json",
   "data": {
      "eventName": "CreateTriggeredAlert",
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
      "compartmentName": "example_compartment",
      "resourceId": "ocid1.triggeredalert.oc1.phx.<unique_ID>",
      "availabilityDomain": "availability_domain",
      "additionalDetails": {
         "budgetId": "ocid1.budget.oc1.phx.<unique_ID>",
         "alertRuleId": "ocid1.alertrule.oc1.phx.<unique_ID>"
      }
   }
}
```

Cloud Guard
Cloud Guard resources that emit events:
- Problems
- Targets

Problem Event Types
These are the event types that problems emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected-Problem</td>
<td>com.oraclecloud.cloudguard.problemdetected</td>
</tr>
<tr>
<td>Remediated-Problem</td>
<td>com.oraclecloud.cloudguard.problemremediated</td>
</tr>
</tbody>
</table>

Detected-Problem Example
This is a reference event for detected problems:

```json
{
}
```
Events

```
"eventType" : "com.oraclecloud.cloudguard.problemdetected",
"cloudEventsVersion" : "0.1",
"eventTypeVersion" : "2.0",
"source" : "CloudGuardResponderEngine",
"eventTime" : "2020-09-02T18:45:39Z",
"contentType" : "application/json",
"data" : {
    "compartmentId" : "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName" : "compartment_name",
    "resourceName" : "problem_name",
    "resourceId" : "ocid1.cloudguardproblem.oc1.iad.<unique_ID>",
    "additionalDetails" : {
        "tenantId" : "ocid1.tenancy.oc1..<unique_ID>",
        "problemDescription" : "problem_description",
        "riskLevel" : "LOW",
        "problemRecommendation" : "example_recommendation",
        "status" : "OPEN",
        "problemType" : "problem_type",
        "resourceName" : "resource_name",
        "resourceId" : "ocid1.vcn.oc1.iad.<unique_ID>",
        "resourceType" : "resource_type",
        "targetId" : "ocid1.cloudguardtarget.oc1..<unique_ID>",
        "labels" : "label1, label2",
        "firstDetected" : "2020-09-02T18:44:44.568Z",
        "lastDetected" : "2020-09-02T18:44:44.568Z",
        "region" : "us-ashburn-1"
    }
},
"eventID" : "<unique_ID>",
"extensions" : {
    "compartmentId" : "ocid1.compartment.oc1..<unique_ID>"
}
```

Remediated-Problem Example

This is a reference event for remediated problems:

```
{
    "eventType" : "com.oraclecloud.cloudguard.problemremediated",
    "cloudEventsVersion" : "0.1",
    "eventTypeVersion" : "2.0",
    "source" : "CloudGuardResponderEngine",
    "eventTime" : "2020-09-02T18:47:00Z",
    "contentType" : "application/json",
    "data" : {
        "compartmentId" : "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName" : "compartment_name",
        "resourceName" : "problem_name",
        "resourceId" : "ocid1.cloudguardproblem.oc1.iad.<unique_ID>",
        "additionalDetails" : {
            "tenantId" : "ocid1.tenancy.oc1..<unique_ID>",
            "problemDescription" : "problem_description",
            "riskLevel" : "CRITICAL",
            "problemRecommendation" : "example_recommendation",
            "status" : "RESOLVED",
            "problemType" : "problem_type",
            "resourceName" : "resource_name",
            "resourceId" : "ocid1.vcn.oc1.iad.<unique_ID>",
            "resourceType" : "resource_type",
            "targetId" : "ocid1.cloudguardtarget.oc1..<unique_ID>",
            "labels" : "label1, label2",
            "firstDetected" : "2020-09-02T18:44:44.145Z",
```
Target Event Types
These are the event types that targets emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target-Information</td>
<td>com.oraclecloud.cloudguard.targetinformation</td>
</tr>
</tbody>
</table>

Target-Information Example
This is a reference event for target information:

```json
{
  "eventType": "com.oraclecloud.cloudguard.targetinformation",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "CloudGuard",
  "eventTime": "2020-02-11T01:29:51.404Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  }
}
```

Compute
Compute resources that emit events:
- [Autoscaling Event Types](#) on page 1833
- [Cluster Network Event Types](#) on page 1834
Autoscaling Event Types

These are the event types that autoscaling configurations and autoscaling policies emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Autoscaling Configuration Compartment</td>
<td>com.oraclecloud.autoscaling.changeautoscalingconfigurationcompartment</td>
</tr>
<tr>
<td>Create Autoscaling Configuration</td>
<td>com.oraclecloud.autoscaling.createautoscalingconfiguration</td>
</tr>
<tr>
<td>Delete Autoscaling Configuration</td>
<td>com.oraclecloud.autoscaling.deleteautoscalingconfiguration</td>
</tr>
<tr>
<td>Scaling Action</td>
<td>com.oraclecloud.autoscaling.scalingaction</td>
</tr>
<tr>
<td>Update Autoscaling Configuration</td>
<td>com.oraclecloud.autoscaling.updateautoscalingconfiguration</td>
</tr>
<tr>
<td>Update Autoscaling Policy</td>
<td>com.oraclecloud.autoscaling.updateautoscalingpolicy</td>
</tr>
</tbody>
</table>

Autoscaling Example

This is a reference event for autoscaling:

```json
{
    "eventType": "com.oraclecloud.autoscaling.scalingaction",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "autoscaling",
    "eventTime": "2019-08-21T04:00:10.046Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "example autoscaling configuration",
        "resourceId": "ocid1.autoscalingconfiguration.oc1.phx.<unique_ID>",
        "additionalDetails": {
            "policyName": "my_policy_name",
            "ruleName": "my_scale_up_condition",
            "actionType": "SCALE_OUT",
            "previousSize": 1,
            "newSize": 2
        }
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>
    }
}
```
Cluster Network Event Types

These are the event types that cluster networks emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Cluster Network Compartment</td>
<td>com.oraclecloud.computemanagement.changeclusternetwork_compartment</td>
</tr>
<tr>
<td>Create Cluster Network Begin</td>
<td>com.oraclecloud.computemanagement.createclusternetwork.begin</td>
</tr>
<tr>
<td>Create Cluster Network End</td>
<td>com.oraclecloud.computemanagement.createclusternetwork.end</td>
</tr>
<tr>
<td>Terminate Cluster Network Begin</td>
<td>com.oraclecloud.computemanagement.terminateclusternetwork.begin</td>
</tr>
<tr>
<td>Terminate Cluster Network End</td>
<td>com.oraclecloud.computemanagement.terminateclusternetwork.end</td>
</tr>
</tbody>
</table>

Cluster Networks Example

This is a reference event for most cluster network events:

```json
{
   "eventType": "com.oraclecloud.computemanagement.createclusternetwork.begin",
   "cloudEventsVersion": "0.1",
   "eventTypeVersion": "2.0",
   "source": "ComputeManagement",
   "eventTime": "2019-09-12T21:45:09.036Z",
   "contentType": "application/json",
   "data": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
      "compartmentName": "example_compartment",
      "resourceName": "my_cluster_network",
      "resourceId": "ocid1.clusternetwork.oc1.uk-london-1.<unique_ID>",
      "availabilityDomain": "<availability_domain>",
   },
   "eventId": "<unique_ID>",
   "extensions": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
   }
}
```

Create cluster network end and terminate cluster network end don't include the availability domain.
## Console History Event Types

These are the event types that console histories emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Console History Begin</td>
<td>com.oraclecloud.computeapi.captureconsolehistory.begin</td>
</tr>
<tr>
<td>Capture Console History End</td>
<td>com.oraclecloud.computeapi.captureconsolehistory.end</td>
</tr>
<tr>
<td>Delete Console History</td>
<td>com.oraclecloud.computeapi.deleteconsolehistory</td>
</tr>
<tr>
<td>Update Console History</td>
<td>com.oraclecloud.computeapi.updateconsolehistory</td>
</tr>
</tbody>
</table>

### Console History Example

This is a reference event for console histories:

```json
{
    "eventType": "com.oraclecloud.computeapi.captureconsolehistory.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ComputeApi",
    "eventTime": "2019-08-20T21:58:13.554Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceId": "ocid1.consolehistory.oc1.iad.<unique_ID>",
        "availabilityDomain": "SoSC:PHX-AD-3"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```
Image Event Types

These are the event types that images emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Image Shape Compatibility</td>
<td>com.oraclecloud.computeapi.addimageshapecompatibility</td>
</tr>
<tr>
<td>Change Image Compartment</td>
<td>com.oraclecloud.computeapi.moveimage</td>
</tr>
<tr>
<td>Create Image Begin</td>
<td>com.oraclecloud.computeapi.createimage.begin</td>
</tr>
<tr>
<td>Create Image End</td>
<td>com.oraclecloud.computeapi.createimage.end</td>
</tr>
<tr>
<td>Delete Image</td>
<td>com.oraclecloud.computeapi.deleteimage</td>
</tr>
<tr>
<td>Export Image Begin</td>
<td>com.oraclecloud.computeapi.exportimage.begin</td>
</tr>
<tr>
<td>Export Image End</td>
<td>com.oraclecloud.computeapi.exportimage.end</td>
</tr>
<tr>
<td>Remove Image Shape Compatibility</td>
<td>com.oraclecloud.computeapi.removeimageshapecompatibility</td>
</tr>
<tr>
<td>Update Image</td>
<td>com.oraclecloud.computeapi.updateimage</td>
</tr>
</tbody>
</table>

Image Example

This is a reference event for most image events:

```json
{
    "eventType": "com.oraclecloud.computeapi.exportimage.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ComputeApi",
    "eventTime": "2019-08-27T04:12:37.397Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.tenancy.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "my_image",
        "resourceId": "ocid1.image.oc1.iad.<unique_ID>",
        "availabilityDomain": "SoSC:PHX-AD-3"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.tenancy.oc1..<unique_ID>"
    }
}
```

Change image compartment doesn't include the resource name or availability domain.
### Instance Event Types

These are the event types that Compute instances and instance attachments emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach Boot Volume Begin</td>
<td>com.oraclecloud.computeapi.attachbootvolume.begin</td>
</tr>
<tr>
<td>Attach Boot Volume End</td>
<td>com.oraclecloud.computeapi.attachbootvolume.end</td>
</tr>
<tr>
<td>Attach Secondary VNIC Begin</td>
<td>com.oraclecloud.computeapi.attachvnic.begin</td>
</tr>
<tr>
<td>Attach Secondary VNIC End</td>
<td>com.oraclecloud.computeapi.attachvnic.end</td>
</tr>
<tr>
<td>Attach Volume Begin</td>
<td>com.oraclecloud.computeapi.attachvolume.begin</td>
</tr>
<tr>
<td>Attach Volume End</td>
<td>com.oraclecloud.computeapi.attachvolume.end</td>
</tr>
<tr>
<td>Change Instance Compartment Begin</td>
<td>com.oraclecloud.computeapi.changeinstancecompartment.begin</td>
</tr>
<tr>
<td>Change Instance Compartment End</td>
<td>com.oraclecloud.computeapi.changeinstancecompartment.end</td>
</tr>
<tr>
<td>Detach Boot Volume Begin</td>
<td>com.oraclecloud.computeapi.detachbootvolume.begin</td>
</tr>
<tr>
<td>Detach Boot Volume End</td>
<td>com.oraclecloud.computeapi.detachbootvolume.end</td>
</tr>
<tr>
<td>Detach Secondary VNIC Begin</td>
<td>com.oraclecloud.computeapi.detachvnic.begin</td>
</tr>
<tr>
<td>Detach Secondary VNIC End</td>
<td>com.oraclecloud.computeapi.detachvnic.end</td>
</tr>
<tr>
<td>Detach Volume Begin</td>
<td>com.oraclecloud.computeapi.detachvolume.begin</td>
</tr>
<tr>
<td>Detach Volume End</td>
<td>com.oraclecloud.computeapi.detachvolume.end</td>
</tr>
<tr>
<td>Instance Action Begin</td>
<td>com.oraclecloud.computeapi.instanceaction.begin</td>
</tr>
<tr>
<td>Instance Action End</td>
<td>com.oraclecloud.computeapi.instanceaction.end</td>
</tr>
<tr>
<td>Launch Instance Begin</td>
<td>com.oraclecloud.computeapi.launchinstance.begin</td>
</tr>
<tr>
<td>Launch Instance End</td>
<td>com.oraclecloud.computeapi.launchinstance.end</td>
</tr>
<tr>
<td>Terminate Instance Begin</td>
<td>com.oraclecloud.computeapi.terminateinstance.begin</td>
</tr>
<tr>
<td>Terminate Instance End</td>
<td>com.oraclecloud.computeapi.terminateinstance.end</td>
</tr>
<tr>
<td>Update Instance</td>
<td>com.oraclecloud.computeapi.updateinstance</td>
</tr>
</tbody>
</table>
Events

Compute Instance Example

This is a reference event for most instance events (attach/detach volume and boot volume events don’t include additional details):

```
{
  "eventType": "com.oraclecloud.computeapi.launchinstance.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "ComputeApi",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "my_instance",
    "resourceId": "ocid1.instance.oc1.phx.<unique_ID>",
    "availabilityDomain": "SoSC:PHX-AD-3",
    "additionalDetails": {
      "imageId": "ocid1.image.oc1.phx.<unique_ID>",
      "shape": "VM.Standard2.1",
      "type": "CustomerVmi"
    }
  },
  "eventID": "<unique_ID>",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  }
}
```

This is a reference event for attach/detach VNIC events:

```
{
  "eventType": "com.oraclecloud.computeapi.attachvnic.end",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "ComputeApi",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "my_instance",
    "resourceId": "ocid1.instance.oc1.phx.<unique_ID>",
    "availabilityDomain": "SoSC:PHX-AD-3",
    "additionalDetails": {
      "subnetId": "ocid1.subnet.oc1.phx.<unique_ID>"
    }
  },
  "eventID": "<unique_ID>",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  }
}
```

This is a reference event for instance action events:

```
{
  "eventType": "com.oraclecloud.computeapi.instanceaction.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "ComputeApi",
  "eventTime": "2019-08-16T12:07:14.623Z",
```
Events

```
"contentType": "application/json",
"data": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  "compartmentName": "example_compartment",
  "resourceName": "my_instance",
  "resourceId": "ocid1.instance.oc1.phx.<unique_ID>",
  "availabilityDomain": "SoSC:PHX-AD-3",
  "additionalDetails": {
    "imageId": "ocid1.image.oc1.phx.<unique_ID>",
    "instanceActionType": "start",
    "shape": "VM.Standard2.1",
    "type": "CustomerVmi"
  }
},
"eventID": "<unique_ID>",
"extensions": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
}
}
```

**Instance Configuration Event Types**

These are the event types that Compute instance configurations emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Instance Configuration Compartment</td>
<td>com.oraclecloud.computemanagement.changeinstanceconfiguration</td>
</tr>
<tr>
<td>Create Instance Configuration</td>
<td>com.oraclecloud.computemanagement.createinstanceconfiguration</td>
</tr>
<tr>
<td>Delete Instance Configuration</td>
<td>com.oraclecloud.computemanagement.deleteinstanceconfiguration</td>
</tr>
<tr>
<td>Launch Instance Configuration Begin</td>
<td>com.oraclecloud.computemanagement.launchinstanceconfiguration.begin</td>
</tr>
<tr>
<td>Launch Instance Configuration End</td>
<td>com.oraclecloud.computemanagement.launchinstanceconfiguration.end</td>
</tr>
<tr>
<td>Update Instance Configuration</td>
<td>com.oraclecloud.computemanagement.updateinstanceconfiguration</td>
</tr>
</tbody>
</table>

**Compute Instance Configuration Example**

This is a reference event for most instance configuration events:

```
{
  "eventType": 
    "com.oraclecloud.computemanagement.createinstanceconfiguration",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "ComputeManagement",
  "eventTime": "2019-08-12T22:52:01.062Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "my_instance_configuration",
```
Launch instance configuration end doesn't include the availability domain.

**Instance Console Connection Event Types**

These are the event types that Compute instance console connections emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Instance Console Connection Begin</td>
<td><code>com.oraclecloud.computeapi.createinstanceconsoleconnection.begin</code></td>
</tr>
<tr>
<td>Create Instance Console Connection End</td>
<td><code>com.oraclecloud.computeapi.createinstanceconsoleconnection.end</code></td>
</tr>
<tr>
<td>Delete Instance Console Connection Begin</td>
<td><code>com.oraclecloud.computeapi.deleteinstanceconsoleconnection.begin</code></td>
</tr>
<tr>
<td>Delete Instance Console Connection End</td>
<td><code>com.oraclecloud.computeapi.deleteinstanceconsoleconnection.end</code></td>
</tr>
<tr>
<td>Update Instance Console Connection Begin</td>
<td><code>com.oraclecloud.computeapi.updateinstanceconsoleconnection.begin</code></td>
</tr>
<tr>
<td>Update Instance Console Connection End</td>
<td><code>com.oraclecloud.computeapi.updateinstanceconsoleconnection.end</code></td>
</tr>
</tbody>
</table>

**Compute Instance Console Connection Example**

This is a reference event for instance console connections:

```json
{
    "eventType": "com.oraclecloud.computeapi.createinstanceconsoleconnection.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ComputeApi",
    "eventTime": "2019-08-12T14:47:35.762Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceId": "ocid1.instanceconsoleconnection.oc1.phx..<unique_ID>",
        "availabilityDomain": "soSc:PHX-AD-3"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>
    }
}
```
## Instance Pool Event Types

These are the event types that Compute instance pools emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach Load Balancer Begin</td>
<td>com.oraclecloud.computemanagement.attachloadbalancer.begin</td>
</tr>
<tr>
<td>Attach Load Balancer End</td>
<td>com.oraclecloud.computemanagement.attachloadbalancer.end</td>
</tr>
<tr>
<td>Change Instance Pool Compartment</td>
<td>com.oraclecloud.computemanagement.changeinstancepoolcompartment</td>
</tr>
<tr>
<td>Create Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.createinstancepool.begin</td>
</tr>
<tr>
<td>Create Instance Pool End</td>
<td>com.oraclecloud.computemanagement.createinstancepool.end</td>
</tr>
<tr>
<td>Detach Load Balancer Begin</td>
<td>com.oraclecloud.computemanagement.detachloadbalancer.begin</td>
</tr>
<tr>
<td>Detach Load Balancer End</td>
<td>com.oraclecloud.computemanagement.detachloadbalancer.end</td>
</tr>
<tr>
<td>Reset Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.resetinstancepool.begin</td>
</tr>
<tr>
<td>Reset Instance Pool End</td>
<td>com.oraclecloud.computemanagement.resetinstancepool.end</td>
</tr>
<tr>
<td>Soft Reset Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.softresetinstancepool.begin</td>
</tr>
<tr>
<td>Soft Reset Instance Pool End</td>
<td>com.oraclecloud.computemanagement.softresetinstancepool.end</td>
</tr>
<tr>
<td>Start Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.startinstancepool.begin</td>
</tr>
<tr>
<td>Start Instance Pool End</td>
<td>com.oraclecloud.computemanagement.startinstancepool.end</td>
</tr>
<tr>
<td>Stop Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.stopinstancepool.begin</td>
</tr>
<tr>
<td>Stop Instance Pool End</td>
<td>com.oraclecloud.computemanagement.stopinstancepool.end</td>
</tr>
<tr>
<td>Terminate Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.terminateinstancepool.begin</td>
</tr>
<tr>
<td>Terminate Instance Pool End</td>
<td>com.oraclecloud.computemanagement.terminateinstancepool.end</td>
</tr>
<tr>
<td>Update Instance Pool Begin</td>
<td>com.oraclecloud.computemanagement.updateinstancepool.begin</td>
</tr>
<tr>
<td>Update Instance Pool End</td>
<td>com.oraclecloud.computemanagement.updateinstancepool.end</td>
</tr>
</tbody>
</table>
**Compute Instance Pools Example**

This is a reference event for most instance pool events:

```json
{
    "eventType": "com.oraclecloud.computemanagement.createinstancepool.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ComputeManagement",
    "eventTime": "2019-08-12T22:52:01.343Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "my_instance_pool",
        "resourceId": "ocid1.instancepool.oc1.phx..<unique_ID>",
        "availabilityDomain": "<availability_domain>",
    },
    "eventId": "<unique_id>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```

These instance pool events don’t include the availability domain: create instance pool end, detach load balancer end, reset instance pool end, soft reset instance pool end, start instance pool end, stop instance pool end, terminate instance pool end, and update instance pool end.

**Container Engine for Kubernetes**

Container Engine for Kubernetes resources that emit events:

- **Cluster Event Types** on page 1842
- **Node Pool Event Types** on page 1843

**Cluster Event Types**

These are the event types that clusters emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Cluster Begin</td>
<td><code>com.oraclecloud.clustersapi.createcluster.begin</code></td>
</tr>
<tr>
<td>Delete Cluster Begin</td>
<td><code>com.oraclecloud.clustersapi.deletecluster.begin</code></td>
</tr>
<tr>
<td>Update Cluster Begin</td>
<td><code>com.oraclecloud.clustersapi.updatecluster.begin</code></td>
</tr>
</tbody>
</table>

**Cluster Example**

This is an example event for clusters:

```json
{
    "eventType": "com.oraclecloud.clustersapi.createcluster.begin",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ClustersAPI",
    "eventId": "<unique_ID>",
    "eventTime": "2020-04-15T16:26:56.848Z",
```
Node Pool Event Types

These are the event types that node pools emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Node Pool Begin</td>
<td>com.oraclecloud.clustersapi.createnodepool.begin</td>
</tr>
<tr>
<td>Delete Node Pool Begin</td>
<td>com.oraclecloud.clustersapi.deletenodepool.begin</td>
</tr>
<tr>
<td>Update Node Pool Begin</td>
<td>com.oraclecloud.clustersapi.updatenodepool.begin</td>
</tr>
</tbody>
</table>

Node Pool Example

This is an example event for node pools:

```json
{
  "eventType": "com.oraclecloud.clustersapi.createnodepool.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "ClustersAPI",
  "eventID": "<unique_ID>",
  "eventTime": "2020-04-15T16:26:59.418Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": "<unique_ID>",
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "my_cluster",
    "resourceId": "ocid1.cluster.oc1.iad.<unique_ID>",
    "availabilityDomain": "my_availability_domain",
    "freeformTags": null,
    "definedTags": null
  }
}
```

Content and Experience

For details about events emitted by Content and Experience, see Service Events.

Database

Database resources that emit events:
Events

- **Autonomous Database events:**
  - Database Service: Autonomous Database Control Plane Event Types on page 1845
  - Database Service: Autonomous Database Data Plane Event Types on page 1846
  - Database Service: Autonomous Container Database Event Types on page 1849
  - Database Service: Autonomous Exadata Infrastructure Event Types on page 1851
- **Bare metal, virtual machine, and Exadata DB system events**
  - Database Service: DB System Event Types on page 1852
  - Database Service: Node (Virtual Machine) Event Types on page 1853
  - Database Service: Database Home Event Types on page 1854
  - Database Service: Database Event Types on page 1855
  - Database Service: Data Guard Association Event Types on page 1860
- **Exadata Cloud Service new infrastructure resource model events**
  - Database Service: Cloud Exadata Infrastructure Events on page 1856
  - Database Service: Exadata Cloud VM Cluster Events on page 1858
- **Data Guard association events**
  - DB system Data Guard Association Events
- **Exadata Cloud® Customer events:** See Oracle Exadata Cloud@Customer Events for full details.
# Database Service: Autonomous Database Control Plane Event Types

These are the event types that Autonomous Databases emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Failover Begin <em>(Emitted if database connection attempts fail for 5 minutes.)</em></td>
<td>com.oraclecloud.databaseservice.automaticfailoverautonomousdatabase.begin</td>
</tr>
<tr>
<td>Automatic Failover End <em>(Emitted after failover completes successfully or unsuccessfully. Unsuccessful automatic failovers may result in data loss. Check the Autonomous Database details page in the Oracle Cloud Infrastructure Console for additional information in the event of an unsuccessful automatic failover.)</em></td>
<td>com.oraclecloud.databaseservice.automaticfailoverautonomousdatabase.end</td>
</tr>
<tr>
<td>Change Compartment Begin</td>
<td>com.oraclecloud.databaseservice.changeautonomousdatabasecompartment.begin</td>
</tr>
<tr>
<td>Change Compartment End</td>
<td>com.oraclecloud.databaseservice.changeautonomousdatabasecompartment.end</td>
</tr>
<tr>
<td>Create Backup Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.database.backup.begin</td>
</tr>
<tr>
<td>Create Backup End</td>
<td>com.oraclecloud.databaseservice.autonomous.database.backup.end</td>
</tr>
<tr>
<td>Create Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.database.instance.create.begin</td>
</tr>
<tr>
<td>Create End</td>
<td>com.oraclecloud.databaseservice.autonomous.database.instance.create.end</td>
</tr>
<tr>
<td>Disable Data Guard Begin</td>
<td>com.oraclecloud.databaseservice.disableautonomousdataguard.begin</td>
</tr>
<tr>
<td>Disable Data Guard End</td>
<td>com.oraclecloud.databaseservice.disableautonomousdataguard.end</td>
</tr>
<tr>
<td>Enable Data Guard Begin</td>
<td>com.oraclecloud.databaseservice.enableautonomousdataguard.begin</td>
</tr>
<tr>
<td>Enable Data Guard End</td>
<td>com.oraclecloud.databaseservice.enableautonomousdataguard.end</td>
</tr>
<tr>
<td>Free Database Automatic Stop Reminder <em>(emitted 48 hours prior to database stop)</em></td>
<td>com.oraclecloud.databaseservice.freeautonomousdatabase.stop.reminder</td>
</tr>
<tr>
<td>Free Database Automatically Stopped</td>
<td>com.oraclecloud.databaseservice.freeautonomousdatabase.stopped</td>
</tr>
<tr>
<td>Free Database Automatic Termination Reminder <em>(emitted 48 hours prior to database termination)</em></td>
<td>com.oraclecloud.databaseservice.freeautonomousdatabase.termination.reminder</td>
</tr>
<tr>
<td>Free Database Automatically Terminated</td>
<td>com.oraclecloud.databaseservice.freeautonomousdatabase.terminated</td>
</tr>
<tr>
<td>Manual Failover Begin</td>
<td>com.oraclecloud.databaseservice.failoverautonomousdatabase.begin</td>
</tr>
<tr>
<td>Manual Failover End <em>(Emitted after failover completes successfully or unsuccessfully. Unsuccessful manual failovers may result in data loss. Check the Autonomous Database details page in the Oracle Cloud Infrastructure Console for additional information in the event of an unsuccessful manual failover.)</em></td>
<td>com.oraclecloud.databaseservice.failoverautonomousdatabase.end</td>
</tr>
<tr>
<td>Peer Database Provisioning Begin</td>
<td>com.oraclecloud.databaseservice.standbyinstance.create.begin</td>
</tr>
<tr>
<td>Peer Database Provisioning End</td>
<td>com.oraclecloud.databaseservice.standbyinstance.create.end</td>
</tr>
<tr>
<td>Restore Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.database.restore.begin</td>
</tr>
<tr>
<td>Restore End</td>
<td>com.oraclecloud.databaseservice.autonomous.database.restore.end</td>
</tr>
<tr>
<td>Start Begin</td>
<td>com.oraclecloud.databaseservice.startautonomousdatabase.begin</td>
</tr>
<tr>
<td>Start End</td>
<td>com.oraclecloud.databaseservice.startautonomousdatabase.end</td>
</tr>
<tr>
<td>Stop Begin</td>
<td>com.oraclecloud.databaseservice.stopautonomousdatabase.begin</td>
</tr>
<tr>
<td>Stop End</td>
<td>com.oraclecloud.databaseservice.stopautonomousdatabase.end</td>
</tr>
<tr>
<td>Switchover Begin</td>
<td>com.oraclecloud.databaseservice.switchoverautonomousdatabase.begin</td>
</tr>
<tr>
<td>Switchover End</td>
<td>com.oraclecloud.databaseservice.switchoverautonomousdatabase.end</td>
</tr>
<tr>
<td>Terminate Begin</td>
<td>com.oraclecloud.databaseservice.deleteautonomousdatabase.begin</td>
</tr>
<tr>
<td>Terminate End</td>
<td>com.oraclecloud.databaseservice.deleteautonomousdatabase.end</td>
</tr>
<tr>
<td>Update Begin</td>
<td>com.oraclecloud.databaseservice.updateautonomousdatabase.begin</td>
</tr>
<tr>
<td>Update End</td>
<td>com.oraclecloud.databaseservice.updateautonomousdatabase.end</td>
</tr>
<tr>
<td>Upgrade Begin</td>
<td>com.oraclecloud.databaseservice.upgradeautonomousdatabasedbversion.begin</td>
</tr>
<tr>
<td>Upgrade End</td>
<td>com.oraclecloud.databaseservice.upgradeautonomousdatabasedbversion.end</td>
</tr>
</tbody>
</table>
Autonomous Database Example

This is a reference event for Autonomous Databases:

```json
{
    "cloudEventsVersion": "0.1",
    "eventId": 
        "<unique_ID>"
    
    "eventType":
    "com.oraclecloud.databasemanager.autonomous.database.backup.begin",
    "source": "databaseservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-07-10T14:06:23Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_database",
        "resourceId": "ocid1.autonomousdatabase.oc1.phx.<unique_ID>",
        "availabilityDomain": "SoSC:PHX-AD-3",
        "freeFormTags": {},
        "definedTags": {},
        "additionalDetails": {
            "cpuCoreCount": 1,
            "lifecycleState": "PROVISIONING",
            "dataStorageSizeInTBs": 1,
            "timeCreated": "2019-07-10T14:06:10.905Z",
            "timeUpdated": "2019-07-10T14:06:10.905Z",
            "serviceConsoleUrl": null,
            "licenseType": null,
            "workloadType": "<Data Warehouse | Transaction Processing>",
            "autonomousDatabaseType": 
                "<Dedicated Infrastructure | Shared Infrastructure>",
        }
    }
}
```

Database Service: Autonomous Database Data Plane Event Types

Autonomous Databases emit "critical" and "information" data plane events. Information events provide important details about the database lifecycle, such as the time when maintenance begins and maintenance ends, or notifications of connections from a new IP address.

Critical events on Autonomous Database are issues that cause disruption to the database.

Both the "information" and "critical" event types use an additionalDetails section of the event message to provide specific details about what is happening within the Autonomous Database emitting the event. Details about the conditions and operations that trigger these two event types follow below.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>com.oraclecloud.databasemanager.autonomous.database.backup.begin</td>
</tr>
<tr>
<td>Information</td>
<td>com.oraclecloud.databasemanager.autonomous.database.backup.begin</td>
</tr>
</tbody>
</table>
In the following example of a "critical" event, you can see within the **additionalDetails** section of the event message that this particular message concerns a "database down" condition that has just ended. The **eventName** and **description** fields provide information regarding the critical situation within the "adwfinance" database:

```json
{
   "cloudEventsVersion": "0.1",
   "eventID": "<unique_ID>",
   "eventType": "com.oraclecloud.databaseservice.autonomous.database.critical",
   "source": "DatabaseService",
   ...
   "additionalDetails": {
      "eventName": "DatabaseDownEnd",
      "dbName": "adwfinance",
      "description": "adwfinance is up and ready for user operations.",
      "workloadType": "Data Warehouse",
      "autonomousDatabaseType": "Shared Infrastructure"
   }
}
```

In the tables below, you can read about the conditions and operations that trigger "critical" and "information" event types. Each condition or operation is identified by a unique **eventName** value.

<table>
<thead>
<tr>
<th>Critical Event - EventName</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AdminPasswordWarning</strong></td>
<td>Generated when Autonomous Database determines that the ADMIN password will expire after a 30 day grace period is complete. ADMIN passwords should be reset after no more than 360 days. The 30 day grace period begins after a password has been in use for 360 days. If the password is not reset during the grace period, the event is generated a second time, 30 days after the first event notification, to notify you that the password has expired and needs to be reset.</td>
</tr>
</tbody>
</table>
| **DatabaseDownBegin**      | The Autonomous Database instance cannot be opened, or the services such as high, low, medium, tp, or tpurgent are not started or available. The following conditions do not trigger **DatabaseDownBegin**:  
   • Operations performed during the maintenance window  
   • Load balancer, network, or backup related issues  
   • A user stopping the instance  
   This event will not be triggered if you are using Autonomous Data Guard and the standby database is not available due to any of the above conditions. |
### Critical Event - EventName

<table>
<thead>
<tr>
<th>EventName</th>
<th>Description</th>
</tr>
</thead>
</table>
| DatabaseDownEnd   | The database is recovered from the down state, meaning the Autonomous Database instance is opened with its services, following a DatabaseDownBegin event. DatabaseDownEnd is triggered only if there was a preceding DatabaseDownBegin event. The following conditions do not trigger DatabaseDownEnd:  
  - Operations performed during the maintenance window  
  - A user starting the instance  
  If you are using Autonomous Data Guard and the primary database goes down, this triggers a DatabaseDownBegin event. If the system fails over to the standby database, this triggers a DatabaseDownEnd event. |
| WalletExpirationWarning | Generated when Autonomous Database determines that a wallet is due to expire in less than six (6) weeks. This event is reported at most once per week.                                                                                                                                   |

### Information Event - EventName

<table>
<thead>
<tr>
<th>EventName</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DatabaseConnection</td>
<td>Generated if a connection is made to the database from a new IP address. A new IP address is defined as an address that has not connected to the database in the last 30 days.</td>
</tr>
<tr>
<td>MaintenanceBegin</td>
<td>Triggered when the maintenance starts and provides the start timestamp (in UTC) for the maintenance. Note: this event does not provide the scheduled start time.</td>
</tr>
<tr>
<td>MaintenanceEnd</td>
<td>Triggered when the maintenance ends and provides the end timestamp (in UTC) for the maintenance. Note: this event does not provide the scheduled end time.</td>
</tr>
<tr>
<td>NewMaintenanceSchedule</td>
<td>Generated when the maintenance date is updated and the new date is shown on the Oracle Cloud Infrastructure Console.</td>
</tr>
<tr>
<td>ScheduledMaintenanceWarning</td>
<td>Generated when the instance is 24 hours from a scheduled maintenance operation, and again when the instance is 1 hour (60 minutes) from the scheduled maintenance.</td>
</tr>
</tbody>
</table>

**Note:**

If you are using Autonomous Data Guard for shared Exadata infrastructure, any of the above listed events that occurs on the standby database does not trigger an Information event.
**Database Service: Autonomous Container Database Event Types**

These are the event types that Autonomous Container Databases emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Compartment</td>
<td>com.oraclecloud.databaseservice.changeautonomouscontainerdatabase.begin</td>
</tr>
<tr>
<td>Create Backup Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.backup.begin</td>
</tr>
<tr>
<td>Create Backup End</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.backup.end</td>
</tr>
<tr>
<td>Create Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.instance.create.begin</td>
</tr>
<tr>
<td>Create End</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.instance.create.end</td>
</tr>
<tr>
<td>Maintenance Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.maintenance.begin</td>
</tr>
<tr>
<td>Maintenance End</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.maintenance.end</td>
</tr>
<tr>
<td>Maintenance Reminder</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.maintenance.reminder</td>
</tr>
<tr>
<td>Maintenance Scheduled</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.maintenance.scheduled</td>
</tr>
<tr>
<td>Restart Begin</td>
<td>com.oraclecloud.databaseservice.restartautonomouscontainerdatabase.begin</td>
</tr>
<tr>
<td>Restart End</td>
<td>com.oraclecloud.databaseservice.restartautonomouscontainerdatabase.end</td>
</tr>
<tr>
<td>Restore Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.restore.begin</td>
</tr>
<tr>
<td>Restore End</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.restore.end</td>
</tr>
<tr>
<td>Terminate Begin</td>
<td>com.oraclecloud.databaseservice.terminateautonomouscontainerdatabase.begin</td>
</tr>
<tr>
<td>Terminate End</td>
<td>com.oraclecloud.databaseservice.terminateautonomouscontainerdatabase.end</td>
</tr>
<tr>
<td>Update Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.instance.update.begin</td>
</tr>
<tr>
<td>Update End</td>
<td>com.oraclecloud.databaseservice.autonomous.container.database.instance.update.end</td>
</tr>
</tbody>
</table>
Events

**Autonomous Container Database Example**

This is a reference event for Autonomous Container Databases:

```
{
    "cloudEventsVersion": "0.1",
    "eventID": "<unique_ID>",
    "eventType": "com.oraclecloud.databaseservice.autonomous.container.database.backup.begin",
    "source": "databaseservice",
    "eventTypeVersion": "2.0",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_container_database",
        "resourceId": "<unique_ID>",
        "availabilityDomain": "all",
        "freeFormTags": {},
        "definedTags": {},
        "additionalDetails": {
            "cpuCoreCount": null,
            "lifecycleState": "ACTIVE",
            "dataStorageSizeInTBs": null,
            "timeCreated": "2019-06-27T21:15:59.000Z",
            "dbUniqueName": "dwrrdtsr_phx289",
            "dbHomeId": "ocid1.autonomoushome.oc1.phx.<unique_ID>",
            "dbName": "dwrrdtsr"
        }
    }
}
```
Database Service: Autonomous Exadata Infrastructure Event Types

These are the event types that Autonomous Exadata Infrastructure instances emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Compartment</td>
<td>com.oraclecloud.databaseservice.changeautonomousexadatainfrastructurebegin</td>
</tr>
<tr>
<td>Create Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.instance.create.begin</td>
</tr>
<tr>
<td>Create End</td>
<td>com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.instance.create.end</td>
</tr>
<tr>
<td>Maintenance Begin</td>
<td>com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.maintenance.begin</td>
</tr>
<tr>
<td>Maintenance End</td>
<td>com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.maintenance.end</td>
</tr>
<tr>
<td>Maintenance Reminder</td>
<td>com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.maintenance.reminder</td>
</tr>
<tr>
<td>Maintenance Scheduled</td>
<td>com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.maintenance.scheduled</td>
</tr>
<tr>
<td>Terminate Begin</td>
<td>com.oraclecloud.databaseservice.terminateautonomousexadatainfrastructure.begin</td>
</tr>
<tr>
<td>Terminate End</td>
<td>com.oraclecloud.databaseservice.terminateautonomousexadatainfrastructure.end</td>
</tr>
<tr>
<td>Update Begin</td>
<td>com.oraclecloud.databaseservice.updateautonomousexadatainfrastructure.begin</td>
</tr>
<tr>
<td>Update End</td>
<td>com.oraclecloud.databaseservice.updateautonomousexadatainfrastructure.end</td>
</tr>
</tbody>
</table>

Autonomous Exadata Infrastructure Example

This is a reference event for Autonomous Exadata Infrastructure instances:

```json
{
    "cloudeventsVersion": "0.1",
    "eventId": "<unique_ID>",
    "eventType": "com.oraclecloud.databaseservice.autonomous.exadata.infrastructure.instance.create.begin",
    "source": "databaseservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-07-10T23:28:12Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "resourceName": "my_exadata_infrastructure_name",
        "compartmentName": "example_compartment_name"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment_name",
        "resourceName": "my_exadata_infrastructure_name"
    }
}
```
Database Service: DB System Event Types

These are the event types that DB systems emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Compartment Begin</td>
<td>com.oraclecloud.databaseservice.changedbsystemcompartment.begin</td>
</tr>
<tr>
<td>Change Compartment End</td>
<td>com.oraclecloud.databaseservice.changedbsystemcompartment.end</td>
</tr>
<tr>
<td>Create Begin</td>
<td>com.oraclecloud.databaseservice.launchdbsystem.begin</td>
</tr>
<tr>
<td>Create End</td>
<td>com.oraclecloud.databaseservice.launchdbsystem.end</td>
</tr>
<tr>
<td>Terminate Begin</td>
<td>com.oraclecloud.databaseservice.terminatedbsystem.begin</td>
</tr>
<tr>
<td>Terminate End</td>
<td>com.oraclecloud.databaseservice.terminatedbsystem.end</td>
</tr>
<tr>
<td>Update IORM Begin</td>
<td>com.oraclecloud.databaseservice.updateiormconfig.begin</td>
</tr>
<tr>
<td>Update IORM End</td>
<td>com.oraclecloud.databaseservice.updateiormconfig.end</td>
</tr>
</tbody>
</table>

DB System Example

This is a reference event for DB Systems:

```json
{
    "cloudEventsVersion": "0.1",
    "contentType": "application/json",
    "data": {
        "additionalDetails": {
            "cpuCoreCount": 1,
            "dataStoragePercentage": 80,
            "dataStorageSizeInGBs": 256,
            "exadataIormConfig": "null",
            "dataStorageSizeInTBs": null,
            "timeCreated": "2019-07-10T23:13:43.136Z",
            "timeUpdated": "2019-07-10T23:28:12.390Z",
            "lifecycleState": "PROVISIONING",
            "availabilityDomain": "XXIT:PHX-AD-3",
            "resourceId": "ocid1.autonomousexainfrastructure.oc1.phx.<unique_ID>",
            "additionalDetails": {
                "cpuCoreCount": 92,
                "lifecycleState": "PROVISIONING",
                "dataStorageSizeInTBs": null,
                "timeCreated": "2019-07-10T23:13:43.136Z",
                "timeUpdated": "2019-07-10T23:28:12.390Z",
                "serviceConsoleUrl": null,
                "licenseType": null,
                "dbName": null
            }
        }
    }
}
```
Database Service: Node (Virtual Machine) Event Types

These are the event types that database nodes emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Begin</td>
<td>com.oraclecloud.databaseservice.dbnodeaction.end</td>
</tr>
<tr>
<td>Update End</td>
<td>com.oraclecloud.databaseservice.dbnodeaction.end</td>
</tr>
</tbody>
</table>

DB System Node Example

This is a reference event for DB system nodes:

```json
{
    "cloudEventsVersion": "0.1",
    "eventID": "<unique_ID>",
    "eventType": "com.oraclecloud.databaseservice.db.node.reboot.begin",
    "source": "databaseservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-07-29T04:43:24Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "",
        "resourceId": "ocid1.dbnode.oc1.phx.<unique_ID>",
        "availabilityDomain": "TGjA:PHX-AD-2",
        "freeFormTags": null,
        "definedTags": null,
        "additionalDetails": {
            "cpuCoreCount": null,
            "lifecycleState": "STARTING",
        }
    }
}
```
Database Service: Database Home Event Types

These are the event types that Database Homes emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Begin</td>
<td>com.oraclecloud.databaseservice.createdbhome.begin</td>
</tr>
<tr>
<td>Create End</td>
<td>com.oraclecloud.databaseservice.createdbhome.end</td>
</tr>
<tr>
<td>Terminate Begin</td>
<td>com.oraclecloud.databaseservice.deletedbhome.begin</td>
</tr>
<tr>
<td>Terminate End</td>
<td>com.oraclecloud.databaseservice.deletedbhome.end</td>
</tr>
<tr>
<td>Update Begin</td>
<td>com.oraclecloud.databaseservice.updatedbhome.begin</td>
</tr>
<tr>
<td>Update End</td>
<td>com.oraclecloud.databaseservice.updatedbhome.end</td>
</tr>
</tbody>
</table>

Database Home Example

This is a reference event for Database Homes:

```json
{
    "cloudEventsVersion": "0.1",
    "eventID": "60600c06-d6a7-4e85-b56a-1de3e6042f57",
    "eventType": "com.oraclecloud.databaseservice.createdbhome.begin",
    "source": "databaseservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-08-29T21:16:04Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1.<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "my_dbhome",
        "resourceId": "DbHome-unique_ID",
        "availabilityDomain": "all",
        "freeFormTags": {},
        "definedTags": {},
        "additionalDetails": {
```
Database Service: Database Event Types

These are the event types that databases in bare metal DB systems, virtual machine DB systems, and Exadata Cloud Service instances emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Backup Begin</td>
<td>com.oraclecloud.databaseservice.automaticbackupdatabase.begin</td>
</tr>
<tr>
<td>Automatic Backup End</td>
<td>com.oraclecloud.databaseservice.automaticbackupdatabase.end</td>
</tr>
<tr>
<td>Create Backup Begin</td>
<td>com.oraclecloud.databaseservice.backupdatabase.begin</td>
</tr>
<tr>
<td>Create Backup End</td>
<td>com.oraclecloud.databaseservice.backupdatabase.end</td>
</tr>
<tr>
<td>Delete Backup Begin</td>
<td>com.oraclecloud.databaseservice.deletebackup.begin</td>
</tr>
<tr>
<td>Delete Backup End</td>
<td>com.oraclecloud.databaseservice.deletebackup.end</td>
</tr>
<tr>
<td>Restore Begin</td>
<td>com.oraclecloud.databaseservice.restoredatabase.begin</td>
</tr>
<tr>
<td>Restore End</td>
<td>com.oraclecloud.databaseservice.restoredatabase.end</td>
</tr>
<tr>
<td>Update Begin</td>
<td>com.oraclecloud.databaseservice.updatedatabase.begin</td>
</tr>
<tr>
<td>Update End</td>
<td>com.oraclecloud.databaseservice.updatedatabase.end</td>
</tr>
<tr>
<td>Upgrade Begin</td>
<td>com.oraclecloud.databaseservice.upgradedatabase.begin</td>
</tr>
<tr>
<td>Upgrade End</td>
<td>com.oraclecloud.databaseservice.upgradedatabase.end</td>
</tr>
</tbody>
</table>

Database Example
This is a reference event for databases:

```json
{
  "eventType": "com.oraclecloud.databaseservice.backupdatabase.begin",
  "udEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DatabaseService",
  "eventTime": "2020-01-08T17:31:43.666Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
    "compartmentName": "example_compartment_name",
    "resourceName": "my_backup",
    "resourceId": "ocid1.dbbkup.oc1.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "additionalDetails": {
      "timeCreated": "2020-01-08T17:31:44Z",
      "lifecycleState": "CREATING",
      "dbSystemId": "ocid1.dbsystem.oc1.<unique_ID>",
      "dbHomeId": "ocid1.dbhome.oc1.<unique_ID>",
      "dbUniqueName": DB1115_iad1dv",
      "dbVersion": "11.2.0.4.190716",
      "databaseEdition": "ENTERPRISE_EDITION_HIGH_PERFORMANCE",
      "autoBackupsEnabled": "false",
      "backupType": "FULL",
      "databaseId": "ocid1.database.oc1.<unique_ID>",
    },
    "definedTags": {
      "My_example_tag_name": {
        "Example_key": "Example_value"
      }
    },
    "eventID": "<unique_ID>",
    "extensions": {
      "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
    }
  }
}
```

Database Service: Cloud Exadata Infrastructure Events

**Note:**

See Database Service: DB System Event Types on page 1852 for additional events related to Exadata DB systems. The events in this section are emitted for systems using the [new Exadata resource model](https://docs.oracle.com/en/cloud/middleware/database/oracle-cloud-infrastructure/userguide/cloud-exadata-resource-model.html).

These are the event types that cloud Exadata infrastructure resources emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Exadata Infrastructure - Create Begin</td>
<td>com.oraclecloud.databaseservice.createcloudexadatainfrastructure.begin</td>
</tr>
<tr>
<td>Cloud Exadata Infrastructure - Create End</td>
<td>com.oraclecloud.databaseservice.createcloudexadatainfrastructure.end</td>
</tr>
<tr>
<td>Cloud Exadata Infrastructure - Change Compartment Begin</td>
<td>com.oraclecloud.databaseservice.changecloudexadatainfrastructurecompartment.begin</td>
</tr>
<tr>
<td>Cloud Exadata Infrastructure - Change Compartment End</td>
<td>com.oraclecloud.databaseservice.changecloudexadatainfrastructurecompartment.end</td>
</tr>
<tr>
<td>Cloud Exadata Infrastructure - Update Begin</td>
<td>com.oraclecloud.databaseservice.updatecloudexadatainfrastructure.begin</td>
</tr>
<tr>
<td>Cloud Exadata Infrastructure - Update End</td>
<td>com.oraclecloud.databaseservice.updatecloudexadatainfrastructure.end</td>
</tr>
</tbody>
</table>
This is a reference event for a Cloud Exadata Infrastructure resource:

```json
{
  "cloudEventsVersion": "0.1",
  "eventId": "<unique_ID>",
  "eventType": "com.oraclecloud.databaseservice.cloudexadatainfrastructuremaintenance.end",
  "source": "DatabaseService",
  "eventTypeVersion": "1.0",
  "eventTime": "2019-06-27T21:16:04.000Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_exadata_infrastructure",
    "resourceId": "ocid1.dbsystem.oc1.eu-frankfurt-1.<unique_ID>",
    "availabilityDomain": "tXPJ:EU-FRANKFURT-1-AD-3",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "subnetId": "ocid1.subnet.oc1.eu-frankfurt-1.<unique_ID>",
      "lifecycleState": "MAINTENANCE_IN_PROGRESS",
      "sshPublicKeys": "...",
      "cpuCoreCount": 32,
      "version": "19.2.8.0.0.191119",
      "nsgIds": "null",
      "backupSubnetId": "ocid1.subnet.oc1.eu-frankfurt-1.<unique_ID>",
      "licenseType": "BRING_YOUR_OWN_LICENSE",
      "dataStoragePercentage": 80,
      "patchHistoryEntries": "null",
      "lifecycleMessage": "The underlying infrastructure of this system (cell storage) is being updated and this will not impact database availability.",
      "exadataIormConfig": "ExadataIormConfigCache(lifecycleState=DISABLED, lifecycleDetails=null, objective=Auto",
```

Oracle Cloud Infrastructure User Guide 1857
Database Service: Exadata Cloud VM Cluster Events

Note:

See Database Service: DB System Event Types on page 1852 for additional events related to Exadata DB systems. The events in this section are emitted for systems using the new Exadata resource model.
These are the event types that Exadata Cloud VM cluster resources emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud VM Cluster - Create Begin</td>
<td>com.oraclecloud.databaseservice.createcloudvmcluster.begin</td>
</tr>
<tr>
<td>Cloud VM Cluster - Create End</td>
<td>com.oraclecloud.databaseservice.createcloudvmcluster.end</td>
</tr>
<tr>
<td>Cloud VM Cluster - Change Compartment Begin</td>
<td>com.oraclecloud.databaseservice.changecloudvmclustercompartment.begin</td>
</tr>
<tr>
<td>Cloud VM Cluster - Change Compartment End</td>
<td>com.oraclecloud.databaseservice.changecloudvmclustercompartment.end</td>
</tr>
<tr>
<td>Cloud VM Cluster - Update Begin</td>
<td>com.oraclecloud.databaseservice.updatecloudvmcluster.begin</td>
</tr>
<tr>
<td>Cloud VM Cluster - Update End</td>
<td>com.oraclecloud.databaseservice.updatecloudvmcluster.end</td>
</tr>
<tr>
<td>Cloud VM Cluster - Update IORM Configuration Begin</td>
<td>com.oraclecloud.databaseservice.updatecloudvmclusteriormconfig.begin</td>
</tr>
<tr>
<td>Cloud VM Cluster - Update IORM Configuration End</td>
<td>com.oraclecloud.databaseservice.updatecloudvmclusteriormconfig.end</td>
</tr>
<tr>
<td>Cloud VM Cluster - Delete Begin</td>
<td>com.oraclecloud.databaseservice.deletecloudvmcluster.begin</td>
</tr>
<tr>
<td>Cloud VM Cluster - Delete End</td>
<td>com.oraclecloud.databaseservice.deletecloudvmcluster.end</td>
</tr>
</tbody>
</table>

This is a reference event for a cloud VM cluster resource:

```json
{
    "cloudEventsVersion": "0.1",
    "eventID": "<unique_ID>",
    "eventType": "com.oraclecloud.databaseservice.updatecloudvmclusteriormconfig.begin",
    "source": "databaseservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2022-06-27T21:16:04.000Z",
    "contentType": "application/json",
    "data": {
        "eventGroupingId": "<unique_ID>",
        "eventName": "UpdateCloudVmClusterIormConfig",
        "compartmentName": "example_compartment",
        "resourceName": "my_container_database",
        "resourceId": "ocid1.cloudvmcluster.oc1.<unique_ID>",
        "resourceVersion": null,
        "additionalDetails": {
            "cloudExadataInfrastructureId": "ocid1.cloudexadatainfrastructure.oc1.<unique_ID>",
            "freeFormTags": {},
            "definedTags": {},
            "licenseType": "BRING_YOUR_OWN_LICENSE",
            "lifecycleState": "AVAILABLE",
```
Database Service: Data Guard Association Event Types

These are the event types that Data Guard associations emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Guard Association - Create Begin</td>
<td>com.oraclecloud.databaseservice.createdataguardassociation.begin</td>
</tr>
<tr>
<td>Data Guard Association - Create End</td>
<td>com.oraclecloud.databaseservice.createdataguardassociation.end</td>
</tr>
<tr>
<td>Data Guard Association - Failover Begin</td>
<td>com.oraclecloud.databaseservice.failoverataguardassociation.begin</td>
</tr>
<tr>
<td>Data Guard Association - Failover End</td>
<td>com.oraclecloud.databaseservice.failoverataguardassociation.end</td>
</tr>
<tr>
<td>Data Guard Association - Reinstate Begin</td>
<td>com.oraclecloud.databaseservice.reinstatedataguardassociation.begin</td>
</tr>
<tr>
<td>Data Guard Association - Reinstate End</td>
<td>com.oraclecloud.databaseservice.reinstatedataguardassociation.end</td>
</tr>
<tr>
<td>Data Guard Association - Switchover Begin</td>
<td>com.oraclecloud.databaseservice.switchoverataguardassociation.begin</td>
</tr>
<tr>
<td>Data Guard Association - Switchover End</td>
<td>com.oraclecloud.databaseservice.switchoverataguardassociation.end</td>
</tr>
</tbody>
</table>

Data Guard Association Example

This is a reference event for Data Guard associations:

```json
{
   "cloudEventsVersion": "0.1",
   "contentType": "application/json",
   "data": {
      "additionalDetails": {
         "ApplyLag": null,
         "DGConfigId": "7e8eff2b-a4cd-474a-abd5-940b05c0b1fd",
         "DGConfigState": "null",
         "DatabaseId": "ocid1.database.oc1.iad.<unique_ID>",
         "DbHomeId": "ocid1.dbhome.oc1.iad.<unique_ID>",
         "DbSystemId": "ocid1.dbsystem.oc1.iad.<unique_ID>",
         "LastSyncedTime": null,
         "SyncState": "null",
         "dcsDgUpdateTimestamp": null,
         "lastUpdatedIdentifier": null,
         "lifeCycleMessage": null,
         "lifecycleState": "PROVISIONING",
      }
   }
}```
    
    "availabilityDomain": "XXIT:US-ASHBURN-AD-1",
    "compartmentId": "ocid1.compartment.oc1.<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceId": "ocid1.dgassociation.oc1.iad.<unique_ID>
},
    "eventId": "5<unique_ID>-4730-9761-e52715b7bc79",
    "eventType": "com.oraclecloud.databaseservice.createdataguardassociation.begin",
    "eventTypeVersion": "2.0",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1.<unique_ID>
    ,
    "source": "DatabaseService"}
## Database Service: External Database Event Types

These are the event types that external database resources emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Container Database - Change Compartment Begin</td>
<td>com.oraclecloud.databaseservice.changeexternalcontainerdatabasebegin</td>
</tr>
<tr>
<td>External Container Database - Change Compartment End</td>
<td>com.oraclecloud.databaseservice.changeexternalcontainerdatabaseend</td>
</tr>
<tr>
<td>External Container Database - Create</td>
<td>com.oraclecloud.databaseservice.createexternalcontainerdatabase</td>
</tr>
<tr>
<td>External Container Database - Delete Begin</td>
<td>com.oraclecloud.databaseservice.deleteexternalcontainerdatabasebegin</td>
</tr>
<tr>
<td>External Container Database - Delete End</td>
<td>com.oraclecloud.databaseservice.deleteexternalcontainerdatabaseend</td>
</tr>
<tr>
<td>External Container Database - Disable Database Management Service Begin</td>
<td>com.oraclecloud.databaseservice.disabledatabasemanagementserviceforexternalcontainerdatabasebegin</td>
</tr>
<tr>
<td>External Container Database - Disable Database Management Service End</td>
<td>com.oraclecloud.databaseservice.disabledatabasemanagementserviceforexternalcontainerdatabaseend</td>
</tr>
<tr>
<td>External Container Database - Enable Database Management Service Begin</td>
<td>com.oraclecloud.databaseservice.enabledatabasemanagementserviceforexternalcontainerdatabasebegin</td>
</tr>
<tr>
<td>External Container Database - Enable Database Management Service End</td>
<td>com.oraclecloud.databaseservice.enabledatabasemanagementserviceforexternalcontainerdatabaseend</td>
</tr>
<tr>
<td>External Container Database - Scan Pluggable Databases Begin</td>
<td>com.oraclecloud.databaseservice.scanexternalcontainerdatabasepluggabledatabasesbegin</td>
</tr>
<tr>
<td>External Container Database - Scan Pluggable Databases End</td>
<td>com.oraclecloud.databaseservice.scanexternalcontainerdatabasepluggabledatabasesend</td>
</tr>
<tr>
<td>External Container Database - Update Begin</td>
<td>com.oraclecloud.databaseservice.updateexternalcontainerdatabasebegin</td>
</tr>
<tr>
<td>External Container Database - Update End</td>
<td>com.oraclecloud.databaseservice.updateexternalcontainerdatabaseend</td>
</tr>
<tr>
<td>External Database Connector - Check Status Begin</td>
<td>com.oraclecloud.databaseservice.checkexternaldatabaseconnectorconnectionstatusbegin</td>
</tr>
<tr>
<td>External Database Connector - Check Status End</td>
<td>com.oraclecloud.databaseservice.checkexternaldatabaseconnectorconnectionstatusend</td>
</tr>
<tr>
<td>External Database Connector - Create Begin</td>
<td>com.oraclecloud.databaseservice.createexternaldatabaseconnectorbegin</td>
</tr>
<tr>
<td>External Database Connector - Create End</td>
<td>com.oraclecloud.databaseservice.createexternaldatabaseconnectorend</td>
</tr>
<tr>
<td>External Database Connector - Delete</td>
<td>com.oraclecloud.databaseservice.deleteexternaldatabaseconnector</td>
</tr>
<tr>
<td>External Database Connector - Update Begin</td>
<td>com.oraclecloud.databaseservice.updateexternaldatabaseconnectorbegin</td>
</tr>
<tr>
<td>External Database Connector - Update End</td>
<td>com.oraclecloud.databaseservice.updateexternaldatabaseconnectorend</td>
</tr>
<tr>
<td>External Non-Container Database - Change Compartment Begin</td>
<td>com.oraclecloud.databaseservice.changeexternalnoncontainerdatabasecompartmentbegin</td>
</tr>
<tr>
<td>External Non-Container Database - Change Compartment End</td>
<td>com.oraclecloud.databaseservice.changeexternalnoncontainerdatabasecompartmentend</td>
</tr>
<tr>
<td>External Non-Container Database - Create</td>
<td>com.oraclecloud.databaseservice.createexternalnoncontainerdatabase</td>
</tr>
<tr>
<td>External Non-Container Database - Delete Begin</td>
<td>com.oraclecloud.databaseservice.deleteexternalnoncontainerdatabasebegin</td>
</tr>
<tr>
<td>External Non-Container Database - Delete End</td>
<td>com.oraclecloud.databaseservice.deleteexternalnoncontainerdatabaseend</td>
</tr>
<tr>
<td>External Non-Container Database - Enable Database Management Service Begin</td>
<td>com.oraclecloud.databaseservice.enabledatabasemanagementserviceforexternalnoncontainerdatabasebegin</td>
</tr>
<tr>
<td>External Non-Container Database - Enable Database Management Service End</td>
<td>com.oraclecloud.databaseservice.enabledatabasemanagementserviceforexternalnoncontainerdatabaseend</td>
</tr>
<tr>
<td>External Non-Container Database - Disable Database Management Service Begin</td>
<td>com.oraclecloud.databaseservice.disabledatabasemanagementserviceforexternalnoncontainerdatabasebegin</td>
</tr>
<tr>
<td>External Non-Container Database - Disable Database Management Service End</td>
<td>com.oraclecloud.databaseservice.disabledatabasemanagementserviceforexternalnoncontainerdatabaseend</td>
</tr>
<tr>
<td>External Non-Container Database - Update Begin</td>
<td>com.oraclecloud.databaseservice.updateexternalnoncontainerdatabasebegin</td>
</tr>
<tr>
<td>External Non-Container Database - Update End</td>
<td>com.oraclecloud.databaseservice.updateexternalnoncontainerdatabaseend</td>
</tr>
<tr>
<td>External Database Connector - Update Begin</td>
<td>com.oraclecloud.databaseservice.updateexternaldatabaseconnectorbegin</td>
</tr>
<tr>
<td>External Database Connector - Update End</td>
<td>com.oraclecloud.databaseservice.updateexternaldatabaseconnectorend</td>
</tr>
</tbody>
</table>
External Container Database Example

```json
{
    "compartmentId": "ocid1.compartment.oc1.......unique_id",
    "compartmentName": "example_name",
    "resourceName": "ocid1.externalnoncontainerdatabase.oc1.......unique_id",
    "resourceId": "ocid1.externalnoncontainerdatabase.oc1.......unique_id",
    "availabilityDomain": "XXIT:PHX-AD-1",
    "freeFormTags": {},
    "definedTags": {},
    "additionalDetails": {
        "id": "ocid1.externalnoncontainerdatabase.oc1.......unique_id",
        "timeCreated": "2020-11-13T21:15:59.000Z",
        "timeUpdated": "2020-11-13T21:15:59.000Z",
        "lifecycleState": "AVAILABLE",
        "lifecycleDetails": "External Non Container Database is available",
        "dbUniqueName": "NCDB122_phx16q",
        "dbId": "3455094890",
        "dbVersion": "12.2.0.1.0",
        "dbEdition": "Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production",
        "timeZone": "US/Pacific",
        "externalCDBId": "ocid1.externalnoncontainerdatabase.oc1.......unique_id",
        "databaseManagementServiceStatus": "ENABLED",
        "databaseManagementServiceConnectorId": "ocid1.externaldatabaseconnector.oc1.......unique_id"
    }
}
```

External Database Connector Example

```json
{
    "compartmentId": "ocid1.compartment.oc1.......unique_id",
    "compartmentName": "example_name",
    "resourceName": "Example connector display name",
    "resourceId": "ocid1.externaldatabaseconnector.oc1.......unique_id",
    "availabilityDomain": "XXIT:PHX-AD-1",
    "freeFormTags": {},
    "definedTags": {},
    "additionalDetails": {
        "id": "ocid1.externaldatabaseconnector.oc1.......unique_id",
        "timeCreated": "2020-11-13T21:15:59.000Z",
        "timeUpdated": "2020-11-13T21:15:59.000Z",
        "connectorType": "MACS",
        "connectorAgentId": "ocid1.macsagent.oc1.......unique_id",
        "lifecycleState": "AVAILABLE",
        "lifecycleDetails": "External External Database Connector is available",
        "externalDatabaseId": "ExampleDBId",
        "connectionStatus": "AVAILABLE",
        "connectionStatusLastUpdated": "2020-11-13T22:15:59.000Z",
        "timeZone": "US/Pacific"
    }
}
```

Data Catalog

For details about events emitted by Data Catalog, see Data Catalog Events.

Data Safe

For details about events emitted by Data Safe, see Oracle Data Safe Events in Oracle Cloud Infrastructure.
Data Science

Data Science resources that emit events:

- Project Event Types on page 1864
- Notebook Session Event Types on page 1865
- Model Event Types on page 1866

Project Event Types

These are the event types that projects emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Project</td>
<td>com.oraclecloud.datascience.createproject</td>
</tr>
<tr>
<td>Delete Project Begin</td>
<td>com.oraclecloud.datascience.deleteproject.begin</td>
</tr>
<tr>
<td>Delete Project End</td>
<td>com.oraclecloud.datascience.deleteproject.end</td>
</tr>
<tr>
<td>Update Project</td>
<td>com.oraclecloud.datascience.deleteproject.end</td>
</tr>
</tbody>
</table>

Project Example

This is a reference event for projects:

```json
{
  "eventType": "com.oraclecloud.datascience.createproject",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "datascience",
  "eventTime": "2019-11-22T01:43:35.246Z",
  "eventID": "<unique_ID>",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "example_project",
    "resourceId": "ocid1.datascienceproject.oc1.iad.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "extensions": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
  }
}
```
Notebook Session Event Types

These are the event types that notebook sessions emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Notebook Session Begin</td>
<td>com.oraclecloud.datascience.activatenotebooksession.begin</td>
</tr>
<tr>
<td>Activate Notebook Session End</td>
<td>com.oraclecloud.datascience.activatenotebooksession.end</td>
</tr>
<tr>
<td>Create Notebook Session Begin</td>
<td>com.oraclecloud.datascience.createnotebooksession.begin</td>
</tr>
<tr>
<td>Create Notebook Session End</td>
<td>com.oraclecloud.datascience.createnotebooksession.end</td>
</tr>
<tr>
<td>Deactivate Notebook Session Begin</td>
<td>com.oraclecloud.datascience.deactivatenotebooksession.begin</td>
</tr>
<tr>
<td>Deactivate Notebook Session End</td>
<td>com.oraclecloud.datascience.deactivatenotebooksession.end</td>
</tr>
<tr>
<td>Delete Notebook Session Begin</td>
<td>com.oraclecloud.datascience.deletenotebooksession.begin</td>
</tr>
<tr>
<td>Delete Notebook Session End</td>
<td>com.oraclecloud.datascience.deletenotebooksession.end</td>
</tr>
<tr>
<td>Update Notebook Session</td>
<td>com.oraclecloud.datascience.updatenotebooksession</td>
</tr>
</tbody>
</table>

Notebook Session Example

This is a reference event for notebook sessions:

```json
{
    "eventType": "com.oraclecloud.datascience.updatenotebooksession",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "datascience",
    "eventTime": "2019-11-22T01:43:35.246Z",
    "eventID": "<unique_ID>",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "example_notebook_session",
        "resourceId": "ocid1.datasciencenotebooksession.oc1.iad.<unique_ID>",
        "availabilityDomain": "<availability_domain>",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        }
    }
}
```
Events

```
"extensions": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
}
```

Model Event Types

These are the event types that models emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Model</td>
<td>com.oraclecloud.datascience.activatemodel</td>
</tr>
<tr>
<td>Create Model</td>
<td>com.oraclecloud.datascience.createmodel</td>
</tr>
<tr>
<td>Deactivate Model</td>
<td>com.oraclecloud.datascience.deactivatemodel</td>
</tr>
<tr>
<td>Delete Model</td>
<td>com.oraclecloud.datascience.deletemodel</td>
</tr>
<tr>
<td>Update Model</td>
<td>com.oraclecloud.datascience.updatemodel</td>
</tr>
</tbody>
</table>

Model Example

This is a reference event for models:

```
{
  "eventType": "com.oraclecloud.datascience.deletemodel",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "datascience",
  "eventTime": "2019-11-22T01:43:35.246Z",
  "eventID": "<unique_ID>",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "example_model",
    "resourceId": "ocid1.datasciencemodel.oc1.iad.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "extensions": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
  }
}
```
Data Transfer

Data Transfer resources that emit events:

- Jobs Event Types on page 1867
- Appliances Event Types on page 1868
- Packages Event Types on page 1869
- Devices Event Types on page 1870
- Appliance Entitlements Event Types on page 1871
- Appliance Export Jobs Event Types on page 1872

Jobs Event Types

These are the event types that job events emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Transfer Job</td>
<td>com.oraclecloud.datatransferservice.addtransferjob</td>
</tr>
<tr>
<td>Update Transfer Job</td>
<td>com.oraclecloud.datatransferservice.updatetransferjob</td>
</tr>
<tr>
<td>Delete Transfer Job</td>
<td>com.oraclecloud.datatransferservice.deletetransferjob</td>
</tr>
<tr>
<td>Move Transfer Job</td>
<td>com.oraclecloud.datatransferservice.movetransferjob</td>
</tr>
</tbody>
</table>

Jobs Examples

```json
{
  "eventType": "com.oraclecloud.datatransferservice.addtransferjob",
  "source": "datatransferservice",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "transfer_job",
    "resourceId": "ocid1.datatransferjob.oc1.phx.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "deviceType": "APPLIANCE",
      "uploadBucketName": "example_bucket",
      "lifecycleState": "example_state"
    }
  }
}
```
Events

**Appliances Event Types**

These are the event types that appliances emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Transfer Appliance</td>
<td>com.oraclecloud.datatransferservice.addtransferappliance</td>
</tr>
<tr>
<td>Update Transfer Appliance</td>
<td>com.oraclecloud.datatransferservice.updatetransferappliance</td>
</tr>
<tr>
<td>Delete Transfer Appliance</td>
<td>com.oraclecloud.datatransferservice.deletetransferappliance</td>
</tr>
</tbody>
</table>

**Appliances Example**

```json
{
    "eventType": "com.oraclecloud.datatransferservice.addtransferappliance",
    "source": "datatransferservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceId": "ocid1.datatransferjob.oc1.phx.<unique_ID>",
        "availabilityDomain": "<availability_domain>",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "additionalDetails": {
            "applianceLabel": "example_label",
            "lifecycleState": "example_state"
        }
    }
}
```
**Packages Event Types**

These are the event types that packages emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Transfer Package</td>
<td>com.oraclecloud.datatransferservice.addtransferpackage</td>
</tr>
<tr>
<td>Update Transfer Package</td>
<td>com.oraclecloud.datatransferservice.updatetransferpackage</td>
</tr>
<tr>
<td>Delete Transfer Package</td>
<td>com.oraclecloud.datatransferservice.deletetransferpackage</td>
</tr>
<tr>
<td>Attach Devices To Transfer Package</td>
<td>com.oraclecloud.datatransferservice.addtransferpackage</td>
</tr>
<tr>
<td>Detach Devices From Transfer Package</td>
<td>com.oraclecloud.datatransferservice.deletetransferpackage</td>
</tr>
</tbody>
</table>

**Packages Example**

```json
{
    "eventType": "com.oraclecloud.datatransferservice.addtransferpackage",
    "source": "datatransferservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "transfer_job",
        "resourceId": "ocid1.datatransferjob.oc1.phx.<unique_ID>",
        "availabilityDomain": "<availability_domain>",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "additionalDetails": {
            "packageLabel": "example_label",
            "lifecycleState": "example_state"
        }
    }
}
```
Events

**Devices Event Types**

These are the event types that devices emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Transfer Device</td>
<td>com.oraclecloud.datatransferservice.addtransferdevice</td>
</tr>
<tr>
<td>Update Transfer Device</td>
<td>com.oraclecloud.datatransferservice.updatetransferdevice</td>
</tr>
<tr>
<td>Delete Transfer Device</td>
<td>com.oraclecloud.datatransferservice.deletetransferdevice</td>
</tr>
</tbody>
</table>

**Devices Example**

```json
{
    "eventType": "com.oraclecloud.datatransferservice.addtransferdevice",
    "source": "datatransferservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
        "compartmentName": "example_compartment",
        "resourceName": "transfer_job",
        "resourceId": "ocid1.datatransferjob.oc1.phx.<unique_ID>"
        "availabilityDomain": "<availability_domain>"
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "additionalDetails": {
            "deviceLabel": "example_label",
            "lifecycleState": "example_state"
        }
    }
}
```
## Appliance Entitlements Event Types

These are the event types that appliance entitlements emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Transfer Appliance Entitlement</td>
<td>com.oraclecloud.datatransferservice.createtransferapplianceentitlement</td>
</tr>
<tr>
<td>Update Transfer Appliance Entitlement</td>
<td>com.oraclecloud.datatransferservice.updateapplianceentitlement</td>
</tr>
<tr>
<td>Delete Transfer Appliance Entitlement</td>
<td>com.oraclecloud.datatransferservice.updateapplianceentitlement</td>
</tr>
</tbody>
</table>

## Appliance Entitlements Example

```json
{
  "eventType": "com.oraclecloud.datatransferservice.createtransferapplianceentitlement",
  "source": "datatransferservice",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_compartment",
    "resourceName": "transfer_appliance_entitlement",
    "resourceId": "ocid1.datatransferapplianceentitlement.oc1.phx.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "requestorName": "Sample User",
      "requestorEmail": "sample.user@oracle.com",
      "lifecycleState": "example_state",
      "lifecycleStateDetails": "example_details"
    }
  }
}
```
**Appliance Export Jobs Event Types**

These are the event types that appliance export jobs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Appliance Export Job</td>
<td>com.oraclecloud.datatransferservice.addapplianceexportjob</td>
</tr>
<tr>
<td>Update Appliance Export Job</td>
<td>com.oraclecloud.datatransferservice.updateapplianceexportjob</td>
</tr>
<tr>
<td>Delete Appliance Export Job</td>
<td>com.oraclecloud.datatransferservice.deleteapplianceexportjob</td>
</tr>
<tr>
<td>Move Appliance Export Job</td>
<td>com.oraclecloud.datatransferservice.moveapplianceexportjob</td>
</tr>
</tbody>
</table>

**Appliance Export Jobs Example**

```json
{
    "eventType": "com.oraclecloud.datatransferservice.addapplianceexportjob",
    "source": "datatransferservice",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "export_job",
        "resourceId": "ocid1.datatransferapplianceexportjob.oc1.phx.<unique_ID>",
        "availabilityDomain": "<availability_domain>",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "additionalDetails": {
            "bucketName": "example_bucket",
            "lifecycleState": "example_state",
            "lifecycleStateDetails": "example_details"
        }
    }
}
```

**Digital Assistant**

For details about events emitted by Digital Assistant, see [Events for Digital Assistant Instances](#).

**File Storage**

File Storage resources that emit events:

- File System Event Types on page 1873 and Snapshot Event Types on page 1874
Events

- **Mount Target Event Types** on page 1875
- **Export Event Types** on page 1876 and **Export Set Event Types** on page 1876

**File System Event Types**

These are the event types that file systems emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change File System Compartment</td>
<td>com.oraclecloud.filestorage.changefilesystemcompartment</td>
</tr>
<tr>
<td>Create File System</td>
<td>com.oraclecloud.filestorage.createfilesystem</td>
</tr>
<tr>
<td>Delete File System</td>
<td>com.oraclecloud.filestorage.deletefilesystem</td>
</tr>
<tr>
<td>Update File System</td>
<td>com.oraclecloud.filestorage.updatefilesystem</td>
</tr>
</tbody>
</table>

**File System Example**

This is a reference event for file systems:

```json
{
    "eventType": "com.oraclecloud.filestorage.createfilesystem",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "filestorage",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>",
        "compartmentName": "example_name",
        "resourceName": "my_filesystem",
        "resourceId": "ocid1.filesystem.oc1..<unique_id>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "unique_ID",
        "extensions": {
            "compartmentId": "ocid1.compartment.oc1..<unique_id>"
        }
    }
}
```
Snapshot Event Types

These are the event types that snapshots emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Snapshot</td>
<td>com.oraclecloud.filestorage.createsnapshot</td>
</tr>
<tr>
<td>Delete Snapshot</td>
<td>com.oraclecloud.filestorage.deletesnapshot</td>
</tr>
</tbody>
</table>

Snapshot Example

This is a reference event for snapshots:

```json
{
    "eventType": "com.oraclecloud.filestorage.createsnapshot",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "filestorage",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>",
        "compartmentName": "example_name",
        "resourceName": "my_snapshot",
        "resourceId": "ocid1.snapshot.oc1..<unique_id>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "unique_ID",
        "extensions": {
            "compartmentId": "ocid1.compartment.oc1..<unique_id>"
        }
    }
}
```
Mount Target Event Types

These are the event types that mount targets emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Mount Target Compartment</td>
<td>com.oraclecloud.filestorage.changemounttargetcompartment</td>
</tr>
<tr>
<td>Create Mount Target</td>
<td>com.oraclecloud.filestorage.createmounttarget</td>
</tr>
<tr>
<td>Delete Mount Target</td>
<td>com.oraclecloud.filestorage.deletemounttarget</td>
</tr>
<tr>
<td>Update Mount Target</td>
<td>com.oraclecloud.filestorage.updatemounttarget</td>
</tr>
</tbody>
</table>

Mount Target Example

This is a reference event for mount targets:

```json
{
    "eventType": "com.oraclecloud.filestorage.createmounttarget",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "filestorage",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>",
        "compartmentName": "example_name",
        "resourceName": "my_mounttarget",
        "resourceId": "ocid1.mounttarget.oc1..<unique_id>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "unique_ID",
        "extensions": {
            "compartmentId": "ocid1.compartment.oc1..<unique_id>"
        }
    }
}
```
### Export Event Types

These are the event types that exports emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Export</td>
<td>com.oraclecloud.filestorage.createexport</td>
</tr>
<tr>
<td>Delete Export</td>
<td>com.oraclecloud.filestorage.deleteexport</td>
</tr>
<tr>
<td>Update Export</td>
<td>com.oraclecloud.filestorage.updateexport</td>
</tr>
</tbody>
</table>

#### Export Example

This is a reference event for exports:

```json
{
    "eventType": "com.oraclecloud.filestorage.createexport",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "filestorage",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>",
        "compartmentName": "example_name",
        "resourceName": "my_export",
        "resourceId": "ocid1.export.oc1..<unique_id>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        }
    },
    "eventID": "unique_ID",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>"
    }
}
```

### Export Set Event Types

These are the event types that export sets emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Export Set</td>
<td>com.oraclecloud.filestorage.deleteexportset</td>
</tr>
<tr>
<td>Update Export Set</td>
<td>com.oraclecloud.filestorage.updateexportset</td>
</tr>
</tbody>
</table>

#### Export Set Example

---

---
This is a reference event for export sets:

```
{
    "eventType": "com.oraclecloud.filestorage.updateexportset",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "filestorage",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>",
        "compartmentName": "example_name",
        "resourceName": "my_exportset",
        "resourceId": "ocid1.exportset.oc1..<unique_id>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        }
    },
    "eventID": "unique_ID",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_id>"
    }
}
```

### Functions

Functions resources that emit events:

- Application Event Types on page 1877
- Function Event Types on page 1878

#### Application Event Types

These are the event types that applications emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Application Compartment</td>
<td>com.oraclecloud.functions.changeapplicationcompartment</td>
</tr>
<tr>
<td>Create Application</td>
<td>com.oraclecloud.functions.createapplication</td>
</tr>
<tr>
<td>Delete Application</td>
<td>com.oraclecloud.functions.deleteapplication</td>
</tr>
<tr>
<td>Update Application</td>
<td>com.oraclecloud.functions.updateapplication</td>
</tr>
</tbody>
</table>

#### Application Example

This is an example event for applications:

```
{
    "eventType": "com.oraclecloud.functions.createapplication",
}
Events

```
"cloudEventsVersion": "0.1",
"eventTypeVersion": "2.0",
"source": "functions",
"eventTime": "2019-07-22T09:33:44.754Z",
"contentType": "application/json",
"data":{
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "my_compartment",
    "resourceName": "my-application",
    "resourceId": "ocid1.fnapp.oc1.phx.<unique_ID>",
    "availabilityDomain": "AD3"
},
"eventID": "<unique_ID>",
"extensions":{
    "compartmentId":"ocid1.compartment.oc1..<unique_ID>"
}
}
```

**Function Event Types**

These are the event types that functions emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Function</td>
<td><code>com.oraclecloud.functions.createfunction</code></td>
</tr>
<tr>
<td>Delete Function</td>
<td><code>com.oraclecloud.functions.deletefunction</code></td>
</tr>
<tr>
<td>Update Function</td>
<td><code>com.oraclecloud.functions.updatefunction</code></td>
</tr>
</tbody>
</table>

**Function Example**

This is an example event for functions:

```
{
    "eventType": "com.oraclecloud.functions.createfunction",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "functions",
    "eventTime": "2019-07-22T09:33:44.754Z",
    "contentType": "application/json",
    "data":{
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "my_compartment",
    "resourceName": "my-function",
    "resourceId": "ocid1.fnfunc.oc1.phx.<unique_ID>",
    "availabilityDomain": "AD3"
    },
    "eventID": "<unique_ID>",
    "extensions":{
    "compartmentId":"ocid1.compartment.oc1..<unique_ID>"
}
}
```

**Health Checks**

Health Checks resources that emit events:
HTTP Monitors Event Types

These are the event types that HTTP monitors emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create HTTP Monitor</td>
<td>com.oraclecloud.healthchecks.createhttpmonitor</td>
</tr>
<tr>
<td>Delete HTTP Monitor</td>
<td>com.oraclecloud.healthchecks.deletehttpmonitor</td>
</tr>
<tr>
<td>Update HTTP Monitor</td>
<td>com.oraclecloud.healthchecks.updatehttpmonitor</td>
</tr>
</tbody>
</table>

HTTP Monitor Example

This is an example event for HTTP monitors:

```
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.healthchecks.createhttpmonitor",
  "source": "healthchecks",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-10-30T12:06:29.451Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_monitor",
    "resourceId": "ocid1.httpmonitor.oc1..<unique_ID>",
    "availabilityDomain": "AD1",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    }
  }
}
```
### Ping Monitor Event Types

These are the event types that ping monitors emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Ping Monitor</td>
<td>com.oraclecloud.healthchecks.createpingmonitor</td>
</tr>
<tr>
<td>Delete Ping Monitor</td>
<td>com.oraclecloud.healthchecks.deletepingmonitor</td>
</tr>
<tr>
<td>Update Ping Monitor</td>
<td>com.oraclecloud.healthchecks.updatepingmonitor</td>
</tr>
</tbody>
</table>

### Ping Monitor Example

This is an example event for ping monitors:

```json
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.healthchecks.createpingmonitor",
  "source": "healthchecks",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-10-30T12:08:11.242Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_monitor",
    "resourceId": "ocid1.pingmonitor.oc1..<unique_ID>",
    "availabilityDomain": "AD1",
    "freeFormTags": { 
      "Department": "Finance"
    },
    "definedTags": { 
      "Operations": { 
        "CostCenter": "42"
      }
    }
  }
}
```

### IAM

IAM resources that emit events:

- [Authentication Policy Event Types](#) on page 1881
- [Credentials Event Types](#) on page 1882
- [Dynamic Group Event Types](#) on page 1883
- [Group Event Types](#) on page 1884
- [Identity Provider Event Types](#) on page 1886
- [Multi-Factor Authentication TOTP Device Event Types](#) on page 1888
- [Policy Event Types](#) on page 1889
- [User Event Types](#) on page 1890
**Authentication Policy Event Types**

This is the event type that authentication policies emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Authentication Policy</td>
<td><code>com.oraclecloud.identityControlPlane.UpdateAuthenticationPolicy</code></td>
</tr>
</tbody>
</table>

**Authentication Policy Example**

This is a reference event for authentication policy events:

```json
{
    "eventType": "com.oraclecloud.identityControlPlane.UpdateAuthenticationPolicy",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "identityControlPlane",
    "eventID": "<unique_ID>",
    "eventTime": "2019-10-21T17:23:54.095Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_compartment",
        "resourceId": "ocid1.compartment.oc1..<unique_ID>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "extensions": {
            "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
        }
    }
}
```
## Credentials Event Types

These are the event types that credentials emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Auth Token</td>
<td>com.oraclecloud.identityControlPlane.CreateAuthToken</td>
</tr>
<tr>
<td>Create Customer Secret Key</td>
<td>com.oraclecloud.identityControlPlane.CreateCustomerSecretKey</td>
</tr>
<tr>
<td>Create or Reset Password</td>
<td>com.oraclecloud.identityControlPlane.CreateOrResetPassword</td>
</tr>
<tr>
<td>Create SMTP Credential</td>
<td>com.oraclecloud.identityControlPlane.CreateSmtpCredential</td>
</tr>
<tr>
<td>Create Swift Password</td>
<td>com.oraclecloud.identityControlPlane.CreateSwiftPassword</td>
</tr>
<tr>
<td>Delete API Key</td>
<td>com.oraclecloud.identityControlPlane.DeleteApiKey</td>
</tr>
<tr>
<td>Delete Auth Token</td>
<td>com.oraclecloud.identityControlPlane.DeleteAuthToken</td>
</tr>
<tr>
<td>Delete Customer Secret Key</td>
<td>com.oraclecloud.identityControlPlane.DeleteCustomerSecretKey</td>
</tr>
<tr>
<td>Delete SMTP Credential</td>
<td>com.oraclecloud.identityControlPlane.DeleteSmtpCredential</td>
</tr>
<tr>
<td>Delete Swift Password</td>
<td>com.oraclecloud.identityControlPlane.DeleteSwiftPassword</td>
</tr>
<tr>
<td>Update Auth Token</td>
<td>com.oraclecloud.identityControlPlane.UpdateAuthToken</td>
</tr>
<tr>
<td>Update Authentication Policy</td>
<td>com.oraclecloud.identityControlPlane.UpdateAuthenticationPolicy</td>
</tr>
<tr>
<td>Update SMTP Credential</td>
<td>com.oraclecloud.identityControlPlane.UpdateSmtpCredential</td>
</tr>
<tr>
<td>UpdateSwift Password</td>
<td>com.oraclecloud.identityControlPlane.UpdateSwiftPassword</td>
</tr>
<tr>
<td>Upload API KEY</td>
<td>com.oraclecloud.identityControlPlane.UploadApiKey</td>
</tr>
</tbody>
</table>

### Credentials Example
Events

This is a reference event for most credential events (create or reset password don't include additional details):

```json
{
  "eventType": "com.oraclecloud.identityControlPlane.DeleteApiKey",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "identityControlPlane",
  "eventID": "<unique_ID>",
  "eventTime": "2019-10-21T17:23:54.095Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_user",
    "resourceId": "<unique_ID>",
    "availabilityDomain": "availability_domain",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "userId": "ocid1.user.oc1..<unique_ID>"
    },
    "extensions": {
      "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
  }
}
```

Dynamic Group Event Types

These are the event types that dynamic groups emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Dynamic Group</td>
<td>com.oraclecloud.identityControlPlane.CreateDynamicGroup</td>
</tr>
<tr>
<td>Delete Dynamic Group</td>
<td>com.oraclecloud.identityControlPlane.DeleteDynamicGroup</td>
</tr>
<tr>
<td>Update Dynamic Group</td>
<td>com.oraclecloud.identityControlPlane.UpdateDynamicGroup</td>
</tr>
</tbody>
</table>

Dynamic Group Example

This is a reference event for dynamic groups:

```json
{
  "eventType": "com.oraclecloud.identityControlPlane.CreateDynamicGroup",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "identityControlPlane",
  "eventID": "<unique_ID>",
  "eventTime": "2019-10-21T17:23:54.095Z",
  "contentType": "application/json",
  "data": {
```
### Group Event Types

These are the event types that groups emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add User to Group</td>
<td><code>com.oraclecloud.identityControlPlane.AddUserToGroup</code></td>
</tr>
<tr>
<td>Create Group</td>
<td><code>com.oraclecloud.identityControlPlane.CreateGroup</code></td>
</tr>
<tr>
<td>Delete Group</td>
<td><code>com.oraclecloud.identityControlPlane.DeleteGroup</code></td>
</tr>
<tr>
<td>Remove User From Group</td>
<td><code>com.oraclecloud.identityControlPlane.RemoveUserFromGroup</code></td>
</tr>
<tr>
<td>Update Group</td>
<td><code>com.oraclecloud.identityControlPlane.UpdateGroup</code></td>
</tr>
</tbody>
</table>

### Group Example

This is a reference event for some groups (create, delete, and update events don't include additional details):

```json
{
    "eventType": "com.oraclecloud.identityControlPlane.AddUserToGroup",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "identityControlPlane",
    "eventID": "<unique_ID>",
    "eventTime": "2019-10-21T17:23:54.095Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_group",
        "resourceId": "ocid1.groupmembership.oc1..<unique_ID>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        }
    }
}
```
"definedTags": {
  "Operations": {
    "CostCenter": "42"
  }
},
"additionalDetails": {
  "userId": "ocid1.user.oc1..<unique_ID>",
  "groupId": "ocid1.group.oc1..<unique_ID>"
},
"extensions": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
}
### Identity Provider Event Types

These are the event types that identity providers emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add User to IdP Group</td>
<td>com.oraclecloud.identityControlPlane.AddUserToIdpGroup</td>
</tr>
<tr>
<td>Create Identity Provider</td>
<td>com.oraclecloud.identityControlPlane.CreateIdentityProvider</td>
</tr>
<tr>
<td>Create Identity Provider Group</td>
<td>com.oraclecloud.identityControlPlane.CreateIdentityProviderGroup</td>
</tr>
<tr>
<td>Create IdP Group Mapping</td>
<td>com.oraclecloud.identityControlPlane.CreateIdpGroupMapping</td>
</tr>
<tr>
<td>Create IdP User</td>
<td>com.oraclecloud.identityControlPlane.CreateIdpUser</td>
</tr>
<tr>
<td>Delete Identity Provider</td>
<td>com.oraclecloud.identityControlPlane.DeleteIdentityProvider</td>
</tr>
<tr>
<td>Delete Identity Provider Group</td>
<td>com.oraclecloud.identityControlPlane.DeleteIdentityProviderGroup</td>
</tr>
<tr>
<td>Delete IdP Group Mapping</td>
<td>com.oraclecloud.identityControlPlane.DeleteIdpGroupMapping</td>
</tr>
<tr>
<td>Delete IdP User</td>
<td>com.oraclecloud.identityControlPlane.DeleteIdpUser</td>
</tr>
<tr>
<td>Remove User From IdP Group</td>
<td>com.oraclecloud.identityControlPlane.RemoveUserFromIdpGroup</td>
</tr>
<tr>
<td>Reset IdP SCIM Client</td>
<td>com.oraclecloud.identityControlPlane.ResetIdpScim</td>
</tr>
<tr>
<td>Update Identity Provider</td>
<td>com.oraclecloud.identityControlPlane.UpdateIdentityProvider</td>
</tr>
<tr>
<td>Update IdP Group Mapping</td>
<td>com.oraclecloud.identityControlPlane.UpdateIdpGroupMapping</td>
</tr>
</tbody>
</table>

### Identity Provider Example

The following reference events are for identity provider events that include additional details. Some identity providers events do not include additional details. These events are create, delete, and update identity providers, as well as delete identity provider group, delete IdP user, and reset IdP SCIM.

This is a reference event for adding and removing users from IdP groups:

```json
{
  "eventType": "com.oraclecloud.identityControlPlane.AddUserToIdpGroup",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "identityControlPlane",
  "eventID": "<unique_ID>",
  "entity": {
    "type": "USER",
    "id": "<unique_ID>",
    "name": "<unique_name>",
    "email": "<unique_email>",
    "firstName": "<unique_firstName>",
    "lastName": "<unique_lastName>",
    "organization": "<unique_organization>",
    "profile": {
      "attributes": {
        "preferred_language": "en",
        "locale": "en",
        "timezone": "America/Los_Angeles"
      }
    }
  }
}
```
This is a reference event for create, update, and delete IdP group mapping:

```
{
"eventType": "com.oraclecloud.identityControlPlane.CreateIdpGroupMapping",
"cloudEventsVersion": "0.1",
"eventTypeVersion": "2.0",
"source": "identityControlPlane",
"eventID": "<unique_ID>",
"eventTime": "2019-10-21T17:23:54.095Z",
"contentType": "application/json",
"data": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  "compartmentName": "example_name",
  "resourceName": "my_group",
  "resourceId": "ocid1.idpgroup.oc1..<unique_ID>",
  "availabilityDomain": "availability_domain",
  "freeFormTags": {
    "Department": "Finance"
  },
  "definedTags": {
    "Operations": {
      "CostCenter": "42"
    }
  },
  "additionalDetails": {
    "userId": "ocid1.user.oc1..<unique_ID>
  }
},
"extensions": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
}
}
```

This is a reference event for create IdP user and create IdP group:

```
{
"eventType": "com.oraclecloud.identityControlPlane.CreateIdpGroupMapping",
"cloudEventsVersion": "0.1",
"eventTypeVersion": "2.0",
"source": "identityControlPlane",
"eventID": "<unique_ID>",
"eventTime": "2019-10-21T17:23:54.095Z",
"contentType": "application/json",
"data": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  "compartmentName": "example_name",
  "resourceName": "my_identityprovider",
  "resourceId": "ocid1.idpmapping.oc1..<unique_ID>",
  "availabilityDomain": "availability_domain",
  "freeFormTags": {
    "Department": "Finance"
  },
  "definedTags": {
    "Operations": {
      "CostCenter": "42"
    }
  },
  "additionalDetails": {
    "idpGroupName": "my_group",
    "groupId": "ocid1.group.oc1..<unique_ID>
  }
},
"extensions": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
}
}
```

This is a reference event for create, update, and delete IdP group mapping:
Multi-Factor Authentication TOTP Device Event Types

These are the event types that MFA TOTP devices emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate MFA TOTP Device</td>
<td>com.oraclecloud.identityControlPlane.ActivateMfaTotpDevice</td>
</tr>
<tr>
<td>Create MFA TOTP Device</td>
<td>com.oraclecloud.identityControlPlane.CreateMfaTotpDevice</td>
</tr>
<tr>
<td>Delete MFA TOTP Device</td>
<td>com.oraclecloud.identityControlPlane.DeleteMfaTotpDevice</td>
</tr>
<tr>
<td>Generate MFA TOTP Device Seed</td>
<td>com.oraclecloud.identityControlPlane.GenerateTotpSeed</td>
</tr>
</tbody>
</table>

Multi-Factor Authentication TOTP Devices Example

This is a reference event for MFA TOTP Devices:

```json
{
    "eventType": "com.oraclecloud.identityControlPlane.CreateMfaTotpDevice",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "identityControlPlane",
    "eventID": "<unique_ID>",
    "eventTime": "2019-10-21T17:23:54.095Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_idpgroup",
        "resourceId": "ocid1.idpgroup.oc1..<unique_ID>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "additionalDetails": {
            "externalIdentifier": "my_externalidentifier"
        },
        "extensions": {
            "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
        }
    }
}
```
Events

```
"data": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  "compartmentName": "example_name",
  "resourceName": "my_user",
  "resourceId": "ocid1.credential.oc1..<unique_ID>",
  "availabilityDomain": "availability_domain",
  "freeFormTags": {
    "Department": "Finance"
  },
  "definedTags": {
    "Operations": {
      "CostCenter": "42"
    }
  },
  "additionalDetails": {
    "userId": "ocid1.user.oc1..<unique_ID>
  }
},
"extensions": {
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>
}
```

Policy Event Types

These are the event types that policies emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Policy</td>
<td>com.oraclecloud.identityControlPlane.CreatePolicy</td>
</tr>
<tr>
<td>Delete Policy</td>
<td>com.oraclecloud.identityControlPlane.DeletePolicy</td>
</tr>
<tr>
<td>Update Policy</td>
<td>com.oraclecloud.identityControlPlane.UpdatePolicy</td>
</tr>
</tbody>
</table>

Policy Example

This is a reference event for policies:

```
{
  "eventType": "com.oraclecloud.identityControlPlane.CreatePolicy",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "identityControlPlane",
  "eventID": "<unique_ID>",
  "eventTime": "2019-10-21T17:23:54.095Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_policy",
    "resourceId": "ocid1.policy.oc1..<unique_ID>",
    "availabilityDomain": "availability_domain",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
```
User Event Types

These are the event types that users emit.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create User</td>
<td>com.oraclecloud.identityControlPlane.CreateUser</td>
</tr>
<tr>
<td>Delete User</td>
<td>com.oraclecloud.identityControlPlane.DeleteUser</td>
</tr>
<tr>
<td>Update User</td>
<td>com.oraclecloud.identityControlPlane.UpdateUser</td>
</tr>
<tr>
<td>Update User Capabilities</td>
<td>com.oraclecloud.identityControlPlane.UpdateUserCapabilities</td>
</tr>
<tr>
<td>Update User State</td>
<td>com.oraclecloud.identityControlPlane.UpdateUserState</td>
</tr>
</tbody>
</table>

User Example

This is a reference event for users:

```json
{
    "eventType": "com.oraclecloud.identityControlPlane.CreateUser",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "identityControlPlane",
    "eventID": "<unique_ID>",
    "eventTime": "2019-10-21T17:23:54.095Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_user",
        "resourceId": "ocid1.user.oc1..<unique_ID>",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "extensions": {
            "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
        }
    }
}
```
Integration

For details about events emitted by Oracle Integration, see Automating with Events.

Networking

Networking resources that emit events:

- DHCP Options Event Types on page 1891
- Dynamic Routing Gateway (DRG) Event Types on page 1892
- DRG Attachment Event Types on page 1893
- Internet Gateway Event Types on page 1894
- Local Peering Gateway (LPG) Event Types on page 1895
- NAT Gateway Event Types on page 1896
- Network Security Group (NSG) Event Types on page 1897
- Private IP Event Types on page 1898
- Public IP Event Types on page 1899
- Route Table Event Types on page 1900
- Security List Event Types on page 1901
- Service Gateway Event Types on page 1902
- Subnet Event Types on page 1903
- VCN Event Types on page 1904
- Virtual Network Interface Card (VNIC) Event Types on page 1904
- VLAN Event Types on page 1905

DHCP Options Event Types

These are the event types that sets of DHCP options emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change DHCP Options Compartment</td>
<td>com.oraclecloud.virtualnetwork.changedhcpoptions</td>
</tr>
<tr>
<td>Create DHCP Options</td>
<td>com.oraclecloud.virtualnetwork.createdhcpoptions</td>
</tr>
<tr>
<td>Delete DHCP Options</td>
<td>com.oraclecloud.virtualnetwork.deletedhcpoptions</td>
</tr>
<tr>
<td>Update DHCP Options</td>
<td>com.oraclecloud.virtualnetwork.updatedhcpoptions</td>
</tr>
</tbody>
</table>

DHCP Options Example

This is a reference event for a set of DHCP options:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createdhcpoptions",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {  
```
Dynamic Routing Gateway (DRG) Event Types

These are the event types that DRGs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create DRG</td>
<td>com.oraclecloud.virtualnetwork.createdrg</td>
</tr>
<tr>
<td>Delete DRG</td>
<td>com.oraclecloud.virtualnetwork.deletedrg</td>
</tr>
<tr>
<td>Update DRG</td>
<td>com.oraclecloud.virtualnetwork.updatedrg</td>
</tr>
</tbody>
</table>

DRG Example

This is a reference event for a DRG:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createdrg",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>"
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.drg.oci.phx.<unique_ID>"
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": { "Department": "Finance"
        },
        "definedTags": { "Operations": { "CostCenter": "42"
        } },
        "eventID": "<unique_ID>",
        "extensions": { "compartmentId": "ocid1.compartment.oci..<unique_ID>" }
    }
}
```
DRG Attachment Event Types

These are the event types that DRG attachments emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create DRG Attachment</td>
<td>com.oraclecloud.virtualnetwork.createdrgattachment</td>
</tr>
<tr>
<td>Delete DRG Attachment</td>
<td>com.oraclecloud.virtualnetwork.deletedrgattachment</td>
</tr>
<tr>
<td>Update DRG Attachment</td>
<td>com.oraclecloud.virtualnetwork.updatedrgattachment</td>
</tr>
</tbody>
</table>

DRG Attachment Example

This is a reference event for a DRG attachment:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createdrgattachment",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>"",
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.drgattachment.oci.phx.<unique_ID>"",
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        }
    }
}
```
Internet Gateway Event Types

These are the event types that internet gateways emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Internet Gateway Compartment</td>
<td>com.oraclecloud.virtualnetwork.changeinternetgateway</td>
</tr>
<tr>
<td>Create Internet Gateway</td>
<td>com.oraclecloud.virtualnetwork.createinternetgateway</td>
</tr>
<tr>
<td>Delete Internet Gateway</td>
<td>com.oraclecloud.virtualnetwork.deleteinternetgateway</td>
</tr>
<tr>
<td>Update Internet Gateway</td>
<td>com.oraclecloud.virtualnetwork.updateinternetgateway</td>
</tr>
</tbody>
</table>

Internet Gateway Example

This is a reference event for an internet gateway:

```json
{
   "eventType": "com.oraclecloud.virtualnetwork.createinternetgateway",
   "cloudEventsVersion": "0.1",
   "eventTypeVersion": "2.0",
   "source": "virtualNetwork",
   "eventTime": "2019-08-12T17:51:42.789Z",
   "contentType": "application/json",
   "data": {
      "compartmentId": "ocid1.compartment.oci..<unique_ID>",
      "compartmentName": "example_name",
      "resourceName": "example_name",
      "resourceId": "ocid1.internetgateway.oci.phx.<unique_ID>",
      "availabilityDomain": "XXIT:PHX-AD-1",
      "freeFormTags": {
         "Department": "Finance"
      },
      "definedTags": {
         "Operations": {
            "CostCenter": "42"
         }
      },
      "eventID": "<unique_ID>",
      "extensions": {
         "compartmentId": "ocid1.compartment.oci..<unique_ID>"
      }
   }
}
```
### Local Peering Gateway (LPG) Event Types

These are the event types that LPGs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Local Peering Gateway Compartment</td>
<td>com.oraclecloud.virtualnetwork.changelocalpeeringgateway_compartment</td>
</tr>
<tr>
<td>Create Local Peering Gateway</td>
<td>com.oraclecloud.virtualnetwork.createlocalpeeringgateway</td>
</tr>
<tr>
<td>Delete Local Peering Gateway</td>
<td>com.oraclecloud.virtualnetwork.deletelocalpeeringgateway</td>
</tr>
<tr>
<td>Update Local Peering Gateway</td>
<td>com.oraclecloud.virtualnetwork.updatelocalpeeringgateway</td>
</tr>
</tbody>
</table>

### LPG Example

This is a reference event for an LPG:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createlocalpeeringgateway",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.localpeeringgateway.oci.phx..<unique_ID>",
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "<unique_ID>",
        "extensions": {
            "compartmentId": "ocid1.compartment.oci..<unique_ID>"
        }
    }
}
```
NAT Gateway Event Types

These are the event types that NAT gateways emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change NAT Gateway Compartment</td>
<td>com.oraclecloud.natgateway.changenatgatewaycompartment</td>
</tr>
<tr>
<td>Create NAT Gateway</td>
<td>com.oraclecloud.natgateway.createnatgateway</td>
</tr>
<tr>
<td>Delete NAT Gateway</td>
<td>com.oraclecloud.natgateway.deletenatgateway</td>
</tr>
<tr>
<td>Update NAT Gateway</td>
<td>com.oraclecloud.natgateway.updatenatgateway</td>
</tr>
</tbody>
</table>

NAT Gateway Example

This is a reference event for NAT gateways:

```json
{
   "eventType": "com.oraclecloud.natgateway.createnatgateway",
   "cloudEventsVersion": "0.1",
   "eventTypeVersion": "2.0",
   "source": "natgateway",
   "eventTime": "2019-08-12T17:51:42.789Z",
   "contentType": "application/json",
   "data": {
      "compartmentId": "ocid1.compartment.oci.<unique_ID>",
      "compartmentName": "example_name",
      "resourceName": "example_name",
      "resourceId": "ocid1.natgateway.oci.phx.<unique_ID>",
      "availabilityDomain": "XXIT:PHX-AD-1",
      "freeFormTags": {
         "Department": "Finance"
      },
      "definedTags": {
         "Operations": {
            "CostCenter": "42"
         }
      }
   },
   "eventID": "<unique_ID>",
   "extensions": {
      "compartmentId": "ocid1.compartment.oci.<unique_ID>"
   }
}
```
### Network Security Group (NSG) Event Types

These are the event types that NSGs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Network Security Group Compartment</td>
<td>com.oraclecloud.virtualnetwork.changenetworksecuritygrouppanagement</td>
</tr>
<tr>
<td>Create Network Security Group</td>
<td>com.oraclecloud.virtualnetwork.createnetworksecuritygroup</td>
</tr>
<tr>
<td>Delete Network Security Group</td>
<td>com.oraclecloud.virtualnetwork.deletenetworksecuritygroup</td>
</tr>
<tr>
<td>Update Network Security Group</td>
<td>com.oraclecloud.virtualnetwork.updatenetworksecuritygroup</td>
</tr>
</tbody>
</table>

### NSG Example

This is a reference event for an NSG:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createnetworksecuritygroup",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.networksecuritygroup.oci.phx.<unique_ID>",
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "<unique_ID>",
        "extensions": {
            "compartmentId": "ocid1.compartment.oci..<unique_ID>"
        }
    }
}
```
Private IP Event Types

These are the event types that private IPs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Private IP</td>
<td>com.oraclecloud.virtualnetwork.createprivateip</td>
</tr>
<tr>
<td>Delete Private IP</td>
<td>com.oraclecloud.virtualnetwork.deleteprivateip</td>
</tr>
<tr>
<td>Update Private IP</td>
<td>com.oraclecloud.virtualnetwork.updateprivateip</td>
</tr>
</tbody>
</table>

Private IP Example

This is a reference event for a private IP:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createprivateip",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
      "compartmentId": "oci1.compartment.oci..<unique_ID>",
      "compartmentName": "example_name",
      "resourceName": "example_name",
      "resourceId": "oci1.privateip.oci.phx.<unique_ID>",
      "availabilityDomain": "XXIT:PHX-AD-1",
      "freeFormTags": {
        "Department": "Finance"
      },
      "definedTags": {
        "Operations": {
          "CostCenter": "42"
        }
      }
    },
    "eventID": "<unique_ID>",
    "extensions": {
      "compartmentId": "oci1.compartment.oci..<unique_ID>"
    }
}
```
Public IP Event Types

These are the event types that public IPs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Public IP Compartment</td>
<td>com.oraclecloud.virtualnetwork.changepublicipcompartment</td>
</tr>
<tr>
<td>Create Public IP</td>
<td>com.oraclecloud.virtualnetwork.createpublicip</td>
</tr>
<tr>
<td>Delete Public IP</td>
<td>com.oraclecloud.virtualnetwork.deletepublicip</td>
</tr>
<tr>
<td>Update Public IP</td>
<td>com.oraclecloud.virtualnetwork.updatepublicip</td>
</tr>
</tbody>
</table>

Public IP Example

This is a reference event for a public IP:

```json
{
  "eventType": "com.oraclecloud.virtualnetwork.createpublicip",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "virtualNetwork",
  "eventTime": "2019-08-12T17:51:42.789Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oci..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "example_name",
    "resourceId": "ocid1.publicip.oci.phx.<unique_ID>",
    "availabilityDomain": "XXIT:PHX-AD-1",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "eventID": "<unique_ID>",
    "extensions": {
      "compartmentId": "ocid1.compartment.oci..<unique_ID>"
    }
  }
}
```
**Route Table Event Types**

These are the event types that route tables emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Route Table Compartment</td>
<td>com.oraclecloud.virtualnetwork.changeroutetable</td>
</tr>
<tr>
<td>Create Route Table</td>
<td>com.oraclecloud.virtualnetwork.createroutetable</td>
</tr>
<tr>
<td>Delete Route Table</td>
<td>com.oraclecloud.virtualnetwork.deleteroutetable</td>
</tr>
<tr>
<td>Update Route Table</td>
<td>com.oraclecloud.virtualnetwork.updateroutetable</td>
</tr>
</tbody>
</table>

**Route Table Example**

This is a reference event for route tables:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createroutetable",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.routetable.oci.phx.<unique_ID>",
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "<unique_ID>",
        "extensions": {
            "compartmentId": "ocid1.compartment.oci..<unique_ID>"
        }
    }
}
```
Security List Event Types

These are the event types that security lists emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Security List Compartment</td>
<td><code>com.oraclecloud.virtualnetwork.changesecuritylist</code></td>
</tr>
<tr>
<td>Create Security List</td>
<td><code>com.oraclecloud.virtualnetwork.createsecuritylist</code></td>
</tr>
<tr>
<td>Delete Security List</td>
<td><code>com.oraclecloud.virtualnetwork.deletesecuritylist</code></td>
</tr>
<tr>
<td>Update Security List</td>
<td><code>com.oraclecloud.virtualnetwork.updatesecuritylist</code></td>
</tr>
</tbody>
</table>

Security List Example

This is a reference event for security lists:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createsecuritylist",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci.<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.securitylist.oci.phx.<unique_ID>",
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        },
        "eventID": "<unique_ID>",
        "extensions": {
            "compartmentId": "ocid1.compartment.oci.<unique_ID>"
        }
    }
}
```
Service Gateway Event Types

These are the event types that service gateways emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach Service</td>
<td>com.oraclecloud.servicegateway.attachserviceid</td>
</tr>
<tr>
<td>Change Service Gateway Compartment</td>
<td>com.oraclecloud.servicegateway.changeservicegatewaycompartment</td>
</tr>
<tr>
<td>Create Service Gateway</td>
<td>com.oraclecloud.servicegateway.createservicegateway</td>
</tr>
<tr>
<td>Delete Service Gateway End</td>
<td>com.oraclecloud.servicegateway.deleteservicegateway.end</td>
</tr>
<tr>
<td>Delete Service Gateway Start</td>
<td>com.oraclecloud.servicegateway.deleteservicegateway.begin</td>
</tr>
<tr>
<td>Detach Service</td>
<td>com.oraclecloud.servicegateway.detachserviceid</td>
</tr>
<tr>
<td>Update Service Gateway</td>
<td>com.oraclecloud.servicegateway.updateservicegateway</td>
</tr>
</tbody>
</table>

Service Gateway Example

This is a reference event for service gateways:

```json
{
  "eventType": "com.oraclecloud.servicegateway.createservicegateway",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "servicegateway",
  "eventTime": "2019-08-12T17:51:42.789Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oci..<unique_ID>>",
    "compartmentName": "example_name",
    "resourceName": "example_name",
    "resourceId": "ocid1.servicegateway.oci.phx.<unique_ID>>",
    "availabilityDomain": "XXIT:PHX-AD-1",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    }
  },
  "eventId": "<unique_ID>>",
  "extensions": {
    "compartmentId": "ocid1.compartment.oci..<unique_ID>>"
  }
}
```
Subnet Event Types

These are the event types that subnets emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Subnet</td>
<td>com.oraclecloud.virtualnetwork.createsubnet</td>
</tr>
<tr>
<td>Delete Subnet</td>
<td>com.oraclecloud.virtualnetwork.deletesubnet</td>
</tr>
<tr>
<td>Update Subnet</td>
<td>com.oraclecloud.virtualnetwork.updatesubnet</td>
</tr>
</tbody>
</table>

Subnet Example

This is a reference event for a subnet:

```json
{
  "eventType": "com.oraclecloud.virtualnetwork.createsubnet",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "virtualNetwork",
  "eventTime": "2019-08-12T17:51:42.789Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oci..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "example_name",
    "resourceId": "ocid1.subnet.oci.phx.<unique_ID>",
    "availabilityDomain": "XXIT:PHX-AD-1",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    }
  }
}
```


VCN Event Types

These are the event types that VCNs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create VCN</td>
<td><code>com.oraclecloud.virtualnetwork.createvcn</code></td>
</tr>
<tr>
<td>Delete VCN</td>
<td><code>com.oraclecloud.virtualnetwork.deletevcn</code></td>
</tr>
<tr>
<td>Update VCN</td>
<td><code>com.oraclecloud.virtualnetwork.updatevcn</code></td>
</tr>
</tbody>
</table>

VCN Example

This is a reference event for VCNs:

```json
{
    "eventType": "com.oraclecloud.virtualnetwork.createvcn",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "virtualNetwork",
    "eventTime": "2019-08-12T17:51:42.789Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "example_name",
        "resourceId": "ocid1.vcn.oci.phx..<unique_ID>",
        "availabilityDomain": "XXIT:PHX-AD-1",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        }
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oci..<unique_ID>"
    }
}
```

Virtual Network Interface Card (VNIC) Event Types

These are the event types that VNICs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update VNIC</td>
<td><code>com.oraclecloud.virtualnetwork.updatevnic</code></td>
</tr>
</tbody>
</table>

VNIC Example

This is a reference event for a VNIC:

```json
{
```

Oracle Cloud Infrastructure User Guide 1904
Events

```
"eventType": "com.oraclecloud.virtualnetwork.updatevnic",
"cloudEventsVersion": "0.1",
"eventTypeVersion": "2.0",
"source": "virtualNetwork",
"eventTime": "2019-08-12T17:51:42.789Z",
"contentType": "application/json",
"data": {
  "compartmentId": "ocid1.compartment.oci..<unique_ID>",
  "compartmentName": "example_name",
  "resourceName": "example_name",
  "resourceId": "ocid1.vnic.oci.phx.<unique_ID>",
  "availabilityDomain": "XXIT:PHX-AD-1",
  "freeFormTags": {
    "Department": "Finance"
  },
  "definedTags": {
    "Operations": {
      "CostCenter": "42"
    }
  }
},
"eventId": "<unique_ID>",
"extensions": {
  "compartmentId": "ocid1.compartment.oci..<unique_ID>"
}
```

### VLAN Event Types

These are the event types that VLANs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create VLAN</td>
<td>com.oraclecloud.virtualnetwork.createvlan</td>
</tr>
<tr>
<td>Update VLAN</td>
<td>com.oraclecloud.virtualnetwork.updatevlan</td>
</tr>
<tr>
<td>Delete VLAN</td>
<td>com.oraclecloud.virtualnetwork.deletevlan</td>
</tr>
</tbody>
</table>

### VLAN Example

This is a reference event for a VLAN:

```
{
  "eventType": "com.oraclecloud.virtualnetwork.createvlan",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "virtualNetwork",
  "eventTime": "2020-04-16T17:44:31.116Z",
  "contentType": "application/json",
  "eventId": "<unique_ID>",
  "extensions": {
    "compartmentId": "ocid1.compartment.oci..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oci..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "example_name",
    ...  
  }
}
```
NoSQL Database Cloud

For details about events emitted by Oracle NoSQL Database Cloud, see Service Events.

Notifications

Notifications resources that emit events:

- Subscriptions Event Types on page 1906
- Topics Event Types on page 1907

Subscriptions Event Types

These are the event types that subscriptions emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Subscription</td>
<td>com.oraclecloud.notification.createsubscription</td>
</tr>
<tr>
<td>Delete Subscription</td>
<td>com.oraclecloud.notification.deletesubscription</td>
</tr>
<tr>
<td>Move Subscription</td>
<td>com.oraclecloud.notification.movesubscription</td>
</tr>
<tr>
<td>Resend Subscription Confirmation</td>
<td>com.oraclecloud.notification.resendsubscription</td>
</tr>
<tr>
<td>Update Subscription</td>
<td>com.oraclecloud.notification.updatesubscription</td>
</tr>
</tbody>
</table>

Subscription Example

This is a reference event for subscriptions:

```json
{
    "eventType": "com.oraclecloud.notification.createsubscription",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "notification",
    "eventTime": "2019-01-10T21:19:24Z",
    "contentType": "application/json",
    "data":{
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "my_compartment",
    }
}
```
Topics Event Types

These are the event types that topics emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Topic</td>
<td>com.oraclecloud.notification.createtopic</td>
</tr>
<tr>
<td>Delete Topic</td>
<td>com.oraclecloud.notification.deletetopic</td>
</tr>
<tr>
<td>Move Topic</td>
<td>com.oraclecloud.notification.movetopic</td>
</tr>
<tr>
<td>Update Topic</td>
<td>com.oraclecloud.notification.updatetopic</td>
</tr>
</tbody>
</table>

Topic Example

This is a reference event for topics:

```
{
  "eventType": "com.oraclecloud.notification.createtopic",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "notification",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "data":{
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "my_compartment",
    "resourceName": "my_topic",
    "resourceId": "ocid1.onstopic.oc1..<unique_ID>",
    "availabilityDomain": "AD3"
  },
  "eventID": "<unique_ID>",
  "extensions":{
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  }
}
```

Object Storage

Object Storage resources that emit events:

- Buckets Event Types on page 1908
- Objects Event Types on page 1908
Buckets Event Types

These are the event types that buckets emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Bucket</td>
<td>com.oraclecloud.objectstorage.createbucket</td>
</tr>
<tr>
<td>Delete Bucket</td>
<td>com.oraclecloud.objectstorage.deletebucket</td>
</tr>
<tr>
<td>Update Bucket</td>
<td>com.oraclecloud.objectstorage.updatebucket</td>
</tr>
</tbody>
</table>

Bucket Example

This is an example event for buckets:

```json
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.objectstorage.createbucket",
  "source": "objectstorage",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-01-10T21:19:24Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_bucket",
    "resourceId": "ocid1.compartment.oc1..<unique_ID>",
    "availabilityDomain": "all",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "namespace": "example_namespace",
      "publicAccessType": "NoPublicAccess",
      "eTag": "f8ff6e9-f602-460f-a6c0-00b5abfa24c7"
    }
  }
}
```

Objects Event Types

Events for objects are handled differently than other resources. Objects do not emit events by default. Use the Console, CLI, or API to enable a bucket to emit events for object state changes. You can enable events for object state changes during or after bucket creation.
These are the event types that objects emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Object</td>
<td>com.oraclecloud.objectstorage.createobject</td>
</tr>
<tr>
<td>Delete Object</td>
<td>com.oraclecloud.objectstorage.deleteobject</td>
</tr>
<tr>
<td>Update Object</td>
<td>com.oraclecloud.objectstorage.updateobject</td>
</tr>
</tbody>
</table>

**Object Example**

This is an example event for objects:

```json
{
    "cloudEventsVersion": "0.1",
    "eventID": "<unique_ID>",
    "eventType": "com.oraclecloud.objectstorage.createobject",
    "source": "objectstorage",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-07-10T13:37:11Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "Example_Compartment",
        "resourceName": "v1/log/10.0.6.166",
        "resourceId": "",
        "availabilityDomain": "all",
        "additionalDetails": {
            "eTag": "8162db5b-50d7-4947-a576-4401798ed2fa",
            "namespace": "my_namespace",
            "archivalState": null,
            "bucketName": "my_bucket",
            "bucketId": "ocid1.bucket.oc1.<unique_ID>"
        }
    }
}
```

**Operations Insights**

Operations Insights resources that emit events:

- Database insights
## Database Insight Event Types

These are the event types that database insights emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest SQL Text</td>
<td>com.oraclecloud.OperationsInsights.IngestSqlText</td>
</tr>
<tr>
<td>List SQL Searches</td>
<td>com.oraclecloud.OperationsInsights.ListSqlSearches</td>
</tr>
</tbody>
</table>
Database Insight Example 1: Read Event

Following is a reference read event for database insights:

```json
{
    "eventType": "com.oraclecloud.OperationsInsights.SummarizeDatabaseInsightResourceCapacityTrend",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "OperationsInsights",
    "eventID": "<unique_ID>",
    "eventTime": "2020-09-01T00:05:46.370Z",
    "contentType": "application/json",
    "data": {
        "eventGroupingId": "<unique_ID>",
        "eventName": "SummarizeDatabaseInsightResourceCapacityTrend",
        "compartmentId": "ocid1.compartment.<realm>..<unique_ID>",
        "compartmentName": "example_compartment_name",
        "resourceName": "example_resource_name",
        "resourceId": "resourceCapacityTrend",
        "availabilityDomain": "SoSC:PHX-AD-3",
        "freeformTags": null,
        "definedTags": null
    }
}
```

Database Insight Example 2: Ingest Event

Following is a reference ingest event for database insights:

```json
{
    "eventType": "com.oraclecloud.OperationsInsights.IngestSqlText",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "OperationsInsights",
    "eventID": "<unique_ID>",
    "eventTime": "2020-09-01T01:09:00.688Z",
    "contentType": "application/json",
    "data": {
        "eventGroupingId": "<unique_ID>",
        "eventName": "IngestSqlText",
        "compartmentId": "ocid1.compartment.<realm>..<unique_ID>",
        "compartmentName": "example_compartment_name",
        "resourceName": "example_resource_name",
        "resourceId": "actions",
        "availabilityDomain": "AD1",
        "freeformTags": null,
        "definedTags": null
    }
}
```

OS Management

For details about events emitted by OS Management, see Creating Automation with Events.

Resource Manager

Resource Manager resources that emit events:

- Job Event Types on page 1912
- Stack Event Types on page 1913
### Job Event Types

These are the event types that jobs emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel Job</td>
<td>com.oraclecloud.oracleresourcemanager.canceljob</td>
</tr>
<tr>
<td>Create Job Begin</td>
<td>com.oraclecloud.oracleresourcemanager.createjob.begin</td>
</tr>
<tr>
<td>Create Job End</td>
<td>com.oraclecloud.oracleresourcemanager.createjob.end</td>
</tr>
<tr>
<td>Update Job</td>
<td>com.oraclecloud.oracleresourcemanager.updatejob</td>
</tr>
</tbody>
</table>

This is a reference event for jobs:

```json
{
    "eventType": "com.oraclecloud.oracleresourcemanager.updateJob",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "OracleResourceManager",
    "eventTime": "2019-07-23T01:46:37.606Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "example_name",
        "resourceId": "ocid1.ormjob.oc1.phx.<unique_ID>",
        "availabilityDomain": "availability_domain"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>
    }
}
```
**Stack Event Types**

These are the event types that stacks emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Compartment Begin</td>
<td>com.oraclecloud.oracleresourcemanager.changestackcompartment.begin</td>
</tr>
<tr>
<td>Change Compartment End</td>
<td>com.oraclecloud.oracleresourcemanager.changestackcompartment.end</td>
</tr>
<tr>
<td>Create Stack</td>
<td>com.oraclecloud.oracleresourcemanager.createstack</td>
</tr>
<tr>
<td>Delete Stack</td>
<td>com.oraclecloud.oracleresourcemanager.deletestack</td>
</tr>
<tr>
<td>Update Stack</td>
<td>com.oraclecloud.oracleresourcemanager.updatestack</td>
</tr>
</tbody>
</table>

This is a reference event for stacks:

```json
{
    "eventType": "com.oraclecloud.oracleresourcemanager.createstack",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "OracleResourceManager",
    "eventTime": "2019-07-23T01:32:10.866Z",
    "contentType": "application/json",
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_compartment",
        "resourceName": "example_name",
        "resourceId": "ocid1.ormstack.oc1.phx.<unique_ID>",
        "availabilityDomain": "availability_domain"
    },
    "eventID": "<unique_ID>",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```

**WAF**

WAF resources that emit events:

- [Waas Policy Event Types](page 1914)
- [Address List Event Types](page 1915)
- [Custom Protection Rule Event Types](page 1916)
- [Certificate Event Types](page 1917)
**Waas Policy Event Types**

These are the event types that Waas policies emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Waas Policy Compartment</td>
<td>com.oraclecloud.waf.changewaaspolicycompartment</td>
</tr>
<tr>
<td>Create Waas Policy Begin</td>
<td>com.oraclecloud.waf.createwaaspolicy.begin</td>
</tr>
<tr>
<td>Create Waas Policy End</td>
<td>com.oraclecloud.waf.createwaaspolicy.end</td>
</tr>
<tr>
<td>Delete Waas Policy Begin</td>
<td>com.oraclecloud.waf.deletewaaspolicy.begin</td>
</tr>
<tr>
<td>Delete Waas Policy End</td>
<td>com.oraclecloud.waf.deletewaaspolicy.end</td>
</tr>
<tr>
<td>Update Waas Policy Begin</td>
<td>com.oraclecloud.waf.updatewaaspolicy.begin</td>
</tr>
<tr>
<td>Update Waas Policy End</td>
<td>com.oraclecloud.waf.updatewaaspolicy.end</td>
</tr>
</tbody>
</table>

**Waas Policy Example**

This is an example event for a Waas policy:

```json
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.waf.updatewaaspolicy.begin",
  "source": "waf",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-10-11T13:40:54.931962577Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_waas_policy",
    "resourceId": "ocid1.waaspolicy.oc1..<unique_ID>",
    "availabilityDomain": "all",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    },
    "additionalDetails": {
      "domain": "example.com"
    }
  }
}
```
**Address List Event Types**

These are the event types that address lists emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Address List Compartment</td>
<td>com.oraclecloud.waf.changeaddresslistcompartment</td>
</tr>
<tr>
<td>Create Address List</td>
<td>com.oraclecloud.waf.createaddresslist</td>
</tr>
<tr>
<td>Delete Address List</td>
<td>com.oraclecloud.waf.deleteaddresslist</td>
</tr>
<tr>
<td>Update Address List</td>
<td>com.oraclecloud.waf.updateaddresslist</td>
</tr>
</tbody>
</table>

**Address List Example**

This is an example event for address lists:

```json
{
  "cloudEventsVersion": "0.1",
  "eventID": "<unique_ID>",
  "eventType": "com.oraclecloud.waf.updateaddresslist",
  "source": "waf",
  "eventTypeVersion": "2.0",
  "eventTime": "2019-10-11T13:40:54.931962577Z",
  "contentType": "application/json",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "example_name",
    "resourceName": "my_waas_address_list",
    "resourceId": "ocid1.waasaddresslist.oc1..<unique_ID>",
    "availabilityDomain": "all",
    "freeFormTags": {
      "Department": "Finance"
    },
    "definedTags": {
      "Operations": {
        "CostCenter": "42"
      }
    }
  }
}
```
Custom Protection Rule Event Types

These are the event types that protection rules emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Custom Protection Rule Compartment</td>
<td>com.oraclecloud.waf.changecustomprotectionrulecom.oraclecloud.waf.changecustomprotectionrulecompartment</td>
</tr>
<tr>
<td>Create Custom Protection Rule</td>
<td>com.oraclecloud.waf.createcustomprotectionrulecom.oraclecloud.waf.createcustomprotectionrulecom.oraclecloud.waf.createcustomprotectionrule</td>
</tr>
<tr>
<td>Delete Custom Protection Rule</td>
<td>com.oraclecloud.waf.deletecustomprotectionrulecom.oraclecloud.waf.deletecustomprotectionrulecom.oraclecloud.waf.deletecustomprotectionrule</td>
</tr>
<tr>
<td>Update Custom Protection Rule</td>
<td>com.oraclecloud.waf.updatecustomprotectionrulecom.oraclecloud.waf.updatecustomprotectionrulecom.oraclecloud.waf.updatecustomprotectionrule</td>
</tr>
<tr>
<td>Update Waas Policy Custom Protection Rules</td>
<td>com.oraclecloud.waf.updatewaaspolicycustomprotectionrulecom.oraclecloud.waf.updatewaaspolicycustomprotectionrulecom.oraclecloud.waf.updatewaaspolicycustomprotectionrule</td>
</tr>
</tbody>
</table>

Protection Rule Example

This is an example event for custom protection rules:

```json
{
    "cloudEventsVersion": "0.1",
    "eventID": "<unique_ID>",
    "eventType": "com.oraclecloud.waf.updatecustomprotectionrule",
    "source": "waf",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-10-11T13:40:54.931962577Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    },
    "data": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "example_name",
        "resourceName": "my_waas_custom_protection_rule",
        "resourceId": "ocid1.waascustomprotectionrule.oc1..<unique_ID>",
        "availabilityDomain": "all",
        "freeFormTags": {
            "Department": "Finance"
        },
        "definedTags": {
            "Operations": {
                "CostCenter": "42"
            }
        }
    }
}
```
**Certificate Event Types**

These are the event types that certificates emit:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Certificate Compartment</td>
<td>com.oraclecloud.waf.changecertificatecompartment</td>
</tr>
<tr>
<td>Create Certificate</td>
<td>com.oraclecloud.waf.createcertificate</td>
</tr>
<tr>
<td>Delete Certificate</td>
<td>com.oraclecloud.waf.deletecertificate</td>
</tr>
<tr>
<td>Update Certificate</td>
<td>com.oraclecloud.waf.updatecertificate</td>
</tr>
</tbody>
</table>

**Certificate Example**

This is an example event for certificates:

```
{
    "cloudEventsVersion": "0.1",
    "eventId": "<unique_ID>",
    "eventType": "com.oraclecloud.waf.updatecertificate",
    "source": "waf",
    "eventTypeVersion": "2.0",
    "eventTime": "2019-10-11T13:40:54.931962577Z",
    "contentType": "application/json",
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    }
}
```

**Events Metrics**

You can monitor performance of your rules by using metrics, alarms, and notifications. This topic describes the metrics emitted by the metric namespace `oci_cloudevents` (the Events service).

Resources: rules. Also measures data for events, which are not resources.

**Prerequisites**

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must
Events give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Overview of the Events Service Metrics

You create rules that specify which events should be delivered to other services for processing. This delivery creates the automation in your tenancy. A rule identifies an event pattern to match and specifies other services to deliver matching events to. Metrics help you measure the success of the rules you create (in terms of pattern matching and delivery) and the quality and scope of the emitted events in your tenancy. For more information, see Overview of Events on page 1784.

Available Metrics: oci_cloudevents

The metrics listed in the following table are automatically available for rules you create. You do not need to enable monitoring to get these metrics.

Each metric includes one or more of the following dimensions:

**RESOURCEID**

The OCID of the rule or compartment to which the metric applies.

**EVENTTYPE**

The type of event emitted by a resource.

**RESOURCEDISPLAYNAME**

The name of the rule.

**ACTIONTYPE**

One or more of the following types of resources that receives an event from the Events service.

- Notifications
- Streaming
- Functions

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublishedEvents</td>
<td>Events Emitted</td>
<td>count</td>
<td>Total number of events emitted by resources in a compartment.</td>
<td>eventType, resourceId</td>
</tr>
<tr>
<td>MatchedEvents</td>
<td>Events Matched</td>
<td>count</td>
<td>If you view the default chart from a rule, this metric provides the total number of events matched for the rule. If you view the chart from the Service Metrics page, this metric gives a total number of matched events for all the rules in a compartment.</td>
<td>resourceDisplayName, resourceId</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>DeliverySucceedEvents</td>
<td>Events Delivered</td>
<td>count</td>
<td>If you view the default chart from a rule, this metric provides the total number of successful deliveries to actions for the rule. If you view the chart from the Service Metrics page, this metric gives a total number of successful deliveries to actions for all the rules in a compartment.</td>
<td>actionType, resourceDisplayName, resourceId</td>
</tr>
<tr>
<td>DeliveryFailedEvents</td>
<td>Delivery Failure</td>
<td>count</td>
<td>If you view the default chart from a rule, this metric provides the total number of unsuccessful deliveries to actions for the rule. If you view the chart from the Service Metrics page, this metric gives a total number of unsuccessful deliveries to actions for all the rules in a compartment.</td>
<td>actionType, resourceDisplayName, resourceId</td>
</tr>
</tbody>
</table>

### Using the Console

#### To view default metric charts for a rule

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose the **Compartment** that contains the rule you want to view, and then click the rule's name.
3. Click **Metrics**. The **Metrics** page displays a default set of charts for the current rule.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

#### To view default metric charts for a compartment

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Application Integration** and click **Events Service**.
2. Choose the **Compartment** that contains the rules you want to monitor.
3. Click **Metrics**. The **Metrics** page displays a default set of charts for the current compartment.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

### Using the API

Use the following APIs for monitoring:

- **Monitoring API** for metrics and alarms
- **Notifications API** for notifications (used with alarms)
Chapter 18

File Storage

This chapter explains how to create file systems, how to manage them, and how to mount them to write files.

Overview of File Storage

Oracle Cloud Infrastructure File Storage service provides a durable, scalable, secure, enterprise-grade network file system. You can connect to a File Storage service file system from any bare metal, virtual machine, or container instance in your Virtual Cloud Network (VCN). You can also access a file system from outside the VCN using VCN peering, Oracle Cloud Infrastructure FastConnect, and Internet Protocol security (IPSec) virtual private network (VPN).

Large Compute clusters of thousands of instances can use the File Storage service for high-performance shared storage. Storage provisioning is fully managed and automatic as your use scales from a single byte to exabytes without upfront provisioning.

The File Storage service supports the Network File System version 3.0 (NFSv3) protocol. The service supports the Network Lock Manager (NLM) protocol for file locking functionality.

Oracle Cloud Infrastructure File Storage employs 5-way replicated storage, located in different fault domains, to provide redundancy for resilient data protection. Data is protected with erasure encoding.

The File Storage service uses the "eventual overwrite" method of data eradication. Files are created in the file system with a unique encryption key. When you delete a single file, its associated encryption key is eradicated, making the file inaccessible. When you delete an entire file system, the file system is marked as inaccessible. The service systematically traverses deleted files and file systems, frees all the used space, and eradicates all residual files.

Use the File Storage service when your application or workload includes big data and analytics, media processing, or content management, and you require Portable Operating System Interface (POSIX)-compliant file system access semantics and concurrently accessible storage. The File Storage service is designed to meet the needs of applications and users that need an enterprise file system across a wide range of use cases, including the following:

- **General Purpose File Storage:** Access to an unlimited pool of file systems to manage growth of structured and unstructured data.
- **Big Data and Analytics:** Run analytic workloads and use shared file systems to store persistent data.
- **Lift and Shift of Enterprise Applications:** Migrate existing Oracle applications that need NFS storage, such as Oracle E-Business Suite and PeopleSoft.
- **Databases and Transactional Applications:** Run test and development workloads with Oracle, MySQL, or other databases.
- **Backups, Business Continuity, and Disaster Recovery:** Host a secondary copy of relevant file systems from on premises to the cloud for backup and disaster recovery purposes.
- **MicroServices and Docker:** Deliver stateful persistence for containers. Easily scale as your container-based environments grow.

Tip:

Watch a video introduction to the service and its capabilities.
File Storage Concepts

Using the File Storage service requires an understanding of the following concepts, including some that pertain to Oracle Cloud Infrastructure Networking:

**MOUNT TARGET**

An NFS endpoint that lives in a subnet of your choice and is highly available. The mount target provides the IP address or DNS name that is used in the mount command when connecting NFS clients to a file system. File systems are exported (made available) through mount targets. When you use the console to create your first file system, the workflow also creates a mount target and export for it.

You can reuse the same mount target to make as many file systems available on the network as you wish. To reuse the same mount target for multiple file systems, create an export in the mount target for each file system.

Mount target limitations:

- Each mount target can accept up to 100,000 NFS client connections.
- If you use in-transit encryption, each mount target can accept up to 64 NFS/SSL client connections. See Using In-transit Encryption on page 1942 for more information.
- By default, you can create two mount targets per account per availability domain. See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

See Managing Mount Targets on page 1980 for more information about working with this resource.

**EXPORT**

Exports control how NFS clients access file systems when they connect to a mount target. File systems are exported (made available) through mount targets. Each mount target maintains an export set which contains one or many exports. A file system must have at least one export in one mount target in order for instances to mount the file system. The information used by an export includes the file system OCID, mount target OCID, export set OCID, export path, and client export options. When you use the console to create your first file system, the workflow also creates a mount target and export for it. Thereafter,

- You can create as many exports in a mount target for different file systems as you wish.
- You can create as many exports in a mount target for a single file system as you wish.
- You can delete and re-create exports in a mount target as often as you need to.
- You can add export options to an export to control access to the file system.

For more information, see Managing Mount Targets on page 1980 and Working with NFS Export Options on page 1934.

**EXPORT SET**

Collection of one or more exports that control what file systems the mount target exports using NFSv3 protocol and how those file systems are found using the NFS mount protocol. Each mount target has an export set. Each file system associated with the mount target has at least one export in the export set.

**EXPORT PATH**

A path that is specified when an export is created. It uniquely identifies the file system within the mount target, letting you associate many file systems to a single mount target. This path is unrelated to any path within the file system itself, or the client mount point path.

The File Storage service adds an export that pairs the file system's Oracle Cloud Identifier (OCID) and path. See Paths in File Systems on page 2006 for more information.
EXPORT OPTIONS

NFS export options are a set of parameters within the export that specify the level of access granted to NFS clients when they connect to a mount target. An NFS export options entry within an export defines access for a single IP address or CIDR block range. You can have up to 100 options per export. For more information, see Working with NFS Export Options on page 1934.

VIRTUAL CLOUD NETWORK (VCN)

A private network that you set up in the Oracle data centers, with firewall rules and specific types of communication gateways that you can choose to use. A VCN covers a single, contiguous IPv4 CIDR block of your choice. For more information about VCNs, see VCNs and Subnets on page 2821 in the Oracle Cloud Infrastructure Networking documentation.

You can set up a service gateway and give your VCN private access to the File Storage service. A service gateway can be used only by resources in the gateway's own VCN. Traffic to the service will not travel through the internet. When creating the service gateway, enable the service label called All <region> Services in Oracle Services Network. It includes the File Storage service. Be sure to update route tables for any subnets that need to access File Storage through the service gateway.

For more information and detailed instructions, see Setting Up a Service Gateway in the Console on page 3260.

SUBNETS

Subdivisions you define in a VCN (for example, 10.0.0.0/24 and 10.0.1.0/24). Subnets contain virtual network interface cards (VNICs), which attach to instances. A subnet can span a region or exist in a single availability domain. A subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. For each subnet, you specify the routing rules and security lists that apply to it. For more information about subnets, see VCNs and Subnets on page 2821 in the Oracle Cloud Infrastructure Networking documentation.

SECURITY RULES

Virtual firewall rules for your VCN. Your VCN comes with a default security list, and you can add more. These security lists provide ingress and egress rules that specify the types of traffic allowed in and out of the instances. You can choose whether a given rule is stateful or stateless. Security list rules must be set up so that clients can connect to file system mount targets.

Network security groups (NSGs). Another method for applying security rules is to set them up in a network security group (NSG), and then add the mount target to the NSG. Unlike security list rules that apply to all VNICs in the subnet, NSGs apply only to resource VNICs you add to the NSG.


SNAPSHOTS

Snapshots provide a consistent, point-in-time view of your file system, and you can take as many snapshots as you need. You pay only for the storage used by your data and metadata, including storage capacity used by snapshots. Each snapshot reflects only data that changed from the previous snapshot. For more information, see Managing Snapshots on page 1990.

Encryption

The File Storage service encrypts all file system and snapshot data at rest. By default all file systems are encrypted using Oracle-managed encryption keys. You have the option to encrypt all of your file systems using the keys that you own and manage using the Vault service.

Note:

Currently, only symmetric Advanced Encryption Standard (AES) keys are supported for file system encryption.
For more information, see Overview of Vault on page 3952.

For information about how to use your own key for new file systems, see Creating File Systems on page 1948. See To update the key for a file system on page 1978 for how to assign or change the key for an existing file system.

Data Transfers

FastConnect offers you the ability to accelerate data transfers. You can leverage the integration between FastConnect and the File Storage service to perform initial data migration, workflow data transfers for large files, and disaster recovery scenarios between two regions, among other things.

File Storage Space Allocation

The File Storage service allocates space in blocks of variable size in a way that is fine-tuned to minimize total customer cost and optimize performance for modern workloads. The minimum block size used is 8192 bytes. For example, if you create a 1-byte file, we allocate 8192 bytes. We use larger blocks to store larger files. To learn more about file system and snapshot usage, see File System Usage and Metering on page 2007.

How File Storage Permissions Work

File Storage service resources include file systems, mount targets, and export sets. The AUTH_UNIX style of authentication and permission checking is supported for remote NFS client requests. You use Oracle Cloud Infrastructure Identity and Access Management (IAM) policy language to define access to Oracle Cloud Infrastructure resources. You can consider exports and snapshots subsidiary resources of export sets and file systems, respectively. As such, they do not need their own permissions. Related resources include Oracle Cloud Infrastructure Compute instances and Oracle Cloud Infrastructure Networking virtual cloud networks (VCNs).

Oracle Cloud Infrastructure users require resource permissions to create, delete, and manage resources. Without the appropriate IAM permissions, you cannot export a file system through a mount target. Until a file system has been exported, Compute instances cannot mount it. For more information about creating an IAM policy, see Let users create, manage, and delete file systems on page 2148.

If you have successfully exported a file system on a subnet, then you use Networking security lists to control traffic to and from the subnet and, therefore, the mount target. Security lists act as a virtual firewall, allowing only the network traffic you specify to and from the IP addresses and port ranges configured in your ingress and egress rules. The security list you create for the subnet lets hosts send and receive packets and mount the file system. If you have firewalls on individual instances, use FastConnect, or use a virtual private network (VPN), the settings for those might also impact security at the networking layer. For more information about creating a security list for the File Storage service, see Creating File Systems on page 1948. See About Security on page 1925 for more information on how different types of security work together in your file system.

Regions and Availability Domains

You can use the File Storage service in all regions. For a list of supported regions, see Regions and Availability Domains on page 180.

When you create file systems and mount targets, you specify the availability domain they are created in. All file system data is then stored entirely within the availability domain the file system resides in. Within an availability domain, the File Storage service uses synchronous replication and high availability failover to keep your data safe and available.

You cannot move a file system to a different availability domain or region. However, you can take a snapshot of your data and use a tool such as rsync to copy your data to a different availability domain or region. To maximize performance for data protection operations, you can use the File Storage Parallel Tools suite. The Parallel File Tools suite provides parallel versions of tar, rm, and cp. See Managing Snapshots on page 1990 for more information on using snapshots to protect your data.

While it is possible to access mount targets from any availability domain in a region, for optimal performance, place File Storage resources in the same availability domain as the Compute instances that access them.
Subnets can be either AD-specific or regional. You can create File Storage resources in either type of subnet. Regional subnets allow Compute instances to connect to any mount target in the subnet regardless of AD, with no additional routing configuration. However, to minimize latency, place mount targets in the same AD as Compute instances just as you would in an AD-specific subnet. For more information, see Overview of VCNs and Subnets on page 2822.

Creating Automation with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

The following File Storage resources emit events:

- File systems
- Snapshots
- Mount targets
- Exports
- Export sets

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Limits on Your File Storage Components

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

To set compartment-specific limits on file systems or mount targets, administrators can use compartment quotas.
Additional Documentation Resources

The following Oracle Cloud Infrastructure File Storage service solution playbooks and white papers are available:

- **Sharing the Application Tier File System in Oracle E-Business Suite Release 12.2 or 12.1.3 Using the Oracle Cloud Infrastructure File Storage Service**
  Learn best practices for using a File Storage service shared application tier file system for Oracle E-Business Suite.

- **Learn about deploying Oracle E-Business Suite on Oracle Cloud Infrastructure**
  Learn how file storage is part of a multihost, secure, high-availability topology for Oracle E-Business Suite.

- **Design a pilot-light disaster recovery (DR) topology**
  Learn how to use file storage in your disaster recovery topology.

About Security

Access Control

The File Storage service uses four different layers of access control. Each layer has its own authorization entities and methods which are separate from the other layers.

| Tip: Watch a video about security in File Storage. |

The **Oracle Cloud Infrastructure (OCI) policy** layer uses policies to control what users can do within Oracle Cloud Infrastructure, such as creating instances, a VCN and its security rules, mount targets, and file systems.

The **Network security** layer controls which instance IP addresses or CIDR blocks can connect to a host file system. It uses VCN security list rules to allow or deny traffic to the mount target, and therefore access to any associated file system.

The **NFS export option** layer is a method of applying access control per-file system export based on source IP address that bridges the Network Security layer and the NFS v.3 Unix Security layer.

The **NFS v.3 Unix security** layer controls what users can do on the instance, such as installing applications, creating directories, mounting external file systems by a local mount point, and reading and writing files.

<table>
<thead>
<tr>
<th>This security layer...</th>
<th>Uses these...</th>
<th>To control actions like...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Oracle Cloud Infrastructure Identity and Access Management</strong></td>
<td>Users and policies</td>
<td>Creating instances and VCNs. Creating, listing, and associating file systems and mount targets.</td>
</tr>
<tr>
<td><strong>Network security</strong></td>
<td>IP addresses, CIDR blocks, security lists</td>
<td>Connecting the client instance to the mount target.</td>
</tr>
<tr>
<td><strong>NFS v.3 Unix security</strong></td>
<td>Unix users, file mode bits</td>
<td>Mounting file systems, reading and writing files.</td>
</tr>
</tbody>
</table>
This security layer... | Uses these... | To control actions like...
--- | --- | ---
NFS export options | File system exports, IP addresses, Unix users | Privileged source port connection, reading and writing files, and limiting root user access on a per-file system basis.

**Oracle Cloud Infrastructure Identity and Access Management**

You can create users and groups in Oracle Cloud Infrastructure. Then, you can use policies to specify which users and groups can create, access, or modify resources such as file systems, mount targets, snapshots, and export options within. See [Overview of Oracle Cloud Infrastructure Identity and Access Management](#) on page 2124 to learn more about how to set up access.

**Network Security**

The network security layer allows you to use VCN network security groups (NSGs) and security rules to block the appropriate ports from specific IP addresses and CIDR blocks and restrict host access. However, it’s on an ‘all or nothing’ basis - the client either can or cannot access the mount target, and therefore all file systems associated with it. See [Ways to Secure Your Network](#) on page 2830 for general information about VCN security groups, security lists, and rules. See [Configuring VCN Security Rules for File Storage](#) on page 1927 for specific information about the security rules necessary for File Storage.

**NFS v.3 Unix security**

File Storage service supports the AUTH_UNIX style of authentication and permission checking for remote NFS client requests. When mounting file systems, we recommend that you use the `-nosuid` option. This option disables set-user-identifier or set-group-identifier bits. Remote users are prevented from gaining higher privileges using a `setuid` program. For more information, see [Mounting File Systems](#) on page 1954.

Remember that users in UNIX aren’t the same as users in Oracle Cloud Infrastructure - they’re not linked or associated in any way. The Oracle Cloud Infrastructure policy layer doesn’t govern anything that happens inside the file system, the UNIX security layer does. Conversely, the UNIX security layer doesn’t govern creating file systems or mount targets in Oracle Cloud Infrastructure.

File Storage does not support file level Access Control Lists (ACLs). Only `user`, `group`, and `world` permissions are supported. File Storage uses the NFSv3 protocol, which doesn’t include support for ACLs. `setfacl` fails on mounted file systems. `getfacl` returns only standard permissions.

**Note:**

Some implementations might extend the NFSv3 protocol and add support for ACLs as part of a separate `rpc` program.

**SETFAACL error example**

This example shows an example of a `setfacl` error:

```
[opc@example setfacl_testing]$ ls -ld test
drwxr--r--. 2 opc opc 0 Jul 2 10:31 test
[opc@example setfacl_testing]$ setfacl -m u:applmgr:r test
setfacl: test: Operation not supported
```

Oracle Cloud Infrastructure User Guide 1926
NFS export options

NFS export options are a method of applying access control at both the network security layer and the NFS v.3 Unix security layer. You can use NFS export options to limit access levels by IP addresses or CIDR blocks connecting to multiple file systems through exports of an associated mount target. Access can be restricted so that each client’s file system is inaccessible and invisible to the other, allowing for managed hosted environment security. Moreover, you can set NFS v.3 Unix security permissions for read-only, read/write, or root-squash for your file systems. See Working with NFS Export Options on page 1934 for more information.

Encryption

Within Oracle Cloud Infrastructure

All data is encrypted at rest. You can leave all encryption-related matters to Oracle, or you can choose to manage your own encryption using the Oracle Cloud Infrastructure Vault (KMS) service. You can use KMS to create master encryption keys and data encryption keys, rotate keys to generate new cryptographic material, enable or disable keys for use in cryptographic operations, assign keys to file systems, and use keys for encryption and decryption.

Note:
Currently, only symmetric Advanced Encryption Standard (AES) keys are supported for file system encryption.

For more information, see Overview of Vault on page 3952.

Between Instances and Mounted File Systems

In-transit encryption provides a way to secure your data between instances and mounted file systems using TLS v. 1.2 (Transport Layer Security) encryption.

In-transit encryption is enabled by installing a client package on your instance. The package creates an NFS endpoint, network namespace, and network interface. A forwarder process receives requests from the NFS client, encrypts them and sends them to the mount target using a TLS tunnel.

For more information, see Using In-transit Encryption on page 1942.

Configuring VCN Security Rules for File Storage

Before you can mount a file system, you must configure security rules to allow traffic to the mount target’s VNIC using specific protocols and ports. Security rules enable traffic for the following:

- Open Network Computing Remote Procedure Call (ONC RPC) rpcbind utility protocol
- Network File System (NFS) protocol
- Network File System (MOUNT) protocol
- Network Lock Manager (NLM) protocol

File Storage Security Rule Scenarios

There are three basic scenarios that require different security rules for File Storage:
Scenario A: Mount target and instance in the same subnet

In this scenario, the mount target that exports the file system is in the same subnet as the instance you want to mount the file system to.

- Stateful ingress from ALL ports in source CIDR block to TCP ports 111, 2048, 2049, and 2050.
- Stateful ingress from ALL ports in source CIDR block to UDP ports 111 and 2048.
- Stateful egress from TCP ALL ports to ports 111, 2048, 2049, and 2050 in destination CIDR block.
- Stateful egress from UDP ALL ports to port 111 in destination CIDR block.

Important:
Oracle recommends that NFS clients be limited to reserved ports. To do this, set the Source Port range to 1-1023. You can also set export options for a file system to require clients to connect from a privileged source port. For more information, see Working with NFS Export Options on page 1934.

Here's an example of the rules for Scenario A set up for a single subnet that contains both the mount target and the instance. In this example, both the mount target and the instance are in CIDR block 10.0.0.0/24:

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source</th>
<th>IP Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>All</td>
<td>2048-2050</td>
<td>TCP traffic for ports: 2048-2050</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>All</td>
<td>111</td>
<td>TCP traffic for ports: 111</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>UDP</td>
<td>All</td>
<td>2048</td>
<td>UDP traffic for ports: 2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>UDP</td>
<td>All</td>
<td>111</td>
<td>UDP traffic for ports: 111</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using a security list

Security lists are associated with subnets. You can set up the required security rules in the default security list for the mount target subnet, or create a new security list. Security list rules apply to all resources in the subnet.

Using a network security group (NSG)

Another method for applying security rules is to set them up in a network security group (NSG), and then add the mount target to the NSG. Unlike security list rules that apply to all VNICs in the subnet, NSGs apply only to the resource VNICs you add to the NSG.

See Ways to Enable Security Rules for File Storage on page 1931 for an overview of these methods and instructions about how to use them to set up security rules.

Scenario B: Mount target and instance in different subnets

In this scenario, the mount target that exports the file system is in a different subnet than the instance you want to mount the file system to. Security rules must be configured for both the mount target and the instance either in a security list for each subnet, or a network security group (NSG) for each resource.

Set up the following the following security rules for the mount target. Specify the instance IP address or CIDR block as the source for ingress rules and the destination for egress rules:
• Stateful ingress from ALL ports in the source instance CIDR block to TCP ports 111, 2048, 2049, and 2050.
• Stateful ingress from ALL ports in the source instance CIDR block to UDP ports 111 and 2048.
• Stateful egress from TCP ports 111, 2048, 2049, and 2050 to ALL ports in the destination instance CIDR block.
• Stateful egress from UDP port 111 ALL ports in the destination instance CIDR block.

**Important:**

Oracle recommends that NFS clients be limited to reserved ports. To do this, set the **Source Port** range to **1-1023**. You can also set export options for a file system to require clients to connect from a privileged source port. For more information, see [Working with NFS Export Options](#) on page 1934.

Next, set up the following security rules for the **instance**. Specify the mount target IP address or CIDR block as the **source** for ingress rules and the **destination** for egress rules:

• Stateful ingress from source mount target CIDR block TCP ports 111, 2048, 2049, and 2050 to ALL ports.
• Stateful ingress from source mount target CIDR block UDP port 111 to ALL ports.
• Stateful egress from ALL ports to destination mount target CIDR block TCP ports 111, 2048, 2049, and 2050.
• Stateful egress from ALL ports to destination mount target CIDR block UDP ports 111 and 2048.

Here's an example of the rules for Scenario B set up in security list rules for the instance and mount target. This example shows rules for specific source and destination CIDR blocks.

**Ingress** rules for the mount target's NSG or subnet security list. The instance CIDR block **10.0.0.0/24** is the source:

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source</th>
<th>IP Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>All</td>
<td>111</td>
<td>TCP traffic for port s: 111</td>
<td>FSS Ingress rule to a sccpt connections fro m the Source - Instan ce subnet CIDR 10.0.0/24 on TCP 111, 2 048-2050</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>All</td>
<td>2048-2050</td>
<td>TCP traffic for port s: 2048-2050</td>
<td>FSS Ingress rule to a sccpt connections fro m the Source - Instan ce subnet CIDR 10.0.0/24 on TCP 111, 2 048-2050</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>UDP</td>
<td>All</td>
<td>111</td>
<td>UDP traffic for port s: 111</td>
<td>FSS Ingress rule to a sccpt connections fro m the Source - Instan ce subnet CIDR 10.0.0/24 on UDP 111 a nd 2048</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>UDP</td>
<td>All</td>
<td>2048</td>
<td>UDP traffic for port s: 2048</td>
<td>FSS Ingress rule to a sccpt connections fro m the Source - Instan ce subnet CIDR 10.0.0/24 on UDP 111 a nd 2048</td>
<td></td>
</tr>
</tbody>
</table>

**Egress** rules for the mount target's NSG or subnet security list. The instance CIDR block **10.0.0.0/24** is the destination:
### Ingress rules for the instance's NSG or subnet security list.

The `mount target` CIDR block `10.0.1.0/24` is the source:

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>TCP</td>
<td>2048-2050</td>
<td>All</td>
<td>TCP traffic for ports: All</td>
<td></td>
<td>Ingress rule for the instance not allowing TCP connections from mount target source ports 2048-2050</td>
</tr>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>TCP</td>
<td>111</td>
<td>All</td>
<td>TCP traffic for ports: All</td>
<td></td>
<td>Ingress rule for the instance not allowing TCP connections from mount target source port 111</td>
</tr>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>UDP</td>
<td>111</td>
<td>All</td>
<td>UDP traffic for ports: All</td>
<td></td>
<td>Ingress rule for the instance not allowing UDP connections from mount target source port 111</td>
</tr>
</tbody>
</table>

0 Selected  
Showing 3 items  
Page 1  

### Egress rules for the instance's NSG or subnet security list.

The `mount target` CIDR block `10.0.1.0/24` is the destination:

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>TCP</td>
<td>All</td>
<td>2048-2050</td>
<td>TCP traffic for ports: 2048-2050</td>
<td></td>
<td>Egress rule for the instance not allowing TCP connections to the mount target port 2048-2050</td>
</tr>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>TCP</td>
<td>All</td>
<td>111</td>
<td>TCP traffic for ports: 111</td>
<td></td>
<td>Egress rule for the instance not allowing TCP connections to the mount target port 111</td>
</tr>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>UDP</td>
<td>All</td>
<td>111</td>
<td>UDP traffic for ports: 111</td>
<td></td>
<td>Egress rule for the instance not allowing UDP connections to the mount target port 111</td>
</tr>
<tr>
<td>No</td>
<td>10.0.1.0/24</td>
<td>UDP</td>
<td>All</td>
<td>2048</td>
<td>UDP traffic for ports: 2048</td>
<td></td>
<td>Egress rule for the instance not allowing UDP connections to the mount target port 2048</td>
</tr>
</tbody>
</table>

### Using a Security List

Security lists are associated with subnets. If you use security lists to set up your security rules, you need to set up the mount target rules in the mount target subnet, and the instance rules in the instance subnet. You can add the rules to the default security list for each subnet, or create new security lists.
Using a network security group (NSG)

Another method for applying security rules is to set them up in a network security group (NSG), and then add the mount target and instance to the NSG. Unlike security list rules that apply to all VNICs in the subnet, NSGs apply only to resource VNICs you add to the NSG.

See Ways to Enable Security Rules for File Storage on page 1931 for an overview of these methods and instructions about how to use them to set up security rules.

**Scenario C: Mount target and instance use in-transit encryption**

In this scenario, in-transit encryption secures your data between instances and mounted file systems using TLS v.1.2 (Transport Layer Security) encryption. See Using In-transit Encryption on page 1942 for more information.

You can limit the source or destination to the IP address or CIDR block of your choice. Alternatively, you can allow traffic from all sources or destinations.

Set up the following security rules for the **mount target**:

- **Stateful ingress** from ALL ports in the source CIDR block to TCP port **2051**.
- **Stateful egress** from TCP port **2051** to ALL ports in the destination CIDR block.

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Source</th>
<th>IP Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>All</td>
<td>2051</td>
<td>TCP traffic for port 2051</td>
<td>Ingress rule allowing traffic from 10.0.0.0/24 to port 2051 for FIB in-bundle encryption.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stateless</th>
<th>Destination</th>
<th>IP Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>Type and Code</th>
<th>Allows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>10.0.0.0/24</td>
<td>TCP</td>
<td>2051</td>
<td>All</td>
<td>TCP traffic for port 2051</td>
<td>Egress rule allowing traffic to 10.0.0.0/24 from port 2051 for FIB in-bundle encryption.</td>
<td></td>
</tr>
</tbody>
</table>

Using a security list

Security lists are associated with subnets. You can set up the required security rules in the default security list for the mount target subnet, or create a new security list. Security list rules apply to all resources in the subnet.

Using a network security group (NSG)

Another method for applying security rules is to set them up in a network security group (NSG), and then add the mount target to the NSG. Unlike security list rules that apply to all VNICs in the subnet, NSGs apply only to resource VNICs you add to the NSG.

See Ways to Enable Security Rules for File Storage on page 1931 for an overview of these methods and instructions about how to use them to set up security rules.

**Ways to Enable Security Rules for File Storage**

The Networking service offers two virtual firewall features that both use security rules to control traffic at the packet level. The two features are:

- **Security lists**: The original virtual firewall feature from the Networking service. When you create a VCN, a default security list is also created. Add the required rules to the security list for the subnet that contains the mount target. (If you're setting up Scenario B: Mount target and instance in different subnets on page 1928, you have to add rules for both subnets.) See Setting Up Required Rules in a Security List on page 1932 for instructions.

- **Network security groups (NSGs)**: A subsequent feature designed for application components that have different security postures. Create an NSG that contains the required rules, and then add the mount target to the NSG. Alternatively, you can add the required rules to a previously existing NSG, and add the mount target to the NSG. Each mount target can belong to up to five (5) NSGs. (If you're setting up Scenario B: Mount target and instance in different subnets on page 1928, you have to add both the mount target and instance to an NSG that contains the required security rules.) See Setting Up Required Rules in a Network Security Group (NSG) on page 1933 for instructions.
Important:

You can use security lists alone, network security groups alone, or both together. It depends on your particular security needs.

If you choose to use both security lists and network security groups, the set of rules that applies to a given mount target VNIC is the combination of these items:

- The security rules in the security lists associated with the VNIC's subnet
- The security rules in all NSGs that the VNIC is in

It doesn't matter which method you use to apply security rules to the mount target VNIC, as long as the ports for protocols necessary for File Storage are correctly configured in the rules applied.

See Security Rules on page 2833, Security Lists on page 2850, and Network Security Groups on page 2841 for more information, examples, and scenarios about how these features interact in your network. Networking Overview on page 2748 provides general information about networking. See About Security on page 1925 for information about how security rules work with other types of security in File Storage.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let network admins manage a cloud network on page 2143 covers management of all networking components, including security lists and NSGs. See the Policy Reference on page 2167 for more information.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Using the Console

Setting Up Required Rules in a Security List

You can add the required rules to a pre-existing security list associated with a subnet, such as the default security list that is created along with the VCN. See To create a security list on page 2853 for more information.

To add required rules to a security list

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. In the Scope section, select the compartment that contains the VCN the subnet is in.
3. Click the name of the VCN.
4. On the details page for the cloud network, in Resources, and then click Security Lists.
5. Click the name of the security list used by the subnet.
7. Click Add Ingress Rules.

- Specify that it's a stateful rule by leaving the check box clear. (For more information about stateful and stateless rules, see Stateful Versus Stateless Rules on page 2839). By default, rules are stateful unless you specify otherwise.
- To allow traffic from the subnet of the cloud network, click Source Type, choose CIDR, and then enter the CIDR block for the subnet. For example, 10.0.0.0/24.
- Click IP Protocol, and then choose the protocol. For example, TCP.
- In Source Port Range, specify the range of ports that you want to allow traffic from. Alternatively, accept the default of All to allow traffic from any source port.
- Click Destination Port Range, and then enter individual ports or a port range. For example, 2048-2050.
8. Click + Additional Ingress Rule to create more ingress rules.
9. When you're done, click Add Ingress Rules.
11. Click Add Egress Rules.
   • Specify that it's a stateful rule by leaving the check box clear.
   • Click Destination Type, choose CIDR, and then enter the CIDR block for the subnet. For example, 10.0.0.0/24.
   • Click IP Protocol, and then choose the protocol. For example, TCP.
   • In Source Port Range, and then enter individual ports or a port range. For example, 2048-2050.
   • In Destination Port Range, accept the default of All to allow traffic to any destination port.
12. Click + Additional Egress Rule to create more egress rules.
13. When you're done, click Add Egress Rules.

**Setting Up Required Rules in a Network Security Group (NSG)**

The general process for setting up NSGs that work with File Storage is:

1. Create an NSG with the required security rules. (Alternatively, you can add them to a previously existing NSG.)
2. Add the mount target (or more specifically, the mount target's VNIC) to the NSG. You can do this when you create the mount target, or you can update the mount target and add it to one or more NSGs that contain the required security rules.
3. If you're setting up Scenario B: Mount target and instance in different subnets on page 1928, you'll have to add both the mount target and instance to an NSG that contains the required security rules.

To create an NSG with the required security rules

Prerequisite: Become familiar with the parts of security rules.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
5. Enter the following:
   • **Name**: A descriptive name for the network security group. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   • **Create in Compartment**: The compartment where you want to create the network security group, if different from the compartment you're currently working in.
   • **Show Tagging Options**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
6. Click Next.
7. Enter ingress rules.
   • Specify that it's a stateful rule by leaving the check box clear. (For more information about stateful and stateless rules, see Stateful Versus Stateless Rules on page 2839). By default, rules are stateful unless you specify otherwise.
   • In **Direction**, choose Ingress.
   • To allow traffic from the subnet of the cloud network, click **Source Type**, choose CIDR, and then enter the CIDR block for the subnet. For example, 10.0.0.0/24.
   • Click IP Protocol, and then choose the protocol. For example, TCP.
   • In **Source Port Range**, specify the range of ports that you want to allow traffic from. Alternatively, accept the default of All to allow traffic from any source port.
   • Click **Destination Port Range**, and then enter individual ports or a port range. For example, 2048-2050.
8. Click + Another Rule to create more ingress rules.
9. Enter egress rules.
   • Specify that it's a stateful rule by leaving the check box clear.
   • In Direction, choose Egress.
   • Click Destination Type, choose CIDR, and then enter the CIDR block for the subnet. For example, 10.0.0.0/24.
   • Click IP Protocol, and then choose the protocol. For example, TCP.
   • In Source Port Range, and then enter individual ports or a port range. For example, 2048-2050.
   • In Destination Port Range, accept the default of All to allow traffic to any destination port.
10. Click + Another Rule to create more egress rules.
11. When you're done, click Create.

To add a mount target to an NSG

• When creating a mount target along with a file system: See To create a file system on page 1948.
• When creating only the mount target: See To create a mount target on page 1983.
• For an existing mount target:
  1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
  2. In the List Scope section, select a compartment.
  3. Find the mount target you're interested in, click the Actions icon (three dots), and then click View Mount Target Details.
  4. In the Mount Target Information tab, click the Edit link next to Network Security Groups.
  5. Select a Compartment and NSG from the list.
  6. Click Save.

To add an instance to an NSG

See To add or remove a resource from an NSG on page 2848 for instructions on how to add an instance to an NSG.

Working with NFS Export Options

This topic describes the basic features of NFS export options, and how to control client access to your file system.

Overview

NFS export options enable you to create more granular access control than is possible using just security list rules to limit VCN access. You can use NFS export options to specify access levels for IP addresses or CIDR blocks connecting to file systems through exports in a mount target. Access can be restricted so that each client's file system is inaccessible and invisible to the other, providing better security controls in multi-tenant environments.

Using NFS export option access controls, you can limit clients' ability to connect to the file system and view or write data. For example, if you want to allow clients to consume but not update resources in your file system, you can set access to Read Only. You can also reduce client root access to your file systems and map specified User IDs (UIDs) and Group IDs (GIDs) to an anonymous UID/GID of your choice. For more information about how NFS export options work with other security layers, see About Security on page 1925.

Tip:
Watch a video about working with NFS export options in File Storage.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users create, manage, and delete file systems on page 2148 allows users to manage NFS export options.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.
Exports

Exports control how NFS clients access file systems when they connect to a mount target. File systems are exported (made available) through mount targets. Each mount target maintains an export set which contains one or many exports. A file system may be exported through one or more mount targets. A file system must have at least one export in one mount target in order for instances to mount the file system. The information used by an export includes the file system OCID, mount target OCID, export set OCID, export path, and client export options. Typically, an export is created in a mount target when the file system is created. Thereafter, you can create additional exports for a file system in any mount target that resides in the same availability domain as the file system.

See To create an export for a file system on page 1972 for more information.

NFS Export Options

NFS export options are a set of parameters within the export that specify the level of access granted to NFS clients when they connect to a mount target. An NFS export options entry within an export defines access for a single IP address or CIDR block range. You can have up to 100 options per export.

Each separate client IP address or CIDR block you want to define access for needs a separate export options entry in the export. For example, if you want to set options for NFS client IP addresses 10.0.0.6, 10.0.0.8, and 10.0.0.10, you need to create three separate entries, one for each IP address.

File Storage service considers the listed order of each export options entry for the export. During an NFS request by a client, File Storage service applies the first set of options that matches the client Source IP address. Only the first set is applied; the rest are ignored.

For example, consider the following two export options entries specifying access for an export:

Entry 1: Source: 10.0.0.0/16, Access: Read Only
Entry 2: Source: 10.0.0.8, Access: Read/Write

In this case, clients who connect to the export from IP address 10.0.0.8 have Read Only access. The request Source IP address is contained in the CIDR block specified in the first entry, and File Storage Service applies the options in the first match.

**Important:** File systems can be associated with one or more exports, contained within one or more mount targets. If the client source IP address does not match any entry on the list for a single export, then that export is not visible to the client. However, the file system could be accessed through other exports on the same or other mount targets. To completely deny client access to a file system, be sure that the client source IP address or CIDR block is not included in any export for any mount target associated with the file system.

The following options can be set to control export access:

- **Source**: The IP address or CIDR block of a connecting NFS client.
- **Require Privileged Source Port (true/false)**: This setting determines whether the NFS clients specified in source are required to connect from a privileged source port. Privileged ports are any port including 1-1023. On Unix-like systems, only the root user can open privileged ports. Setting this value to true disallows requests from unprivileged ports. The default for this setting is different depending on how the export is created. Creating an export without an explicit ClientOption array sets the requirePrivilegedSourcePort attribute of the client option to false. When you create a ClientOption array explicitly, requirePrivilegedSourcePort defaults to true.

For example, creating an export in the Console using the default selections sets requirePrivilegedSourcePort to false. Creating an export in the API along with a ClientOption array sets requirePrivilegedSourcePort to true.
Important:

When **Require Privileged Source Port** is set to **true**, you also have to follow these additional configuration steps:

1. When mounting the file system from a Unix-like system, include the `resvport` option in your mount command when mounting. For example:

   ```
   sudo mount -o resvport 10.x.x.x:/fs-export-path /mnt/yourmountpoint
   ```

   For more information, see [Mounting File Systems From Unix-Style Instances](#) on page 1957.

2. When mounting the file system from a Windows system, be sure the `UseReserverdPort` registry key value is set to **1**.

   For more information, see [Mounting File Systems From Windows Instances](#) on page 1964.

- **Access (Read Only, Read_Write):** This setting specifies the source NFS client access. If unspecified, defaults to **Read_Write**.
- **Identity Squash: (All, Root, None):** This setting determines whether the source clients accessing the file system have their User ID (UID) and Group ID (GID) remapped to `anonymousUid` and `anonymousGid`. If you choose **All**, all users and groups are remapped. If **Root**, only the root user UID/GID combination 0/0 is remapped. If **None**, no users are remapped. If unspecified, defaults to **None**.
- **anonymousUid:** This setting is used along with the **Identity Squash** option. When remapping users, you can use this setting to change the default `anonymousUid` of **65534** to any user ID of your choice.
- **anonymousGid:** This setting is used along with the **Identity Squash** option. When remapping groups, you can use this setting to change the default `anonymousGid` of **65534** to any group ID of your choice.

**Typical Access Control Scenarios**

When you create file system and export, the NFS export options for that file system are set to the following defaults, which allow full access for all NFS client source connections. These defaults must be changed if you want to restrict access:

- **Source:** 0.0.0.0/0 (All)
- **Require Privileged Source Port:** False
- **Access:** Read_Write
- **Identity Squash:** None

**Scenario A: Control Host Based Access**

Provide a managed hosted environment for two clients. The clients share a mount target, but each has their own file system, and cannot access each other's data. For example:

- Client A, who is assigned to CIDR block 10.0.0.0/24, requires Read/Write access to file system A, but not file system B.
- Client B, who is assigned to CIDR block 10.1.1.0/24, requires Read/Write access to file system B, but not file system A.
- Client C, who is assigned to CIDR block 10.2.2.0/24, has no access of any kind to file system A or file system B.
- Both file systems A and B are associated to a single mount target, MT1. Each file system has an export contained in the export set of MT1.

Since Client A and Client B access the mount target from different CIDR blocks, you can set the client options for both file system exports to allow access to only a single CIDR block. Client C is denied access by not including its IP address or CIDR block in the NFS export options for any export of either file system.
**Console Example**

Set the export options for file system A to allow Read/Write access only to Client A, who is assigned to CIDR block 10.0.0.0/24. Client B and Client C are not included in this CIDR block, and cannot access the file system.

![Edit Export Options](image)

Set the export options for file system B to allow Read/Write access only to Client B, who is assigned to CIDR block 10.1.1.0/24. Client A and Client C are not included in this CIDR block, and cannot access the file system.

![Edit Export Options](image)

**CLI Example**

Set the export options for file system A to allow Read_Write access only to Client A, who is assigned to CIDR block 10.0.0.0/24. Client B and Client C are not included in this CIDR block, and cannot access the file system.

```
oci fs export update --export-id <File_system_A_export_ID> --export-options '[["source":"10.0.0.0/24","require-privileged-source-port":"true","access":"READ_WRITE","identity-squash":"NONE","anonymous-uid":"65534","anonymous-gid":"65534"]]
```

Set the export options for file system B to allow Read_Write access only to Client B, who is assigned to CIDR block 10.1.1.0/24. Client A and Client C are not included in this CIDR block, and cannot access the file system.

```
oci fs export update --export-id <File_system_B_export_ID> --export-options '[["source":"10.1.1.0/24 ","require-privileged-source-port":"true","access":"READ_WRITE","identity-squash":"NONE","anonymous-uid":"65534","anonymous-gid":"65534"]]
```

**API Example**

Set the export options for file system A to allow READ_WRITE access only to Client A, who is assigned to CIDR block 10.0.0.0/24. Client B and Client C are not included in this CIDR block, and cannot access the file system.

```
PUT/<Current_API_Version>/exports/<File_System_A_export_OCID>
Host: filestorage.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{"exportOptions": [
]}
```
Set the export options for file system B to allow READ_WRITE access only to Client B, who is assigned to CIDR block 10.1.1.0/24. Client A and Client C are not included in this CIDR block, and cannot access the file system.

```json
{
    "source": "10.1.1.0/24",
    "requirePrivilegedSourcePort": true,
    "access": "READ_WRITE",
    "identitySquash": "NONE",
    "anonymousUid": 65534,
    "anonymousGid": 65534
}
}
```

**Scenario B: Limit the Ability to Write Data**

Provide data to customers for consumption, but don't allow them to update the data.

For example, you'd like to publish a set of resources in file system A for an application to consume, but not change. The application connects from IP address 10.0.0.8.

**Console Example**

Set the source IP address 10.0.0.8 to Read Only in the export for file system A:

```bash
oci fs export update --export-id <File_System_A_export OCID> --export-options '{"source":"10.0.0.8","require-privileged-source-port":"true","access":"READ_ONLY","identitysquash":"NONE","anonymousuid":65534,"anonymousgid":65534}
```

**CLI Example**

Set the source IP address 10.0.0.8 to READ_ONLY in the export for file system A:
**API Example**

Set the source IP address 10.0.0.8 to READ_ONLY in the export for file system A:

```plaintext
PUT/<Current_API_Version>/exports/<File_System_A_export_OCID>
Host: filestorage.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
   "exportOptions": [
   {
      "source": "10.0.0.8",
      "requirePrivilegedSourcePort": true,
      "access": "READ_ONLY",
      "identitySquash": "NONE",
      "anonymousUid": 65534,
      "anonymousGid": 65534
   }
   ]
}
```

**Scenario C: Improve File System Security**

To increase security, you'd like to limit the root user's privileges when connecting to File System A. Use Identity Squash to remap root users to UID/GID 65534. In Unix-like systems, this UID/GID combination is reserved for 'nobody', a user with no system privileges.

**Console Example**

```
```

**CLI Example**

```
oci fs export update --export-id <File_System_A_export_OCID> --export-options '[]{"source": "0.0.0.0/0","require-privileged-source-port": "true","access": "READ_WRITE","identitysquash": "ROOT","anonymousuid": "65534","anonymousgid": "65534"}]
```

**API Example**

```
PUT/<Current_API_Version>/exports/<File_System_A_export_OCID>
Host: filestorage.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
   "exportOptions": [
   {
      "source": "0.0.0.0/0",
      "requirePrivilegedSourcePort": true,
      "access": "READ_WRITE",
      "identitySquash": "ROOT",
      "anonymousUid": 65534,
      "anonymousGid": 65534
   }
   ]
}
```
File Storage

Tip:

If you don't want a file system to be visible to any clients, you can set all of the properties in the `exportOptions` array to empty values. For example,

```
{
    "exportOptions": [
        {
            "source": "",
            "requirePrivilegedSourcePort": "",
            "access": "",
            "identitySquash": ""
        }
    ]
```

Using the Console

To set export options for a file system

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the List Scope section, select a compartment. All of the file systems in the selected compartment are displayed.
3. Find the file system you want to set export options for, click the Actions icon (three dots), and then click View File System Details.
4. In the Exports list, find the export you want to set export options in, click the Actions icon (three dots), and then click View Export Details. If there is no export listed for the file system, you can create one. See To create an export for a file system on page 1972 for more information.

Tip:

To be sure you be sure that you select the correct export, check the following:

- **The export path**: This path uniquely identifies the file system within the mount target. No two exports in a mount target can have the same export path, even if the exports are for the same file system.
- **The mount target name**: File systems can be exported through more than one mount target. Be sure that you've selected the export for the correct mount target.

5. Click Edit Export Options.
6. Make one or more of these changes:
   - Change an export option entry in the list.
   - Click +Another Option to create a new export option entry.
   - Click the Actions icon (three dots) for an entry and move it up or down in the list.
7. When you're done, click Update.

Using the CLI

For information about using the CLI, see Command Line Interface (CLI) on page 4192.

To create an export

Open a command prompt and run `oci fs export create` to create an export for a specified file system within a specified export set. This example creates an export along with its NFS export options.

For example:

```
oci fs export create --export-set-id <export_set_OCID> --file-system-id <file_system_OCID> --path "</pathname>" --export-options '{"source":"10.0.0.0/16","requireprivilegedsourceport":"true","access":"READWRITE","identitysquash":null,"access":null,"identitysquash":null}'
```
Important:

Export Path Names

The path must start with a slash (/) followed by a sequence of zero or more
slash-separated elements. For any two export resources associated with the
same export set, the path sequence for the first export resource can’t contain
the complete path element sequence of the second export sequence. Paths
can’t end in a slash. No path element can be a period (.) or two periods in
sequence (...). Lastly, no path can exceed 255 bytes.

Examples:

Acceptable:

/example and /path
/example1 and /example2

Not Acceptable:

/example and /example/path
/ and /example
/example/
/example/path/.. /example1

To update export options

Open a command prompt and run `oci fs export update` to update export options for a specified file system, use `--export-options`.

For example:

```
oci fs export update --export-id <export_OCID> --export-options '[["source":"<0.0.0.0/0>"],"require-privileged-source-port":"true","require-privileged-source-port":"true","access":"READ_ONLY","identity-squash":"ROOT","anonymous-uid":"65534","anonymous-gid":"65534"]'
```

WARNING: Updates to export-options will replace any existing values. Are you sure you want to continue? [y/N]: y

Tip:

If you don’t want a file system to be visible to any clients, you can set all of
the properties in Client Options to empty values. For example,

```
oci fs export update --export-id <export_OCID> --export-options '[["source":"","require-privileged-source-port":"true","require-privileged-source-port":"true","access":"READ_ONLY","identity-squash":"ROOT","anonymous-uid":"65534","anonymous-gid":"65534"]]
```

To list exports

Open a command prompt and run `oci fs export list` to list all exports in a specified compartment.

For example:

```
oci fs export list --compartment-id <target_compartment_id>
```
To delete an export

Open a command prompt and run `oci fs export delete` to delete an export.

For example:

```
oci fs export delete --export-id <export_OCID>
```

Caution:
When you delete an export, you can no longer mount the file system using the file path specified in the deleted export.

Using the API

- CreateExport
- UpdateExport
- ListExports
- GetExport
- DeleteExport

Using In-transit Encryption

In-transit encryption provides a way to secure your data between instances and mounted file systems using TLS v.1.2 (Transport Layer Security) encryption. Together with other methods of security such as Oracle Cloud Infrastructure Vault (KMS) and File Storage's encryption-at-rest, in-transit encryption provides for end-to-end security.

- For general information about getting started with file systems, see Overview of File Storage on page 1920.
- For more information on the Vault service, see Overview of Vault on page 3952.
- For more information on securing your file system, see About Security on page 1925 and the Securing File Storage on page 3687 reference in the Security Guide.

How In-transit Encryption is Enabled

In-transit encryption doesn't require any updates to your file system's mount target or export configuration. To enable in-transit encryption, you install a package called `oci-fss-utils` on your instance. The `oci-fss-utils` package creates a network namespace and virtual network interface on your instance and provides a local NFS endpoint. The `oci-fss-utils` package also runs a forwarder process in the background called `oci-fss-forwarder`.

The network namespace isolates the forwarder process from your instance's networking environment. The virtual network interface provides the forwarder process a unique IP address. The local NFS endpoint provides NFS connection capability.

The file system is mounted using a special command that initiates encryption. After the file system is mounted, the `oci-fss-forwarder` process connects the local NFS client to the NFS endpoint. The process then receives requests from the NFS client, encrypts them and sends them to the mount target using a TLS tunnel.

Here are the general steps for setting up In-transit encryption:

1. Download the `oci-fss-utils` package. For instructions, see Task 1: Download the OCI-FSS-UTILS package on page 1943
2. Install the `oci-fss-utils` package on the instance. For instructions, see Task 2: Install the OCI-FSS-UTILS package on Oracle Linux or CentOS on page 1944
3. Use the in-transit encryption command to mount the file system. For instructions, see Task 3: Mount the file system with the encryption command on page 1944

Limitations and Considerations

- The in-transit encryption installation package is distributed as an RPM for Oracle Linux and CentOS and can be downloaded at cloud-infrastructure-file-storage-downloads.html
• You must install the `oci-fss-utils` package on every instance that requires encrypted access to a mount target.
• The number of encrypted NFS/TLS connections for a single mount target is limited to 64. This limitation is caused by TLS memory requirements. Unlike NFS connections, TLS connections do not share memory buffers. So, once a TLS connection has been established, the allocated memory stays dedicated to it.
• DNS hostnames are not supported for mounting encrypted file systems with `oci-fss-forwarder`. Use the mount target IP address to mount encrypted file systems.

**Setting up In-transit Encryption**

**Prerequisites**

• Add the following new rules to the security list for the mount target subnet. Alternatively, you can add the following rules to a Network Security Group (NSG) and then add the mount target to the NSG. For more information and instructions about adding security list rules for File Storage, see Configuring VCN Security Rules for File Storage on page 1927.
  - A stateful **ingress** rule allowing TCP traffic to a **Destination Port Range** of 2051.
  - A stateful **egress** rule allowing TCP traffic from a **Source Port Range** of 2051.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard (unencrypted) access to File Storage mount targets requires access to the following ports:</td>
</tr>
<tr>
<td>• Stateful ingress to TCP ports 111, 2048, 2049, and 2050.</td>
</tr>
<tr>
<td>• Stateful ingress to UDP ports 111 and 2048.</td>
</tr>
<tr>
<td>• Stateful egress from TCP ports 111, 2048, 2049, and 2050.</td>
</tr>
<tr>
<td>• Stateful egress from UDP port 111.</td>
</tr>
</tbody>
</table>

If you have previously set up rules for standard access, and you want to enforce encrypted access only, then you can disable the standard access ports.

---

Only the rules for TCP port 2051 are required for encrypted access.

**Setup Tasks**

**Task 1: Download the OCI-FSS-UTILS package**

Internet access is required to download the RPM installation package. If the destination instance doesn't have internet access, you can download the RPM to a staging instance on your network and then use the `scp` command to securely copy the RPM from the staging instance to the destination instance.

The `scp` command requires an SSH key pair to authenticate a remote user. If your instances are UNIX-style systems, you probably already have the `ssh-keygen` utility installed. To determine if it's installed, open a shell or terminal and type `ssh-keygen` on the command line. If it's not installed, you can obtain OpenSSH for UNIX from [http://www.openssh.com/portable.html](http://www.openssh.com/portable.html).

1. (Optional) Create a directory for the RPM installation package on the destination instance. For example:

   ```bash
   sudo mkdir -p /<rpm_directory_name>
   ```

2. Download the `oci-fss-utils` package from [cloud-infrastructure-file-storage-downloads.html](http://cloud-infrastructure-file-storage-downloads.html) to the directory on the destination instance or to a staging instance on your network.

   If you've downloaded the package directly to the destination instance, skip the next step and proceed directly to **Task 2: Install the OCI-FSS-UTILS package on Oracle Linux or CentOS** on page 1944.

   If you've downloaded the package to a staging instance, proceed to the next step in these instructions.
3. Open a terminal window on the staging instance, and use the `scp` command to securely copy the RPM from the staging instance to the destination instance. For example:

```
scp -i <private_key> <path_to_.rpm> <username>@<destination-public-ip-address>:/<rpm_directory_name>
```

After the RPM package is downloaded to the target instance, proceed to **Task 2: Install the OCI-FSS-UTILS package on Oracle Linux or CentOS** on page 1944.

**Task 2: Install the OCI-FSS-UTILS package on Oracle Linux or CentOS**

1. Open a terminal window on the destination instance.
2. Install the package using the following command:

```
sudo yum localinstall oci-fss-utils-<version>.rpm
```

The package creates a namespace called `ns1` in your instance, which contains a default network interface for ethernet traffic. A network interface pair is created for each mount target.

After the package has finished installing, proceed to **Task 3: Mount the file system with the encryption command** on page 1944.

**Task 3: Mount the file system with the encryption command**

1. Open a terminal window in your instance.
2. Create a mount point by typing the following, replacing `yourmountpoint` with the local directory from which you want to access your file system.

```
sudo mkdir -p /mnt/yourmountpoint
```

3. Mount the file system using the following command:

```
sudo mount -t oci-fss 10.x.x.x:/fs-export-path /mnt/yourmountpoint
```

Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target, `fs-export-path` with the export path you specified when associating the file system with the mount target, and `yourmountpoint`
with the path to the local mount point. The export path is the path to the file system (relative to the mount target IP address).

**Important:**

DNS hostnames are not currently supported for mounting file systems with the `mount -t oci-fss` command. You must use the mount target IP address.

Example output from the `mount -t oci-fss` command:

```
```

Each time you mount a file system using this command, a new `oci-fss` service is initiated with an incrementing sequence number between 2 and 255. For example, `oci-fss-2.service`, `oci-fss-3.service`, and so on.

**Tip:**

You can use the `resvport` option to restrict the client to using a specific reserved port. For example:

```
sudo mount -t oci-fss -o resvport=900 10.x.x.x:/fs-export-path /mnt/yourmountpoint
```

### Managing In-transit Encryption

**To auto-mount a file system**

Auto-mount ensures that a file system is automatically re-mounted on an instance if it is rebooted.

1. Open a terminal window on the instance. Mount the file system as described in.
2. Open the `/etc/fstab` file for editing:

   ```
cd /etc

vi fstab
```
   
3. Add the following line to the `fstab` file:

   ```
10.x.x.x:/fs-export-path /mnt/yourmountpoint oci-fss x-systemd.requires=oci-fss-init.service,defaults,nofail 0 0
```

Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target, `fs-export-path` with the export path you specified when associating the file system with the mount target, and `yourmountpoint` with the path to the local mount point.

**Tip:**

You can use the `resvport` option to restrict the client to using a specific reserved port. For example:

```
10.x.x.x:/fs-export-path /mnt/yourmountpoint oci-fss x-systemd.requires=oci-fss-init.service,defaults,nofail,resvport=900 0 0
```
To unmount a file system

When you unmount a file system, you must use another oci-fss-utils command to ensure that the associated local network namespace is removed:

1. Open a terminal window on the instance.
2. Use the following command to unmount the file system:

   ```
   sudo umount -t oci-fss /mnt/yourmountpoint
   ```

   Replace `yourmountpoint` with the path to the local mount point.

To uninstall the OCI-FSS-UTILS package

1. First, unmount all mounted file systems. For instructions, see To unmount a file system on page 1946.
2. Open a terminal window on the instance.
3. Type the following command to uninstall the oci-fss package:

   ```
   sudo yum remove oci-fss-utils
   ```

Troubleshooting

If you experience issues with in-transit encryption, try the following techniques:

Verify that you have all the security list rules set up correctly for the mount target subnet.

In-transit encryption requires the following security list rules:

- A stateful **ingress** rule allowing **TCP** traffic to a **Destination Port Range** of **2051**.
- A stateful **egress** rule allowing **TCP** traffic from a **Source Port Range** of **2051**.

For more information and instructions, see Security Rules on page 2833.

Verify that the oci-fss service is running for the mounted file system.

If it is not, restart the service.

To verify the service is running

When you mount a file system using the `mount.oci-fss` command, it creates a systemd-managed service called `oci-fss<sequence_number>.service`. `<sequence_number>` is an incrementing value between 2-255. An `oci-fss` service is created for every file system mounted using the command. The exact name of the service is displayed as output when the file system is mounted.

For example:

   ```
   ```

1. Open a terminal window on the instance.
2. Verify that the service is running using the following command:

   ```
   systemctl status oci-fss-<sequence_number>
   ```

To start the service

1. Open a terminal window on the instance.
2. Use the following command to start the service:

   ```
   systemctl start oci-fss-<sequence_number>
   ```
Verify that the namespace ns1 has been created and contains a network interface.

To verify the network namespace

1. Open a terminal window on the instance.
2. Use the following command to verify the namespace and see the network interface:

   ```bash
   sudo ip netns exec ns1 ip link list
   ```

   You should see output displaying all the ethernet devices within namespace ns1. For example:

   ```
   1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN mode DEFAULT group default qlen 1000
   default qdisc noop state DOWN mode DEFAULT group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   3: v-peer1@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DEFAULT group default qlen 1000
   link/ether be:5b:35:2d:e9:54 brd ff:ff:ff:ff:ff:ff link-netnsid 0
   ```

Verify that IP forwarding is running on the instance.

Installing oci-fss-utils automatically turns on IP forwarding. However, you may have other processes running on the instance that disable it.

To verify that IP forwarding is running on the instance

1. Open a terminal window on the instance.
2. Use the following command to view the status of IP forwarding:

   ```bash
   # sysctl net.ipv4.ip_forward
   net.ipv4.ip_forward = 1
   ```

   An output value of 1 means that IP forwarding is enabled. This value is read from the /proc/sys/net/ipv4/ip_forward file.

   If the output value is 0, then IP forwarding is not enabled for the instance. Enable IP forwarding by following the instructions in To enable IP forwarding on the instance on page 1947.

To enable IP forwarding on the instance

If IP forwarding is not currently enabled on the instance, you must enable it and make the change permanent.

1. Open a terminal window on the instance.
2. Type the following command to open the /etc/sysctl.conf file:

   ```bash
   sudo vi /etc/sysctl.conf
   ```

   3. Remove the # to uncomment this line: # net.ipv4.ip_forward=1. If the value is 0, change it to 1.
   4. Type :wq to save the file and exit the editor.

Use the tcpdump utility to analyze traffic between the oci-fss service and the NFS client.

To obtain information using TCPDUMP

1. Open a terminal window on the instance.
2. Type the following command:

   ```bash
   sudo ip netns exec ns1 tcpdump -i v-peer2 "port 2049"
   ```

Use the journalctl command to view any messages that may have been logged by systemd regarding the service.

To obtain information from the SYSTEMD journal

1. Open a terminal window on the instance.
2. Type the following command:

```
journalctl -f -u oci-fss-<version>
```

- `f` displays the most recent journal entries, and prints new entries as they are appended to the journal.
- `-u` specifies a specific `systemd` service unit. In this case, `oci-fss-<sequence_number>` is the specified unit. If no unit is specified, `journalctl` returns all `systemd` entries.

## Creating File Systems

You can create a shared file system in the cloud using the File Storage service. Network access to your file system is provided through a mount target. Exports control how NFS clients access file systems when they connect to a mount target. File systems must have at least one export in one mount target for any instance to mount and use the file system. When you use the console to create your first file system, the workflow also creates a mount target and export for it.

### Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users create, manage, and delete file systems on page 2148 allows users to create file systems. Since mount targets are network endpoints, users must also have "use" permissions for VNICs, private IPs, private DNS zones, and subnets to create or delete a mount target. See the Policy Reference on page 2167 for more information.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

### Prerequisites

Before you create a file system, you need:

- At least one Virtual Cloud Network (VCN) in a compartment. For more information, see VCNs and Subnets on page 2821.
- Correctly configured security rules for the file system mount target. Security rules can be created in the security list for the mount target subnet, or in a Network Security Group (NSG) that you add the mount target to. See Security Rules on page 2833 for information about how security rules work in Oracle Cloud Infrastructure. Use the instructions in Configuring VCN Security Rules for File Storage on page 1927 to set up security rules correctly for your file systems.

### Using the Console

#### To create a file system

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the left-hand navigation, in the List Scope section, under Compartment, select a compartment.
3. Click Create File System.

**Note:**

File systems are encrypted by default. You cannot turn off encryption.
4. You can choose to accept the system defaults, or change them by clicking **Edit Details**.

**File System Information:**

- **Name:** File Storage service creates a default name using "FileSystem-YYMMDD-HHMM". Optionally, change the default name for the file system. It doesn't have to be unique; an Oracle Cloud Identifier (OCID) uniquely identifies the file system. Avoid entering confidential information.

- **Availability domain:** The first availability domain selected in the left panel list is used as default.

- **Encryption:** File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. Optionally, you can encrypt the data in this file system using your own Vault encryption key.

**Note:**

Currently, only symmetric Advanced Encryption Standard (AES) keys are supported for file system encryption.

To use Vault for your encryption needs, select **Encrypt using customer-managed keys** check box. Then, select the **Vault compartment** and **Vault** that contain the master encryption key you want to use. Also select the **Master encryption key compartment** and **Master encryption key**. For more information about encryption, see **Overview of Vault** on page 3952.

**Caution:**

*Be sure to back up your vaults and keys.* Deleting a vault and key otherwise means losing the ability to decrypt any resource or data that the key was used to encrypt. For more information, see **Backing Up Vaults and Keys** on page 4003.

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

**Export Information**

Mount targets use exports to manage access to file systems. The path name uniquely identifies the file system within the mount target, and is used by an instance to mount the file system.

- **Export Path:** The File Storage service creates a default export path using the file system name. Optionally, replace the default export path name with a new path name, preceded by a forward slash (/). For example, /fss. This value specifies the mount path to the file system (relative to the mount target IP address or hostname). Avoid entering confidential information.

**Important:**

The export path must start with a slash (/) followed by a sequence of zero or more slash-separated elements. For multiple file systems associated with a single mount target, the export path sequence for the first file system cannot contain the complete path element sequence of the second file system export path sequence. Export paths cannot end in a slash. No export path element can be a period (.) or two periods in sequence (..). No export path can exceed 1024 bytes. Lastly, no export path element can exceed 255 bytes. For example:

Acceptable:

/example and /path
/example and /example2

Not Acceptable:

/example and /example/path
/ and /example
Caution:

If one file system associated to a mount target has '/' specified as an export path, you can't associate another file system with that mount target.

Note:

Export paths cannot be edited after the export is created. If you want to use a different export path, you must create a new export with the desired path. Optionally, you can then delete the export with the old path.

For more information, see Paths in File Systems on page 2006.

- **Use Secure Export Options**: Select to set the export options to require NFS clients to use a privileged port (1-1023) as its source port. This option enhances security because only a client with root privileges can use a privileged source port. After the export is created, you can edit the export options to adjust security. See Working with NFS Export Options on page 1934 for more information.

Caution:

Leaving the "Use Secure Export Options" setting disabled allows unprivileged users to read and modify any file or directory on the target file system.

- **Mount Target Information**:

File systems must be associated with a mount target to be mounted by an instance.

If you have one or more previously created mount targets in the availability domain, the File Storage service automatically chooses the most recently created mount target in the list. If you don't have a mount target in the selected availability domain, the File Storage service creates one using the following defaults.

- **Mount Target Name**: File Storage service creates a default mount target name using "Mount-YYYYMMDD-HHMM".
- **Compartment**: The compartment you're currently working in.
- **Virtual Cloud Network**: The first VCN listed in the current compartment is used as default.
- **Configure Network Security Groups**: Select this option to add this mount target to an NSG you've created. Choose an NSG from the list. Each mount target can belong to up to five (5) NSGs.

Important:

Rules for the NSG you select must be configured to allow traffic to the mount target's VNIC using specific protocols and ports. For more information, see Configuring VCN Security Rules for File Storage on page 1927.

- **Subnet**: The most recently created subnet listed in the selected availability domain is used as default. Subnets can be either AD-specific or regional (regional ones have "regional" after the name). For more information, see VCNs and Subnets on page 2821.

5. If you want to accept the defaults for the mount target, click Create. The file system is created with the information displayed. If you want to choose another mount target or change the default information, click the Edit Details link.
6. In the **Mount Target Information** section, specify details for the mount target that is associated with the file system:

- **Select an Existing Mount Target:** Choose this option if you want to associate the file system with a mount target you already created. Choose the **Mount Target** from the list. Click the **click here** link in the dialog box if you want to enable compartment selection for the mount target.

  **Tip:**

  If there aren't any mount targets in the current combination of availability domain and compartment, this option is disabled. You can:

  - Choose a different compartment.
  - Choose a different availability domain in the **File System Information** section.
  - Create a new mount target.

- **Create a New Mount Target:** Choose this option if you want to create a new mount target associated with this file system. By default, the mount target is created in your current compartment and you can use network resources in that compartment. Click the **click here** link in the dialog box if you want to enable compartment selection for the mount target, its VCN, or subnet resources.

  **Important:**

  The mount target is always in the same availability domain as the file system. While it is possible to access mount targets from any AD in a region, for optimal performance, your mount target and file system should be in the same availability domain as the Compute instances that access them. For more information, see **Regions and Availability Domains** on page 1923.

- **Create in Compartment:** Specify the compartment you want to create the mount target in.

- **New Mount Target Name:** Optionally, replace the default with a friendly name for the mount target. It doesn't have to be unique; an Oracle Cloud Identifier (OCID) uniquely identifies the mount target. Avoid entering confidential information.

  **Note:**

  The mount target name is different than the DNS hostname, which is specified in step 7.

- **Virtual Cloud Network Compartment:** The compartment containing the cloud network (VCN) in which to create the mount target.

- **Virtual Cloud Network:** Select the cloud network (VCN) where you want to create the new mount target.

- **Configure Network Security Groups:** Select this option to add this mount target to an NSG you've created. Choose an NSG from the list.

  **Important:**

  Rules for the NSG you select must be configured to allow traffic to the mount target's VNIC using specific protocols and ports. For more information, see **Configuring VCN Security Rules for File Storage** on page 1927.

- **Subnet Compartment:** Specify the compartment containing a subnet within the VCN to attach the mount target to.

- **Subnet:** Select a subnet to attach the mount target to. Subnets can be either AD-specific or regional (regional ones have "regional" after the name). For more information, see **VCNs and Subnets** on page 2821.

  **Caution:**

  Each mount target requires three internal IP addresses in the subnet to function. Do not use /30 or smaller subnets for mount target creation.
because they do not have sufficient available IP addresses. Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

7. Optionally, click **Show Advanced Options** to configure the mount target's advanced options.

- **IP Address:** You can specify an unused IP address in the subnet you selected for the mount target.
- **Hostname:** You can specify a hostname you want to assign to the mount target.

**Note:**
The File Storage service constructs a fully qualified domain name (FQDN) by combining the hostname with the FQDN of the subnet the mount target is located in.

For example,
myhostname.subnet123.dnslabel.oraclevcn.com.

Once created, the hostname may be changed in the mount target's Details page. See Managing Mount Targets on page 1980 for more information.

8. Click **Create**.

The File Storage service typically creates the file system and mount target within seconds. Next, mount the file system from an instance so that you can read and write directories and files in your file system. See Mounting File Systems on page 1954 for instructions about obtaining mount commands for your operating system type and mounting your file system.

### Using the command line interface (CLI)

For information about using the CLI, see Command Line Interface (CLI) on page 4192.

#### To create a file system

Open a command prompt and run `oci fs file-system create` to create a file system. For example:

```
oci fs file-system create --availability-domain <target_availability_domain> --display-name "<My File System>" --compartment-id <target_compartment_id>
```

Avoid entering confidential information.

The file system is created.

File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. Optionally, you can encrypt the data in this file system using your own Vault encryption key. For more information, see Overview of Vault on page 3952.

For example:

```
oci fs file-system create --availability-domain AAbC:US-ASHBURN-AD-1 --display-name "My File System" --compartment-id ocid1.compartment.oc1..<unique_id> --kms-key-id --kms-key-id ocid1.key.oc1.phx.<unique_id>
```

#### To create a file system that is encrypted with a Key Management Key

File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. Optionally, you can encrypt the data in this file system using your own Vault encryption key.
Note:
Currently, only symmetric Advanced Encryption Standard (AES) keys are supported for file system encryption.

For more information, see Overview of Vault on page 3952.

Caution:
Be sure to back up your vaults and keys. Deleting a vault and key otherwise means losing the ability to decrypt any resource or data that the key was used to encrypt. For more information, see Backing Up Vaults and Keys on page 4003.

Open a command prompt and run `oci fs file-system create` to create a file system that is encrypted with a key management key.

```
oci fs file-system create --availability-domain <target_availability_domain> --display-name "<My File System>" --compartment-id <target_compartment_id> --kms-key-id <target_key_id>
```

For example:

```
oci fs file-system create --availability-domain AAbC:US-ASHBURN-AD-1 --display-name "My File System" --compartment-id ocid1.compartment.oc1..<unique_id> --kms-key-id ocid1.key.oc1.iad.<unique_id>
```

To create a mount target
You can create a mount target for file systems in a specified compartment and subnet. A file system can only be associated with a mount target in the same availability domain.

Caution:
Each mount target requires three internal IP addresses in the subnet to function. Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses. Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.

Open a command prompt and run `oci fs mount-target create` to create a mount target.

For example:

```
oci fs mount-target create --availability-domain <target_availability_domain> --compartment-id <target_compartment_id> --subnet-id <subnet_OCID> --display-name "<My Mount Target>"
```

Avoid entering confidential information.

To create an export
An export is a file system together with the path that can be used to mount it. Each export resource belongs to one export set.

Open a command prompt and run `oci fs export create` to create an export for a specified file system within a specified export set.

For example:

```
oci fs export create --export-set-id <export_set_OCID> --file-system-id <file_system_OCID> --path "<pathname>"
```
Important:

The export path must start with a slash (/) followed by a sequence of zero or more slash-separated elements. For multiple file systems associated with a single mount target, the export path sequence for the first file system cannot contain the complete path element sequence of the second file system export path sequence. Export paths cannot end in a slash. No export path element can be a period (.) or two periods in sequence (..). No export path can exceed 1024 bytes. Lastly, no export path element can exceed 255 bytes. For example:

Acceptable:
/example and /path
/example and /example2

Not Acceptable:
/example and /example/path
/ and /example
/example/
/example/path/../../example1

Caution:

If one file system associated to a mount target has ‘/’ specified as an export path, you can't associate another file system with that mount target.

Note:

Export paths cannot be edited after the export is created. If you want to use a different export path, you must create a new export with the desired path. Optionally, you can then delete the export with the old path.

For more information, see Paths in File Systems on page 2006.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to create file systems:

- CreateFileSystem
- CreateMountTarget
- CreateExport

Mounting File Systems

Users of Unix-style operating systems and Windows Server 2012 R2 and later versions can connect to a file system and write files. Mount targets serve as file system network access points for file systems. After your mount target is assigned an IP address, you can use it together with the file system export path to mount the file system. On the instance from which you want to mount the file system, you need to install an NFS client. For Unix-style operating systems, you create a mount point. When you mount the file system, the mount point effectively represents the root directory of the File Storage file system, allowing you to write files to the file system from the instance. Windows operating systems use a drive letter assignment instead of a mount point to represent root access.
Prerequisites

- The file system must have at least one export in at least one mount target. When you create a new file system, an export for the file system is created at the same time. See Creating File Systems on page 1948 for more information.

Mounting File Systems From an Instance

Mounting File Systems From Unix-Style Instances on page 1957 (Including Oracle Linux DB instances)
Mounting File Systems From Windows Instances on page 1964

Obtaining Mount Command Samples

Mount command samples that include mount information for a specific mount target and file system are available in the Console. Samples are available for the following operating system images:

- Oracle Linux
- CentOS
- Debian
- Red Hat Linux
- Ubuntu

Here’s an example of the information contained in a mount command sample. The file system name is used to create directory names:

If you specified a hostname for the mount target, the sample uses the FQDN in the commands. If you didn't specify a hostname, the sample uses the mount target IP address. Using a FQDN to mount your file system is optional; even if you specified a hostname, you can edit the command to use the IP address instead. If you use an FQDN to mount the
file system, ensure that the the FQDN correctly resolves to the mount target's IP address. For more information, see DNS in Your Virtual Cloud Network on page 2910.

Mount command samples mount the file system at the file system root directory. Mount command samples don't include subdirectory information for the file system. If you want to mount a subdirectory of the file system, you must edit the sample to append the subdirectory path to the export path. For more information on mounting subdirectories in Linux-type instances, see To mount a file system subdirectory (Linux). For more information on mounting subdirectories in Windows instances, see To mount a file system subdirectory (Windows).

Caution:

When mounting file systems, the following mount option combination is not supported by the File Storage service:

- `soft` when the file system is mounted with the read/write mount option (`-o rw`). This combination can cause corruption of your data.

The following mount options or mount option combinations are not recommended for use with the File Storage service:

- `soft` when the file system is mounted with the read-only mount option (`-o ro`) and the `timeo` has been specified as less than 300 seconds. This combination can cause a profusion of I/O error responses.
- `rsize`, or `wsize`. These options cause issues with performance.

Note:

When mounting file systems, Network Lock Manager (NLM) is enabled for file locking by default. The default requires no specified mount option. Typical NFS workloads function normally using the default.

Some applications might require you to specify the `nolock` mount option. Refer to your application documentation for best practices regarding this mount option.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users create, manage, and delete file systems on page 2148 allows users to obtain mount commands.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Using the Console

To get mount command samples

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the List Scope section, select a compartment.
   
   The Console displays a list of file systems that have already been created in the compartment, if any.
3. Find the file system you want to mount, click the Actions icon (three dots), and then click View File System Details.
4. In Resources, click Exports.
5. Find the export in the mount target you want to use to mount the file system, click the Actions icon (three dots), and then click **Mount Commands**.

**Tip:**

To be sure that you select the correct export, check the following:

- **The export path:** This path uniquely identifies the file system within the mount target. **No two exports in a mount target can have the same export path, even if the exports are for the same file system.**
- **The mount target name:** File systems can be exported through more than one mount target. Be sure that you've selected the export for the correct mount target.

6. In **Image**, choose the image of the Compute instance you want to mount the file system to.
7. Click the **Copy** link to copy the commands.

Next, mount the file system from a **Unix-style** or **Windows** instance.

### Mounting File Systems From Unix-Style Instances

Users of Ubuntu and Linux operating systems can use the command line to connect to a file system and write files. **Mount targets** serve as network access points for file systems. After your mount target is assigned an IP address, you can use it together with the **export path** to mount the file system. On the instance from which you want to mount the file system, you need to install an NFS client and create a mount point. When you mount the file system, the mount point effectively represents the root directory of the File Storage file system, allowing you to write files to the file system from the instance. You can mount to any directory within the file system.

### Prerequisites

- The file system must have at least one export in at least one mount target. When you create a new file system, an export for the file system is created at the same time. See **Creating File Systems** on page 1948 for more information.
- Correctly configured security rules for the mount target. See **Security Rules** on page 2833 for information about how security rules work in Oracle Cloud Infrastructure. Use the instructions in **Configuring VCN Security Rules for File Storage** on page 1927 to set up security rules correctly for your file systems.

### Mounting File Systems

You can use the following instructions to construct your mount commands, or use the Console to get mount command samples that include all the information for a specific mount target and file system. For more information, see **Obtaining Mount Command Samples** on page 1955.

Mount command samples mount the file system at the file system root directory. Mount command samples don’t include subdirectory information for the file system. If you want to mount your Linux-type instance at a subdirectory of the file system, you must edit the sample to append the subdirectory path to the export path. For more information, see **To mount a file system subdirectory** on page 1963.

**Caution:**

When mounting file systems, the following mount option combination is **not supported** by the File Storage service:

- **soft** when the file system is mounted with the read/write mount option (\(-o\) **rw**). **This combination can cause corruption of your data.**

The following mount options or mount option combinations are **not recommended** for use with the File Storage service:

- **soft** when the file system is mounted with the read-only mount option (\(-o\) **ro**), and the **timeo** has been specified as less than 300 seconds. **This combination can cause a profusion of I/O error responses.**
- **rsize**, or **wsize**. **These options cause issues with performance.**
Note:

When mounting file systems, Network Lock Manager (NLM) is enabled for file locking by default. The default requires no specified mount option. Typical NFS workloads function normally using the default.

Some applications might require you to specify the `nolock` mount option. Refer to your application documentation for best practices regarding this mount option.

To mount a file system from Ubuntu or Debian

1. Open a command window. Then, get the NFS client by copying and pasting the Install Command from the Console or type the following:

   ```
sudo apt-get install nfs-common
   ```

2. Create a mount point by copying and pasting the Create Mount Point Command from the Console or type the following, replacing `yourmountpoint` with the local directory from which you want to access your file system.

   ```
sudo mkdir -p /mnt/yourmountpoint
   ```

3. Mount the file system by copying and pasting the Mount Command from the Console or type the following:

   ```
sudo mount -o nosuid,resvport 10.x.x.x:/fs-export-path /mnt/yourmountpoint
   ```

   - Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target.
   - Replace `fs-export-path` with the export path you specified when associating the file system with the mount target.
   - Replace `yourmountpoint` with the path to the local mount point.

   **Tip:**

   IP address and export path information is available in the Details page of the mount target associated with your file system. See To view details of a mount target on page 1984 for more information.

   **Caution:**

   Omitting the `-o nosuid` option may allow unprivileged users to escalate their permissions to ‘root’. The `nosuid` option disables set-user-identifier or set-group-identifier bits within the mounted system, which are rarely used.

   **Note:**

   The `-o resvport` option is required when the “Require Privileged Source Port” export option is used and otherwise optional. It causes the mounting filesystem to connect from a privileged source port (1-1023). See Working with NFS Export Options on page 1934 for more information.

4. View the file system.

   ```
df -h
   ```

5. Write a file to the file system by typing the following. Replace `yourmountpoint` with the path to the local mount point and `helloworld` with your file name.

   ```
sudo touch /mnt/yourmountpoint/helloworld
   ```
6. Verify that you can view the file by typing the following. Replace `yourmountpoint` with the path to the local mount point.

```bash
cd /mnt/yourmountpoint
ls
```

See [Mount Command Fails](page 2012) in [Troubleshooting Your File System](page 2010) on page 2010 for more information about common issues you may encounter.

**To mount a file system from Linux, Red Hat, or CentOS**

1. Open a command window. Then, get the NFS client by copying and pasting the **Install Command** from the Console or typing the following:

```bash
sudo yum install nfs-utils
```

2. Create a mount point by copying and pasting the **Create Mount Point Command** from the Console or type the following, replacing `yourmountpoint` with the local directory from which you want to access your file system.

```bash
sudo mkdir -p /mnt/yourmountpoint
```

3. Mount the file system by copying and pasting the **Mount Command** from the Console or type the following:

```bash
sudo mount -o nosuid,resvport 10.x.x.x:/fs-export-path /mnt/yourmountpoint
```

- Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target.
- Replace `fs-export-path` with the export path you specified when associating the file system with the mount target.
- Replace `yourmountpoint` with the path to the local mount point.

**Tip:**

IP address and export path information is available in the **Details** page of the mount target associated with your file system. See [To view details of a mount target](page 1984) on page 1984 for more information.

**Caution:**

Omitting the `-o nosuid` option may allow unprivileged users to escalate their permissions to 'root'. The `nosuid` option disables set-user-identifier or set-group-identifier bits within the mounted system, which are rarely used.

**Note:**

The `-o resvport` option is required when the “Require Privileged Source Port” export option is used and otherwise optional. It causes the mounting filesystem to connect from a privileged source port (1-1023). See [Working with NFS Export Options](page 1934) on page 1934 for more information.

4. View the file system.

```bash
df -h
```

5. Write a file to the file system by typing the following. Replace `yourmountpoint` with the path to the local mount point and `helloworld` with your file name.

```bash
sudo touch /mnt/yourmountpoint/helloworld
```
6. Verify that you can view the file by typing the following. Replace `yourmountpoint` with the path to the local mount point.

```
cd /mnt/yourmountpoint
ls
```

See Mount Command Fails on page 2012 in Troubleshooting Your File System on page 2010 for more information about common issues you may encounter. See if you want to mount a subdirectory of the file system.

To mount a file system from a Database VM instance

Database VM instances are built on Oracle Linux 6.8, unlike Oracle Linux Compute instances, which run on version 7.4. The NFS Utilities package is pre-installed on DB instances, but the Open Network Computing Remote Procedure Call (ONC RPC) rpcbind utility is disabled by default. Oracle Linux 6.8 does not have systemd, so DB instances are managed differently than OL compute instances. An Oracle DB instance comes with a set of iptables rules that excludes any non-database ports and need to be updated to allow mount target traffic.

1. SSH to the DB system.

```
ssh -i <private_key_path> opc@<db_system_ip_address>
```

2. Start the rpcbind service by typing the following:

```
sudo service rpcbind start
```

3. Use the chkconfig command to enable starting rpcbind service at system startup.

```
sudo chkconfig rpcbind on
```

4. Change the default configuration of iptables to include the mount target IP address and allow traffic by typing the following. Replace `10.x.x.x` with the local subnet address assigned to the mount target for the file system. Save the new iptables entries.

```
sudo iptables -A INPUT -p tcp -s 10.x.x.x -j ACCEPT
sudo iptables -A OUTPUT -p tcp -s 10.x.x.x -j ACCEPT
sudo service iptables save
```

5. Create a mount point by typing the following, replacing `yourmountpoint` with the local directory from which you want to access your file system.

```
sudo mkdir -p /mnt/yourmountpoint
```
6. Mount the file system by copying and pasting the **Mount Command** from the Console or type the following:

```bash
sudo mount -t nfs -o nosuid,resvport,tcp,vers=3 10.x.x.x:/fs-export-path /mnt/yourmountpoint
```

- Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target.
- Replace `fs-export-path` with the export path you specified when associating the file system with the mount target.
- Replace `yourmountpoint` with the path to the local mount point.

**Tip:**

IP address and export path information is available in the **Details** page of the mount target associated with your file system. See [*To view details of a mount target*](#) on page 1984 for more information.

**Caution:**

Omitting the `-o nosuid` option may allow unprivileged users to escalate their permissions to 'root'. The **nosuid** option disables set-user-identifier or set-group-identifier bits within the mounted system, which are rarely used.

**Note:**

The `-o resvport` option is required when the “Require Privileged Source Port” export option is used and otherwise optional. It causes the mounting filesystem to connect from a privileged source port (1-1023). See [*Working with NFS Export Options*](#) on page 1934 for more information.

See [*Mount Command Fails*](#) on page 2012 in [*Troubleshooting Your File System*](#) on page 2010 for more information about common issues you may encounter.

### To auto-mount a file system

Auto-mount ensures that a file system is automatically re-mounted on an instance if it is rebooted.

1. Open a command window. Then, mount the file system using the steps described in the previous section.
2. Type the following command to get the file system entry point:

```bash
sudo cat /etc/mtab |grep -i nfs
```

3. Copy the file system entry point, and open the `/etc/fstab` file:

```bash
cd /etc
vi fstab
```

4. Add the following line to the `fstab` file:

```bash
<file_system_ip_address>:<file_system_path_name><your_local_mount_point>
nfs defaults,nofail,nosuid,resvport 0 0
```

**Caution:**

Omitting the `-o nosuid` option may allow unprivileged users to escalate their permissions to 'root'. The **nosuid** option disables set-user-identifier
or set-group-identifier bits within the mounted system, which are rarely used.

**Important:**

Be sure to add the `nofail` option to each entry. This option ensures that an unavailable file system does not cause the instance reboot process to fail.

**Note:**

The `-o resvport` option is required when the “Require Privileged Source Port” export option is used and otherwise optional. It causes the mounting filesystem to connect from a privileged source port (1-1023). See *Working with NFS Export Options* on page 1934 for more information.

5. Save the `/etc/fstab` file.

See *Mount Command Fails* on page 2012 in *Troubleshooting Your File System* on page 2010 for more information about common issues you may encounter.

**Mounting File System Subdirectories**

If your file system has an existing directory structure, you can mount any file system subdirectory. The subdirectory becomes the effective root directory at the mount point of the instance, and excludes sibling directories.

For example, suppose "FileSystem1" has an export path of `/FileSystem1` and a directory structure like this:

```
(MountTarget1)
10.0.0.16: /FileSystem1
```

```
/rootdirectory
```

```
/directoryA
```

```
/FileA
```

```
/directoryB
```

```
/FileB
```

The file system is exported from "MountTarget1" which has an IP address of `10.0.0.16`.

The following command mounts `directoryA` to the instance mount point `/mnt/mymountpoint`:

```
sudo mount -o nosuid,resvport 10.0.0.16:/FileSystem1/rootdirectory/directoryA /mnt/mymountpoint
```
Neither directoryB or FileB would be accessible from the instance mount point.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mounting a subdirectory to limit access to sibling directories is not sufficient to secure your file system. For information on security methods, see About Security on page 1925.</td>
</tr>
</tbody>
</table>

To mount a file system subdirectory

1. Open a command window. Then, get the NFS client by copying and pasting the Install Command from the Console or typing the following:

   ```bash
   sudo yum install nfs-utils
   ```

2. Create a mount point by copying and pasting the Create Mount Point Command from the Console or type the following, replacing yourmountpoint with the local directory from which you want to access your file system.

   ```bash
   sudo mkdir -p /mnt/yourmountpoint
   ```

3. Mount the file system by copying and editing the Mount Command from the Console or type the following:

   ```bash
   sudo mount -o nosuid,resvport 10.x.x.x:/fs-export-path/directory-path /mnt/yourmountpoint
   ```

   - Replace 10.x.x.x: with the local subnet IP address assigned to your mount target.
   - Replace fs-export-path with the export path you specified when associating the file system with the mount target.
   - Replace directory-path with the path from the root directory to subdirectory you want to mount.
   - Replace yourmountpoint with the path to the local mount point.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and export path information is available in the Details page of the mount target associated with your file system. See To view details of a mount target on page 1984 for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omitting the -o nosuid option may allow unprivileged users to escalate their permissions to 'root'. The nosuid option disables set-user-identifier or set-group-identifier bits within the mounted system, which are rarely used.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The -o resvport option is required when the “Require Privileged Source Port” export option is used and otherwise optional. It causes the mounting filesystem to connect from a privileged source port (1-1023). See Working with NFS Export Options on page 1934 for more information.</td>
</tr>
</tbody>
</table>

4. View the file system.

   ```bash
   df -h
   ```

5. Write a file to the file system by typing the following. Replace yourmountpoint with the path to the local mount point and helloworld with your file name.

   ```bash
   sudo touch /mnt/yourmountpoint/helloworld
   ```
6. Verify that you can view the file by typing the following. Replace `yourmountpoint` with the path to the local mount point.

```
cd /mnt/yourmountpoint
ls
```

To unmount a file system

1. Open a terminal window on the instance.
2. Use the following command to unmount the file system:

```
sudo umount /mnt/yourmountpoint
```

Replace `yourmountpoint` with the path to the local mount point.

Writing to File Systems

When a file system is created, its root directory is owned by the root user. If you're connecting from an Oracle-provided Linux or CentOS instance, the default user is opc. If you're connecting from an Oracle-provided Ubuntu instance, the default user is ubuntu. These default users are not root users, so you can't initially write a file or directory to a new file system with these users. Depending on your security requirements, there are several ways to proceed:

- Connect as the root user. Then, create files or directories in the new file system.
- Connect as the root user. Then, change the ownership or permissions of the file system root directory to allow other users (such as opc or ubuntu) to write to the file system.
- Connect as the root user. Then, create subdirectories with ownership or permissions that allow other users to write to the subdirectory.

Learn more about updating file and directory ownership and permissions.

- Connect as the default user. Then, use the `sudo` command to write or to change permissions or ownership of files or directories. The `sudo` command temporarily provides a regular user with root user permissions. Here's an example of using the `sudo` command to write to the file system:

```
sudo touch /mnt/yourmountpoint/helloworld
```

Learn more about the `sudo` command.

For more information on accessing Oracle-provided instances, see Connecting to an Instance on page 733.

Mounting File Systems From Windows Instances

Users of Windows Server 2012 R2 and later versions can mount a file system on any available drive letter using the mount target IP address and the file system export path.

The Windows NFS client must be installed on the instance from which you want to mount the file system.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Windows NFS client may require a restart of your system.</td>
</tr>
</tbody>
</table>

Access to NFS file systems requires UNIX-style user and group identities, which are not the same as Windows user and group identities. To enable users to access NFS shared resources, Windows client for NFS accesses file systems anonymously, using AnonymousGid and AnonymousUid. On brand new file systems, write permissions are only granted to the root user. The AnonymousGid and AnonymousUid identity values must be configured to allow write access.
After you have installed the NFS client and correctly mapped user identities, you can mount the file system to any available drive letter using the command line or Map network drive. You can access your file system through the chosen drive letter to write files.

**Prerequisites**

- The file system must have at least one export in at least one mount target. When you create a new file system, an export for the file system is created at the same time. See [Creating File Systems](page 1948) for more information.
- Correctly configured security rules for the mount target. See [Security Rules](page 2833) for information about how security rules work in Oracle Cloud Infrastructure. Use the instructions in [Configuring VCN Security Rules for File Storage](page 1927) to set up security rules correctly for your file systems.

**Caution:**

- Updating the 'AnonymousGid' and 'AnonymousUid' values require registry changes to your system.

**Caution:**

- When mounting file systems, the following mount option combination is **not supported** by the File Storage service:
  - `soft` when the file system is mounted with the read/write mount option `-o rw`. **This combination can cause corruption of your data.**

**Caution:**

- The following mount options or mount option combinations are **not recommended** for use with the File Storage service:
  - `soft` when the file system is mounted with the read-only mount option `-o ro` and the `timeo` has been specified as less than 300 seconds.
    - **This combination can cause a profusion of I/O error responses.**
  - `rsize`, or `wsize`. These options cause issues with performance.

**Note:**

- When mounting file systems, Network Lock Manager (NLM) is enabled for file locking by default. The default requires no specified mount option. Typical NFS workloads function normally using the default.
- Some applications might require you to specify the `nolock` mount option. Refer to your application documentation for best practices regarding this mount option.

### Using Windows Command Prompt

**To mount a file system from Windows Server Command Prompt**

If you are using Oracle-provided Windows images, the NFS client is already installed, and the correct user identities are mapped. Skip to step 4.

1. **Open Windows PowerShell and run as Administrator:**
   
   a. Go to **Start** and click the **Windows PowerShell** icon.
   
   b. In Windows PowerShell, type the following to run as Administrator:

   ```bash
   Start-Process powershell -Verb runAs
   ```

   c. In the **User Account Control** window, click **Yes**. A new Administrator: PowerShell window opens. You can close the standard PowerShell window to avoid confusing them.

2. **In Administrator: PowerShell, get the NFS client by typing the following:**

   ```bash
   Install-WindowsFeature -Name NFS-Client
   ```
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default -Name AnonymousUid -Value 0
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default -Name AnonymousGid -Value 0
Stop-Service -Name NfsClnt
Restart-Service -Name NfsRdr
Start-Service -Name NfsClnt

**Important:**

If you've set export options for your file system to require clients to connect from a privileged source port (1-1023), then you must set the `UseReservedPorts` registry key to 1.

For example:

Set-ItemProperty HKLM:\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default -Name UseReservedPorts -Value 1

For more information, see [Working with NFS Export Options](#) on page 1934.

3. **Close** the Administrator: PowerShell window.

   Open a **standard Command Prompt Window**:

   a. Click **Start**, then click **Command Prompt**.

   **Important:**

   NFS file systems mounted as Administrator are not available to standard users.

4. In the standard Windows Command Line (CMD) window, mount the file system by typing the following. Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target, `fs-export-path` with the export path you specified when associating the file system with the mount target, and `X:` with the drive letter of any available drive you want to map the file system to.

   ```bash
   mount 10.x.x.x:/fs-export-path X:
   ```

   **Tip:**

   IP address and export path information is available in the **Details** page of the mount target associated with your file system. See [To view details of a mount target](#) on page 1984 for more information.

   **Important:**

   The export path is the path to the file system (relative to the mount target IP address or hostname). If you did not specify a path when you associated the file system and mount target, then "/" represents the full extent of the mount target. In that case, you must use a "!" when mounting the file system. For example: `mount 10.0.0.0://! X:

5. Write a file to the file system by typing the following. Replace `X:` with the drive letter you used in step 10 and `helloworld` with your file name.

   ```bash
   X:
   echo > helloworld.txt
   ```
6. Verify that you can view the file by typing the following.

```
  dir
```

See Troubleshooting Windows NFS Connections on page 2026 for more information about common issues you might encounter.

**Using Windows File Explorer**

To mount a file system from Windows Server File Explorer

If you are using Oracle-provided Windows images, the NFS client is already installed, and the correct user identities are mapped. Skip to step 9.

1. Open **Windows PowerShell** and run as **Administrator**:
   
   a. Go to **Start** and click the **Windows PowerShell** icon.
   
   b. In Windows PowerShell, type the following to run as Administrator:

   ```
   Start-Process powershell -Verb runAs
   ```
   
   c. In the **User Account Control** window, click **Yes**. A new Administrator: PowerShell window opens. You can close the standard PowerShell window to avoid confusing them.

2. In Administrator: PowerShell, get the NFS client by typing the following:

   ```
   Install-WindowsFeature -Name NFS-Client
   ```

3. If necessary, restart your system.

4. Open the registry editor (regedit) to map the AnonymousGid and AnonymousUid to the root user.

   **Caution:**
   
   User identity mapping requires changes to your system registry.

   a. Click **Windows Search**.
   
   b. Enter `regedit` in the **Search** field and press **Enter**.
   
   c. Click **Yes** to allow changes to your device.
   
   d. Click **HKEY_LOCAL_MACHINE**. Then, browse to: `Software\Microsoft\ClientForNFS\CurrentVersion\Default`.

5. Add a new DWORD32 registry entry for **AnonymousGid**:

   a. Click **Edit**, and select **New DWORD (32 bit) Value**.
   
   b. In the **Name** field, enter **AnonymousGid**. Leave the value at 0.
6. Repeat step 5 to add a second DWORD32 registry entry named `AnonymousUid` with a value of 0.

   ![Registry Editor](image)

   **Important:**

   If you’ve set export options for your file system to require clients to connect from a privileged source port (1-1023), then you must set the `UseReservedPorts` registry key to 1.

   For more information, see Working with NFS Export Options on page 1934.

7. Open Windows Command Line (CMD) and run as Administrator:

   a. Go to Start and scroll down to Apps.
   b. In the Windows System section, press Ctrl+Shift and click Command Prompt.

8. In the Windows Command Line (CMD) window, restart the NFS Client by typing the following:

   ```
   nfsadmin client stop
   nfsadmin client start
   ```

9. Open File Explorer and select This PC. In the Computer tab, select Map network drive.

10. Select the Drive letter that you want to assign to the file system.

11. In the Folder field, enter the following. Replace `10.x.x.x` with the local subnet IP address assigned to your mount target, and `fs-export-path` with the export path you specified when associating the file system with the mount target.

   ```
   \10.x.x.x\fs-export-path
   ```

   **Tip:**

   IP address and export path information is available in the Details page of the mount target associated with your file system. See To view details of a mount target on page 1984 for more information.

   **Important:**

   The export path is the path to the file system (relative to the mount target IP address or hostname). If you did not specify a path when you associated the file system and mount target, then "\" represents the full extent of the file system.
mount target. In that case, you must use a "!" when entering the file system folder path. For example: `\10.0.0.0\!`

12. Click the Finish button when complete.

See Troubleshooting Windows NFS Connections on page 2026 for more information about common issues you might encounter.

**Mounting File System Subdirectories**

If your file system has an existing directory structure, you can mount any file system subdirectory. The subdirectory becomes the effective root directory at the mount point of the instance, and excludes sibling directories.

For example, suppose "FileSystem1" has an export path of `/FileSystem1` and a directory structure like this:

![Diagram of file system structure]

The file system is exported from "MountTarget1" which has an IP address of 10.0.0.16.

The following command mounts `directoryA` to drive letter X:

```
mount 10.0.0.16:/rootdirectory/directoryA X:
```

Neither `directoryB` or `FileB` would be accessible from drive X.

**Caution:**

Mounting a subdirectory to limit access to sibling directories is not sufficient to secure your file system. For information on security methods, see About Security on page 1925.

To mount a file system subdirectory

1. Choose the method you want to use to mount the file system Using Windows Command Prompt on page 1965 or Using Windows File Explorer on page 1967.
2. Follow the instructions to install the NFS client and add the registry entries for AnonymousGid and AnonymousUid.

3. After the NFS client is installed and registry entries are added, both mounting methods describe how to enter the mount information for the file system. Depending on which method you use, edit the mounting information to append the subdirectory path to the export path:

   a. If you're Using Windows Command Prompt on page 1965, type the following command (step 4):
      - Replace 10.x.x.x: with the local subnet IP address assigned to your mount target.
      - Replace fs-export-path with the export path you specified when associating the file system with the mount target.
      - Replace directory-path with the path from the root directory to subdirectory you want to mount.

      
      ```
      mount 10.x.x.x:/fs-export-path/directory-path X:
      ```

   b. If you're Using Windows File Explorer on page 1967, enter the following in the Folder field of the drive letter you want to map the file system to (step 11):
      - Replace 10.x.x.x: with the local subnet IP address assigned to your mount target.
      - Replace fs-export-path with the export path you specified when associating the file system with the mount target.
      - Replace directory-path with the path from the root directory to subdirectory you want to mount.

      ```
      \10.x.x.x\fs-export-path\directory-path
      ```

Managing File Systems

In the File Storage service, file systems are associated with a single compartment. When you select a compartment, the Console displays all file systems in the compartment. You can also see exports and snapshots associated with each file system. If there are no file systems in the compartment, see Creating File Systems on page 1948 for instructions about creating one.

The compartment has policies that indicate what actions a user can take to manage file system. UNIX permissions control what actions a user can take on the files stored in the file system. See About Security on page 1925 for more information.

Actions you can take to manage a file system include:

- Viewing file system details
- Editing file system settings
- Viewing associated file system resources
- Creating an export for the file system
- Deleting a file system

You can perform most administrative tasks for your file systems using the Console, Command Line Interface (CLI), or API. You can use the Console to list mount targets exporting a specific file system. Use the API or CLI if you want to list all mount targets in a compartment.

To access a file system, it must have at least one export in one mount target. Next, mount the file system from an instance, and then you can create directories and read and write files. For more information about creating an export for a file system, see To create an export for a file system on page 1972 in this topic. For more information about accessing your file system, see Mounting File Systems.

Limitations and Considerations

- Each tenancy in a region can have 1 CreateFileSystem or ChangeFilesystemCompartment operation in progress at a time. See 409 error occurs when creating or moving a file system or mount target for more information.
Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users create, manage, and delete file systems on page 2148 allows users to manage file systems.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Moving File Systems to a Different Compartment

You can move file systems from one compartment to another. When you move a file system to a new compartment, its associated snapshots move with it. After you move the file system to the new compartment, inherent policies apply immediately and affect access to the file system and snapshots through the Console. Moving these resources doesn't affect access to file systems and snapshots from mounted instances. For more information, see Managing Compartments on page 2431.

Details About Your File System

The file system details page provides the following information about your file system:

FILE SYSTEM OCID

Every Oracle Cloud Infrastructure resource has an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). You need your file system's OCID to use the Command Line Interface (CLI) or the API. You also need the OCID when contacting support. See Resource Identifiers on page 197.

Availability Domain

When you create a file system, you specify the availability domain that it resides in. An availability domain is one or more data centers located within a region. You need your file system's availability domain to use the Command Line Interface (CLI) or the API. For more information, see Regions and Availability Domains on page 180.

CREATED

The date and time that the file system was created.

COMPARTMENT

When you create a file system, you specify the compartment that it resides in. A compartment is a collection of related resources (such as cloud networks, compute instances, or file systems) that are only accessible to those groups that have been given permission by an administrator in your organization. You need your file system's compartment to use the Command Line Interface (CLI) or the API. For more information, see Managing Compartments on page 2431.

UTILIZATION

Metered size of the file system that gets updated hourly. For more information, see File System Usage and Metering on page 2007.
RESOURCES

Resources such as exports and snapshots that are associated with the file system are listed here. Click the resource type link to see a list of each individual resource. Each export in the list shows the file system's export path and mount target. You need the export path to mount a file system.

Using the Console
To view file system details

The File Storage service displays a list of file systems in each compartment.

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the List Scope section, select a compartment.
3. To view information about a file system, find the file system, click the Actions icon (three dots), and then click View File System Details.

To change the file system name

You can change the display name of the file system.

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the List Scope section, select a compartment.
3. To view information about a file system, find the file system, click the Actions icon (three dots), and then click View File System Details.
4. Click Rename.
5. Enter the new file system name. Avoid entering confidential information. Then click Rename.

To create an export for a file system

Exports control how NFS clients access file systems when they connect to a mount target. File systems are exported (made available) through mount targets. Each mount target maintains an export set which contains one or many exports. A file system may be exported through one or more mount targets. A file system must have at least one export in one mount target in order for instances to mount the file system. The information used by an export includes the file system OCID, mount target OCID, export set OCID, export path, and client export options. Typically, an export is created in a mount target when the file system is created. Thereafter, you can create additional exports for a file system in any mount target that resides in the same availability domain as the file system.

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the left-hand navigation, in the List Scope section, under Compartment, select a compartment.
3. Click the name of the file system you want to create an export for, and click Create Export.

Note:

File systems are encrypted by default. You cannot turn off encryption.

4. You can choose to accept the system defaults, or change them by clicking Edit Details.
5. If you want to accept the defaults for the mount target, click Create. The file system is created with the information displayed. If you want to choose another mount target or change the default information, click the Edit Details link.
6. In the Mount Target Information section, specify details for the mount target that is associated with the file system:

   • Select an Existing Mount Target: Choose this option if you want to associate the file system with a mount target you already created. Choose the Mount Target from the list. Click the click here link in the dialog box if you want to enable compartment selection for the mount target.

Tip:

If there aren't any mount targets in the current combination of availability domain and compartment, this option is disabled. You can:

   • Choose a different compartment.
• Create a new mount target.

• **Create a New Mount Target:** Choose this option if you want to create a new mount target associated with this file system. By default, the mount target is created in your current compartment and you can use network resources in that compartment. Click the [click here](#) link in the dialog box if you want to enable compartment selection for the mount target, its VCN, or subnet resources.

  **Important:**

  The mount target is always in the same availability domain as the file system. While it is possible to access mount targets from any AD in a region, for optimal performance, your mount target and file system should be in the same availability domain as the Compute instances that access them. For more information, see [Regions and Availability Domains](#) on page 1923.

• **Create in Compartment:** Specify the compartment you want to create the mount target in.

• **New Mount Target Name:** Optionally, replace the default with a friendly name for the mount target. It doesn't have to be unique; an Oracle Cloud Identifier (OCID) uniquely identifies the mount target. Avoid entering confidential information.

  **Note:**

  The mount target name is different than the DNS hostname, which is specified in step 7.

• **Virtual Cloud Network Compartment:** The compartment containing the cloud network (VCN) in which to create the mount target.

• **Virtual Cloud Network:** Select the cloud network (VCN) where you want to create the new mount target.

• **Configure Network Security Groups:** Select this option to add this mount target to an NSG you've created. Choose an NSG from the list.

  **Important:**

  Rules for the NSG you select must be configured to allow traffic to the mount target's VNIC using specific protocols and ports. For more information, see [Configuring VCN Security Rules for File Storage](#) on page 1927.

• **Subnet Compartment:** Specify the compartment containing a subnet within the VCN to attach the mount target to.

• **Subnet:** Select a subnet to attach the mount target to. Subnets can be either AD-specific or regional (regional ones have "regional" after the name). For more information, see [VCNs and Subnets](#) on page 2821.

  **Caution:**

  Each mount target requires three internal IP addresses in the subnet to function. Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses. Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.

• **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Optionally, click **Show Advanced Options** to configure the mount target's advanced options.

   - **IP Address:** You can specify an unused IP address in the subnet you selected for the mount target.
   - **Hostname:** You can specify a hostname you want to assign to the mount target.

   **Note:**
   The File Storage service constructs a fully qualified domain name (FQDN) by combining the hostname with the FQDN of the subnet the mount target is located in.

   For example, myhostname.subnet123.dnslabel.oraclevcn.com.

   Once created, the hostname may be changed in the mount target's Details page. See **Managing Mount Targets** on page 1980 for more information.

8. Click **Create**.

Next, mount the file system from an instance so that you can read and write directories and files in your file system. See **Mounting File Systems** on page 1954 for instructions about obtaining mount commands for your operating system type and mounting your file system.

**To set the file system reported size**

The File Storage service reports file system capacity as 8589934592 gibibytes (GiB) and 8589934592 gibinodes (GiI) by default. Sometimes, application installers perform a space requirement check prior to running an installation process but cannot correctly interpret the reported size or reported inodes of the file system. When this occurs, you can define the file system size reported to the operating system by setting the **Reported Size** or **Reported Inodes** value in the file system's mount target. Typically, setting the size to 1024 GiB and the inodes to 1024 GiI permits successful installation.

   **Important:**
   Changing the **Reported Size** or **Reported Inodes** for a mount target affects all file systems exported by the mount target. Changing these values does not limit the amount of data you can store.

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. In the **List Scope** section, select a compartment.
3. Find the mount target you're interested in, click the Actions icon (three dots), and then click **View File System Details**.
4. In **Exports**, click on the mount target name.
5. Click the **Reported Size (in GiB) Edit** or the **Reported Inodes (in GiI)** icon.
6. Enter the maximum free space in gibibytes or the maximum inodes in gibinodes you want the File Storage service to report.
7. Click the **Save** icon.

   **Important:**
   There can be a delay of up to 1 hour when reporting file system usage, either in the console or by using the df command. For more information, see **File System Usage and Metering** on page 2007.

**To manage tags for a file system**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. In the **List Scope** section, select a compartment.
3. Find the file system you're interested in, click the Actions icon (three dots), and then click **View File System Details**.
4. Click the **Tags** tab to view or edit the existing tags. Or click **Apply tag(s)** to add new ones.
For more information, see Resource Tags on page 211.

**To move a file system to a different compartment**

1. Open the Console,
2. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
3. In the List Scope section, select a compartment.
4. Find the file system in the list, click the the Actions icon (three dots), and then click Change Compartment.
5. Choose the destination compartment from the list.
6. Click Change Compartment.

The file system is moved immediately. Moving a file system doesn't affect mounted instances.

**To move a file system to a different subnet**

There might be situations where you need to move a file system to a different subnet. For example, since you can't change subnet size, you might need to move the file system to a larger or smaller subnet as your needs change.

1. Create the new subnet. See VCNs and Subnets on page 2821 for instructions.
2. Create a new mount target in the new subnet. See To create a mount target on page 1983 for instructions.
3. Create new export with the same export path in the new mount target to the file system. See To create an export for a file system on page 1972 for instructions.
   - Choose Select Existing Mount Target
   - Be sure that the export path for the new export is exactly the same as the export path for the original export.
     The original and new mount target can exist at the same time without issue.
4. Switch over the instance mount point to the new mount target. This can be done at any time convenient to your maintenance schedule:
   a. Stop any workload application processes running on the instance mount point.
   b. Unmount the file system. See To unmount a file system on page 1964 for instructions.
   c. Mount the file system using the new mount target, but the same mount point that was previously used.
      For example: If the file system was mounted with the original mount target like this:
      ```
sudo mount 10.0.0.10:/my-export-path /mnt/MyMountPoint
      ```
      Then the new mount command would look like this:
      ```
sudo mount 10.1.1.10:/my-export-path /mnt/MyMountPoint
      ```
   d. Update any system configuration files that use the old export path. For example, /etc/fstab.
   e. Start workload applications and verify that they can access the file system as expected.
   f. After testing and verification is complete, you can delete the original mount target and subnet.

**To assign a key to a file system**

File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. Optionally, you can encrypt the data in this file system using your own Vault encryption key.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently, only symmetric Advanced Encryption Standard (AES) keys are supported for file system encryption.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be sure to back up your vaults and keys. Deleting a vault and key otherwise means losing the ability to decrypt any resource or data that the key was used for.</td>
</tr>
</tbody>
</table>

---

Oracle Cloud Infrastructure User Guide
File Storage

Prerequisites:

- At least one key vault and key in the Vault service. For more information, see Overview of Vault on page 3952.
- Correctly set permissions that allow the File Storage service to use keys. For example:

  ```bash
  Allow service FssOciProd to use keys in compartment <compartment_name>
  ```

For more information, see Common Policies on page 2142.

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. Under List Scope, in the Compartment list, choose the compartment that contains the file system that you want to encrypt with a Vault master encryption key.
3. From the list of file systems, click the file system name.
4. Next to Encryption Key, click Edit.
5. In Encryption Type, select Encrypt using customer-managed keys.
6. Choose the vault compartment, vault, key compartment, and key.
7. When you are finished, click Save Changes.

To specify Oracle-managed keys for a file system

File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. However, if you assign a Vault key to a file system, you can later return the file system to using Oracle-managed keys for encryption. For more information, see Overview of Vault on page 3952.

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. Under List Scope, in the Compartment list, choose the compartment that contains the file system that you want to encrypt with a Vault master encryption key.
3. From the list of file systems, click the file system name.
4. Next to Encryption Key, click Edit.
5. In Encryption Type, select Encrypt using Oracle-managed keys.
6. When you are finished, click Save Changes.

To delete a file system

You can permanently delete a file system.

Caution:

You cannot undo this operation. Any data in a file system is permanently deleted with the file system. Snapshots of the file system are permanently deleted with the file system. You cannot recover a deleted file system or its snapshots.

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the List Scope section, select a compartment.
3. Find the file system you want to delete.
4. Click the Actions icon (three dots), and then click View File System Details.
5. Delete all of the file system's exports:
   - In Exports, select the check box for all exports listed, and then click Delete.
6. When all of the exports are deleted, click Delete to delete the file system.

The file system is deleted immediately, along with all of its snapshots.

Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI) on page 4192.
To list file systems

Open a command prompt and run `oci fs file-system list` to list all the file systems in a specified availability domain and compartment.

For example:

```
oci fs file-system list --availability-domain <target_availability_domain> --compartment-id <target_compartment_id>
```

To get a specific file system

Open a command prompt and run `oci fs file-system get` to retrieve information about a specific file system.

For example:

```
oci fs file-system get --file-system-id <file_system_OCID>
```

To update a file system

Open a command prompt and run `oci fs file-system update` to update a specific file system's information.

For example:

```
oci fs file-system update --file-system-id <file_system_OCID> --display-name "<New File System Name>"
```

Avoid entering confidential information.

To create an export for a file system

Exports control how NFS clients access file systems when they connect to a mount target. File systems are exported (made available) through mount targets. Each mount target maintains an export set which contains one or many exports. A file system may be exported through one or more mount targets. A file system must have at least one export in one mount target in order for instances to mount the file system. The information used by an export includes the file system OCID, mount target OCID, export set OCID, export path, and client export options. Typically, an export is created in a mount target when the file system is created. Thereafter, you can create additional exports for a file system in any mount target that resides in the same availability domain as the file system.

Open a command prompt and run `oci fs export create` to create an export for a specified file system within a specified export set.

For example:

```
oci fs export create --export-set-id <export_set_OCID> --file-system-id <file_system_OCID> --path "</pathname>"
```

**Important:**

The export path must start with a slash (/) followed by a sequence of zero or more slash-separated elements. For multiple file systems associated with a single mount target, the export path sequence for the first file system cannot contain the complete path element sequence of the second file system export path sequence. Export paths cannot end in a slash. No export path element can be a period (.) or two periods in sequence (..). No export path can exceed 1024 bytes. Lastly, no export path element can exceed 255 bytes. For example:

Acceptable:

```
/example and /path
```

```
/example and /example2
```
For more information, see Paths in File Systems on page 2006.

**To set the file system reported free space**

Some existing application installers perform a capacity check before running an installation process. Sometimes an installation fails because of too much available capacity. The File Storage service currently reports 8 exabytes of available capacity by default for each file system.

Customers can define how much free capacity is reported as available to the operating system.

Open a command prompt and type in the following command:

```bash
oci fs export-set update --export-set-id <export_set_OCID> --max-fs-stat-bytes <number_of_bytes>
```

**Important:**

The maximum free space setting affects each export in the export set. Setting the maximum free space does not limit the amount of data you can store.

**To move a file system to a different compartment**

```bash
oci fs file-system change-file-system-compartment --file-system-id <file_system_OCID> --compartment-id <destination_compartment_OCID>
```

**To update the key for a file system**

File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. Optionally, you can encrypt the data in this file system using your own Vault encryption key.

**Note:**

Currently, only symmetric Advanced Encryption Standard (AES) keys are supported for file system encryption.

**Caution:**

Be sure to back up your vaults and keys. Deleting a vault and key otherwise means losing the ability to decrypt any resource or data that the key was used to encrypt. For more information, see Backing Up Vaults and Keys on page 4003.
Prerequisites:

- At least one key vault and key in the Vault service. For more information, see Overview of Vault on page 3952.
- Correctly set permissions that allow the File Storage service to use keys. For example:

  ```
  Allow service FssOclProd to use keys in compartment <compartment_name>
  ```

  For more information, see Common Policies on page 2142.

Open a command prompt and run `oci fs file-system update` to update the file system with a new key.

```
oci fs file-system update --file-system-id <file_system_OCID> --kms-key-id <target_key_id>
```

For example:

```
oci fs file-system update --file-system-id ocid1.filesystem.oc1.phx.<unique_id> --kms-key-id ocid1.key.oc1.phx.<unique_id>
```

To specify Oracle-managed keys for a file system

File systems use Oracle-managed keys by default, which leaves all encryption-related matters to Oracle. However, if you assign a Vault key to a file system, you can later return the file system to using Oracle-managed keys for encryption.

Open a command prompt and run `oci fs file-system update`. Leave the `--kms-key-id` value unspecified.

```
oci fs file-system update --file-system-id <file_system_OCID> --kms-key-id ""
```

For example:

```
oci fs file-system update --file-system-id ocid1.filesystem.oc1.phx.<unique_id> --kms-key-id ""
```

To delete a file system

You can delete a file system if no non-deleted export resources reference it. Deleting a file system also deletes all its snapshots.

Open a command prompt and run `oci fs file-system delete` to delete a file system.

For example:

```
oci fs file-system delete --file-system-id <file_system_OCID>
```

Caution:

You cannot undo this operation. Any data in a file system is permanently deleted with the file system. Snapshots of the file system are permanently deleted with the file system. You cannot recover a deleted file system or its snapshots.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage file systems:
Managing Mount Targets

This topic describes the basics of managing mount targets.

Overview

Actions you can take to manage a mount target include:

- Viewing mount target details
- Obtaining mount command samples
- Creating a new export and file system
- Editing exports and export options
- Change the reported size of exported file systems
- Deleting a mount target

You can perform most administrative tasks for your mount targets using the Console, Command Line Interface (CLI), or API. You can use the Console to list mount targets exporting a specific file system. Use the API or CLI if you want to list all mount targets in a compartment.

Mount Target

A mount target is an NFS endpoint that lives in a VCN subnet of your choice and provides network access for file systems. The mount target provides the IP address or DNS name that is used together with a unique export path to mount the file system. When you use the console to create your first file system, the workflow also creates a mount target and export for it.

You can reuse the same mount target to make as many file systems available on the network as you wish. To reuse the same mount target for multiple file systems, create an export in the mount target for each file system.

Exports

Exports control how NFS clients access file systems when they connect to a mount target. File systems are exported (made available) through mount targets. Each mount target maintains an export set which contains one or many exports. A file system may be exported through one or more mount targets. A file system must have at least one export in one mount target in order for instances to mount the file system. The information used by an export includes the file system OCID, mount target OCID, export set OCID, export path, and client export options. When you use the console to create your first file system, the workflow also creates a mount target and export for it. Thereafter:

- You can create as many exports in a mount target for different file systems as you wish.
- You can create as many exports in a mount target for a single file system as you wish.
- You can delete and re-create exports in a mount target as often as you need to.
- You can add export options to an export to control access to the file system.

NFS Export Options

NFS export options are a set of parameters within the export that specify the level of access granted to NFS clients when they connect to a mount target. An NFS export options entry within an export defines access for a single IP address or CIDR block range. You can have up to 100 options per export.

For more information, see Working with NFS Export Options on page 1934.
Limitations and Considerations

- Each availability domain is limited to two mount targets by default.
  See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.
- Each mount target can accept up to 100,000 NFS client connections. If you use in-transit encryption, each mount target can accept up to 64 NFS/SSL client connections. See Using In-transit Encryption on page 1942 for more information.
- Each tenancy in a region can have 1 CreateMountTarget or ChangeMountTargetCompartment operation in progress at a time. See 409 error occurs when creating or moving a file system or mount target for more information.
- Each mount target requires three internal IP addresses in the subnet to function:
  - Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.
  - The third IP address is used to create a new VNIC for the mount target during failover. The original primary IP address is retained.
  - The File Storage service doesn't "reserve" the third IP address required for high availability failover.
  - Use care to ensure that enough unallocated IP addresses remain available for your mount targets to use during failover.
  - Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses for mount target creation.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users create, manage, and delete file systems on page 2148 allows users to manage mount targets. Since mount targets are network endpoints, users must also have "use" permissions for VNICs, private IPs, private DNS zones, and subnets to create or delete a mount target. See the Policy Reference on page 2167 for more information.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Moving Mount Targets to a Different Compartment

You can move mount targets from one compartment to another. When you move a mount target to a new compartment, its associated export set and exports move with it. After you move the mount target to the new compartment, inherent policies apply immediately and affect access to the mount target, export set, and exports through the Console. Moving these resources doesn't affect access to file systems and snapshots from mounted instances. For more information, see Managing Compartments on page 2431.

Details About Your Mount Target

The mount target details page provides the following information about your mount target:
MOUNT TARGET OCID

Every Oracle Cloud Infrastructure resource has an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). You need your mount target's OCID to use the Command Line Interface (CLI) or the API. You also need the OCID when contacting support.

CREATED

The date and time that the mount target was created.

Availability Domain

When you create a mount target, you specify the availability domain that it resides in. An availability domain is one or more data centers located within a region. You need your mount target's availability domain to use the Command Line Interface (CLI) or the API. For more information, see Regions and Availability Domains on page 180.

COMPARTMENT

When you create a mount target, you specify the compartment that it resides in. A compartment is a collection of related resources (such as cloud networks, compute instances, or file systems) that are accessible only to those groups that have been given permission by an administrator in your organization. You need your mount target's compartment to use the Command Line Interface (CLI) or the API. For more information, see Managing Compartments on page 2431.

REPORTED SIZE (GIB)

The maximum capacity in gibibytes reported by the file systems exported through this mount target. The File Storage service currently reports 8589934592 gibibytes (GiB) of available capacity by default. If you are installing an application that requires a specific reported size, you can change the reported size. Typically, setting the size to 1024 GiB is sufficient for most applications. This value is updated hourly. See To set the file system reported size on page 1985 for more information.

REPORTED INODES (GII)

The maximum capacity in gibiinodes reported by the file systems exported through this mount target. The File Storage service currently reports gibiinodes (GiI) of available inodes by default. If you are installing an application that requires specific reported inodes, you can change the reported inodes. Typically, setting the inodes to 1024 GiI is sufficient for most applications. This value is updated hourly. See To set the file system reported size on page 1985 for more information.

NETWORK SECURITY GROUPS

The network security groups that the mount target belongs to. Each mount target can belong to up to five (5) NSGs. See To add a mount target to a network security group on page 1986 for more information.

VIRTUAL CLOUD NETWORK

The VCN that contains the subnet where the mount target VNIC resides.

SUBNET

The subnet within the VCN where the mount target VNIC resides. Subnets can be either AD-specific or regional (regional ones have "regional" after the name). For more information, see VCNs and Subnets on page 2821.

IP ADDRESS

The IP address that was assigned to the mount target when it was created. You need your mount target's IP address to mount associated file systems.

HOSTNAME

The hostname that was assigned to the mount target, if any. For more information about hostnames, see DNS in Your Virtual Cloud Network on page 2910.
**FULLY QUALIFIED DOMAIN NAME**

The hostname together with the subnet domain name. For more information, see DNS in Your Virtual Cloud Network on page 2910. If you specify a hostname, you can use the FQDN to mount the file system.

**EXPORT SET OCID**

The OCID of the mount target's export set resource. Each mount target has one export set, which contains all of the exports for the mount target. You need your mount target's export set OCID when you perform export-related tasks in the Command Line Interface (CLI) or the API.

**EXPORTS**

All of the mount target's exports are listed here. The export path and name of each file system is also listed. You need the export path to mount a file system.

**Using the Console**

**To create a mount target**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>While it is possible to access mount targets from any AD in a region, for optimal performance, your mount targets should be in the same availability domain as the Compute instances that access them. For more information, see Regions and Availability Domains on page 1923.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
2. In the List Scope section, select a compartment.
   The Console displays a list of mount targets that have already been created in the compartment, if any.
3. Click Create Mount Target.
4. Enter the required mount target information. Click the click here link in the dialog box if you want to enable compartment selection for the mount target, its VCN, or subnet resources:
   - **New Mount Target Name**: Optionally, replace the default with a friendly name for the mount target. It doesn't have to be unique; an Oracle Cloud Identifier (OCID) uniquely identifies the mount target. Avoid entering confidential information.
     
     | Note: |
     |---|
     | The mount target name is different than the DNS hostname, which is specified in step 5. |
   - **Virtual Cloud Network Compartment**: The compartment containing the cloud network (VCN) in which to create the mount target.
   - **Virtual Cloud Network**: Select the cloud network (VCN) where you want to create the new mount target.
   - **Configure Network Security Groups**: Select this option to add this mount target to an NSG you've created. Choose an NSG from the list.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules for the NSG you select must be configured to allow traffic to the mount target's VNIC using specific protocols and ports. For more</td>
</tr>
</tbody>
</table>
information, see Configuring VCN Security Rules for File Storage on page 1927.

- **Subnet Compartment**: Specify the compartment containing a subnet within the VCN to attach the mount target to.

- **Subnet**: Select a subnet to attach the mount target to. Subnets can be either AD-specific or regional (regional ones have "regional" after the name). For more information, see VCNs and Subnets on page 2821.

  **Caution:**
  
  Each mount target requires three internal IP addresses in the subnet to function. Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses. Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.

5. Optionally, click Show Advanced Options to configure the mount target's advanced options.

   - **IP Address**: You can specify an unused IP address in the subnet you selected for the mount target.
   
   - **Hostname**: You can specify a hostname you want to assign to the mount target.

       **Note:**
       
       The File Storage service constructs a fully qualified domain name (FQDN) by combining the hostname with the FQDN of the subnet the mount target is located in.

       For example, `myhostname.subnet123.dnslabel.oraclevcn.com`.

       Once created, the hostname may be changed in the mount target's Details page. See Managing Mount Targets on page 1980 for more information.

6. Click Create.

   **To view details of a mount target**

   1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
   2. In the List Scope section, select a compartment.

       The Console displays a list of mount targets that have already been created in the compartment, if any.

   3. Find the mount target you're interested in, click the Actions icon (three dots), and then click View Mount Target Details.

   **To change the mount target name**

   You can change the display name of the mount target.

       **Note:**
       
       Changing the display name doesn't affect mounting file systems exported through the mount target.

   1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
   2. In the List Scope section, select a compartment.
   3. To view information about a file system, find the file system, click the Actions icon (three dots), and then click View Mount Target Details.
   4. Click Rename.
   5. Enter the new mount target name. Avoid entering confidential information. Then click Rename.
**To create an export and a new file system**

Exports control how NFS clients access file systems when they connect to a mount target. File systems must have at least one export in at least one mount target in order for instances to mount the file system. The following steps create an export and a new file system. If you want to create an export for an existing file system, see **To create an export for a file system** on page 1972.

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **Mount Targets**.
2. In the left-hand navigation, in the **List Scope** section, under **Compartment**, select a compartment.
3. Click the name of the mount target you want to create an export for, and click **Create Export**.

   **Note:**
   File systems are encrypted by default. You cannot turn off encryption.

4. You can choose to accept the system defaults, or change them by clicking **Edit Details**.
5. Click **Create**.

Next, mount the file system from an instance so that you can read and write directories and files in your file system. See **Mounting File Systems** on page 1954 for instructions about obtaining mount commands for your operating system type and mounting your file system.

**To set the file system reported size**

The File Storage service reports file system capacity as 8589934592 gibibytes (GiB) and 8589934592 gibiinodes (GiI) by default. Sometimes, application installers perform a space requirement check prior to running an installation process but cannot correctly interpret the reported size or reported inodes of the file system. When this occurs, you can define the file system size reported to the operating system by setting the **Reported Size** or **Reported Inodes** value in the file system's mount target. Typically, setting the size to 1024 GiB and the inodes to 1024 GiI permits successful installation.

   **Important:**
   Changing the **Reported Size** or **Reported Inodes** for a mount target affects all file systems exported by the mount target. **Changing these values does not limit the amount of data you can store.**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **Mount Targets**.
2. In the **List Scope** section, select a compartment.
3. Find the mount target you're interested in, click the Actions icon (three dots), and then click **View Mount target Details**.
4. Click the **Reported Size (in GiB) Edit** or the **Reported Inodes (in GiI)** icon.
5. Enter the maximum size in gibibytes or the maximum inodes in gibiinodes you want the File Storage service to report.
6. Click the **Save** icon.

   **Important:**
   There can be a delay of up to 1 hour when reporting file system usage, either in the console or by using the `df` command. For more information, see **File System Usage and Metering** on page 2007.

**To delete an export**

**Note:**
Deleting an export does not impact the data stored in the associated file system. Deleting an export disconnects any instance that mounts the file system with the deleted export path. Mount targets that have no exports still count toward your service limit.

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **Mount Targets**.
2. In the List Scope section, select a compartment.
3. Find the mount target you're interested in, click the Actions icon (three dots), and then click View Mount target Details.
4. In Exports, find the export you want to delete.
5. Click the Actions icon (three dots), and then click Delete.

To manage tags for a mount target
1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
2. In the List Scope section, select a compartment.
3. Find the mount target you're interested in, click the Actions icon (three dots), and then click View Mount Target Details.
4. Click the Tags tab to view or edit the existing tags. Or click Apply tag(s) to add new ones.

For more information, see Resource Tags on page 211.

To move a mount target to a different compartment
1. Open the navigation menu, Under Core Infrastructure, click File Storage and then click Mount Targets.
2. In the List Scope section, select a compartment.
3. Find the mount target in the list, click the the Actions icon (three dots), and then click Change Compartment.
4. Choose the destination compartment from the list.
5. Click Change Compartment.

To add a mount target to a network security group
You can add the mount target to one or more Network Security Groups (NSGs). File storage requires specific rules to be configured for NSGs that are associated with mount targets. For more information, see Configuring VCN Security Rules for File Storage on page 1927.
1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
2. In the List Scope section, select a compartment.
3. Find the mount target you're interested in, click the Actions icon (three dots), and then click View Mount Target Details.
4. In the Mount Target Information tab, click the Edit link next to Network Security Groups.
5. Select a Compartment and NSG from the list.
6. Click Save.

To delete a mount target
1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
2. In the List Scope section, select a compartment.
3. Find the mount target you want to delete.
4. Click the Actions icon (three dots), and then click Delete.

Caution:
Deleting the mount target also deletes all of its exports of associated file systems. File systems are no longer available through the deleted mount target.

Deleting a mount target has no effect on file system data or file system snapshots.

Using the Command Line Interface (CLI)
For information about using the CLI, see Command Line Interface (CLI) on page 4192.
To create a mount target

You can create a mount target for file systems in a specified compartment and subnet. A file system can only be associated with a mount target in the same availability domain.

**Caution:**

Each mount target requires three internal IP addresses in the subnet to function. Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses. Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.

Open a command prompt and run `oci fs mount-target create` to create a mount target.

For example:

```
oci fs mount-target create --availability-domain <target_availability_domain> --compartment-id <target_compartment_id> --subnet-id <subnet_OCID> --display-name "<My Mount Target>"
```

Avoid entering confidential information.

You can create a mount target that is added to a network security group (NSG).

For example:

```
oci fs mount-target create --availability-domain <target_availability_domain> --compartment-id <target_compartment_id> --subnet-id <subnet_OCID> --display-name "<My Mount Target>" --nsg-ids ['"<nsg_OCID_1>", "<nsg_OCID_2>']
```

To update a mount target

Open a command prompt and run `oci fs mount-target update` to update a specific mount target's information or to add it to a network security group (NSG).

For example:

```
oci fs mount-target update --mount-target-id <mount_target_OCID> --display-name "<New Mount Target Name>" --nsg-ids ['"<nsg1_OCID>", "<nsg2_OCID>']
```

Avoid entering confidential information.

To delete a mount target

Open a command prompt and run `oci fs mount-target delete` to delete a mount target. Deleting a mount target also deletes the mount target's VNICs.

For example:

```
oci fs mount-target delete --mount-target-id <mount_target_OCID>
```

**Caution:**

Deleting a mount target can cause any clients that have mounted an associated file system to hang. Be sure to have all clients unmount the file systems before deleting the mount target.

To list mount targets

You cannot use the Console to list mount targets. Use the command line interface or the API from a host machine running a UNIX-style operating system.
Open a command prompt and run `oci fs mount-target list` to list all mount targets in a specified availability domain and compartment.

For example:

```
oci fs mount-target list --availability-domain <target_availability_domain> --compartment-id <target_compartment_OCID>
```

**To get a specific mount target**

Open a command prompt and run `oci fs mount-target get` to retrieve information about a specific mount target.

For example:

```
oci fs mount-target get --mount-target-id <mount_target_OCID>
```

**To create an export**

Exports control how NFS clients access file systems when they connect to a mount target. File systems are exported (made available) through mount targets. Each mount target maintains an export set which contains one or many exports. A file system may be exported through one or more mount targets. A file system must have at least one export in one mount target in order for instances to mount the file system. The information used by an export includes the file system OCID, mount target OCID, export set OCID, export path, and client export options. Typically, an export is created in a mount target when the file system is created. Thereafter, you can create additional exports for a file system in any mount target that resides in the same availability domain as the file system.

Open a command prompt and run `oci fs export create` to create an export for a specified file system within a specified export set.

For example:

```
oci fs export create --export-set-id <export_set_OCID> --file-system-id <file_system_OCID> --path "</pathname>"
```

**Important:**

The export path must start with a slash (/) followed by a sequence of zero or more slash-separated elements. For multiple file systems associated with a single mount target, the export path sequence for the first file system cannot contain the complete path element sequence of the second file system export path sequence. Export paths cannot end in a slash. No export path element can be a period (.) or two periods in sequence (..). No export path can exceed 1024 bytes. Lastly, no export path element can exceed 255 bytes. For example:

Acceptable:

```
/example and /path
/example and /example2
```

Not Acceptable:

```
/example and /example/path
/ and /example
/example/
/example/path/../example1
```
Caution:
If one file system associated to a mount target has '/' specified as an export path, you can't associate another file system with that mount target.

Note:
Export paths cannot be edited after the export is created. If you want to use a different export path, you must create a new export with the desired path. Optionally, you can then delete the export with the old path.

For more information, see Paths in File Systems on page 2006.

To list exports
Open a command prompt and run `oci fs export list` to list all exports in a specified compartment.
For example:

```
oci fs export list --compartment-id <target_compartment_id>
```

To get a specific export
Open a command prompt and run `oci fs export get` to retrieve information about a specific export.
For example:

```
oci fs export get --export-id <export_OCID>
```

To delete an export
Open a command prompt and run `oci fs export delete` to delete an export.
For example:

```
oci fs export delete --export-id <export_OCID>
```

Caution:
When you delete an export, any file system referenced by the export is no longer accessible through the associated mount target.

To list export sets
Open a command prompt and run `oci fs export-set list` to list all export sets in a specified availability domain and compartment.
For example:

```
oci fs export-set list --availability-domain <target_availability_domain> --compartment-id <target_compartment_OCID>
```

To get a specific export set
Open a command prompt and run `oci fs export-set get` to retrieve information about a specific export set.
For example:

```
oci fs export-set get --export-set-id <export_set_OCID>
```

To update an export set
Open a command prompt and run `oci fs export-set update` to update a specific export set's information.
For example:

```bash
oci fs export-set update --export-set-id <export_set_OCID> --display-name "<New Export Set Name>"
```

**To set the file system reported size**

The File Storage service reports file system capacity as 8589934592 gibibytes (GiB) and 8589934592 gibiliodes (GiI) by default. Sometimes, application installers perform a space requirement check prior to running an installation process but cannot correctly interpret the reported size or reported inodes of the file system. When this occurs, you can define the file system size reported to the operating system by setting the **Reported Size** or **Reported Inodes** value in the export set of the file system's mount target. Typically, setting the size to 1024 GiB and the inodes to 1024 GiI permits successful installation.

**Important:**

Changing the **Reported Size** or **Reported Inodes** for a mount target affects all file systems exported by the mount target. **Changing these values does not limit the amount of data you can store.**

**Important:**

There can be a delay of up to 1 hour when reporting file system usage, either in the console or by using the `df` command. For more information, see [File System Usage and Metering](#) on page 2007.

Open a command prompt and type in the following command:

```bash
oci fs export-set update --export-set-id <export_set_OCID> --max-fs-stat-bytes <number_of_bytes>
```

**To move a mount target to a different compartment**

```bash
oci fs mount-target change-mount-target-compartment --mount-target-id <mount_target_OCID> --compartment-id <destination_compartment_OCID>
```

**Using the API**

- CreateMountTarget
- UpdateMountTarget
- DeleteMountTarget
- GetMountTarget
- ListMountTargets
- ChangeMountTargetCompartment
- CreateExport
- DeleteExport
- GetExport
- ListExports
- UpdateExportSet
- GetExportSet
- ListExportSets

**Managing Snapshots**

The File Storage service supports snapshots for data protection of your file system. Snapshots are a consistent, point-in-time view of your file systems. Snapshots are copy-on-write, and scoped to the entire file system. The File Storage service encrypts all file system and snapshot data at rest. You can take as many snapshots as you need.
Data usage is metered against differentiated snapshot data. If nothing has changed within the file system since the last snapshot was taken, the new snapshot does not consume more storage. For more information, see File System Usage and Metering on page 2007.

Snapshots are accessible under the root directory of the file system at .snapshot/name. When you use an NFSv3 client to perform operations such as ls, du, or find on the snapshot directory, the service automatically exports the directory. The client uses nfs_d_automount() to detect and mount the directory. After the directory is detected and mounted the first time, the client mounts the directory automatically.

For data protection, you can use a tool that supports NFSv3 to copy your data to a different availability domain, region, file system, object storage, or remote location.

For best performance, we recommend that you use the parallel tar (partar) and parallel copy (parcp) tools provided in the File Storage Parallel File Toolkit for this purpose. These tools work best with parallel workloads and requests. The Parallel File Toolkit is available for Oracle Linux, Red Hat Enterprise Linux, and CentOS. You can use rsync or regular tar for other operating system types. See Installing the Parallel File Tools on page 1994 for more information.

Tip: Watch a video about protecting data with snapshots in File Storage.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let users create, manage, and delete file systems on page 2148 allows users to create and delete snapshots.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Details About Your Snapshot

The Details page provides the following information about your snapshot:

SNAPSHOT OCID

Every Oracle Cloud Infrastructure resource has an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). You need your snapshot's OCID to use the Command Line Interface (CLI) or the API. You also need the OCID when contacting support. See Resource Identifiers on page 197.

CREATED

The date and time that the snapshot was created.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Using the Console

To create a snapshot

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. In the List Scope section, select a compartment.
3. In the File Systems list, locate the file system you want to take a snapshot of. Click the Actions icon (three dots), and then click View File System Details.
4. In Resources, click Snapshots.
5. Click **Create Snapshot**.
6. Fill out the required information:
   - **Name**: Enter a name for the snapshot. It must be unique among all other snapshots for this file system. The name can't be changed. Avoid entering confidential information.
7. Click **Create Snapshot**. The snapshot is accessible under the root directory of the file system at `.snapshot/name`.

**To view details of a snapshot**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. In the **List Scope** section, select a compartment.
3. In the **File Systems** list, locate the file system you took the snapshot of. Click the Actions icon (three dots), and then click **View File System Details**.
4. In **Resources**, click **Snapshots**.
5. In the **Snapshots** list, locate the snapshot you're interested in. Click the Actions icon (three dots), and then click **View Snapshot Details**.

**To create a snapshot from a Unix-style instance**

You can create a snapshot from an instance that you've mounted the file system to. Snapshots are created under the root folder of your file system, in a hidden directory named `.snapshot`.

1. Connect to your instance and open a command window.
2. Navigate to your file system's hidden `.snapshot` directory. Type the following, replacing `yourmountpoint` with the name of the directory where you mounted the file system.

   ```shell
cd /mnt/yourmountpoint/.snapshot
   mkdir snapshot-Jan1
   ls
   ```

**To restore a snapshot**

Snapshots are created under the root folder of your file system, in a hidden directory named `.snapshot`.

You can restore a file within the snapshot, or an entire snapshot using the `cp` command. Use the `-r` option when restoring a snapshot that contains subdirectories.

For example:

```shell
cp -r .snapshot/snapshot_name/* destination_directory_name
```

Optionally, you can use `rsync`, `tar`, or another tool that supports NFSv3 to copy your data to another remote location. For optimal performance, use the **Parallel File Tools**.

For example:

```shell
parcp .snapshot/snapshot_name/* destination_directory_name
```

**To manage tags for a snapshot**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. In the **List Scope** section, select a compartment.
3. In the **File Systems** list, locate the file system you took the snapshot of. Click the Actions icon (three dots), and then click **View File System Details**.

4. In **Resources**, click **Snapshots**.

5. In the **Snapshots** list, locate the snapshot you're interested in. Click the Actions icon (three dots), and then click **View Snapshot Details**.

6. Click the **Tags** tab to view or edit the existing tags. Or click **Apply tag(s)** to add new ones.

For more information, see **Resource Tags** on page 211.

**To delete a snapshot**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. In the **List Scope** section, select a compartment.
3. Find the file system with the snapshot you want to delete.
4. Click the Actions icon (three dots), and then click **View File System Details**.
5. In **Resources**, click **Snapshots**.
6. Find the snapshot you want to delete.
7. Click **Delete**.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192.

**To create a snapshot**

You can create a snapshot of a file system. A snapshot is a point-in-time view of the file system. The snapshot is accessible at `.snapshot/name`.

Open a command prompt and run `oci fs snapshot create` to create a snapshot of a file system.

For example:

```
oci fs snapshot create --file-system-id <file_system_OCID> --name "<January1>"
```

Avoid entering confidential information.

**To list snapshots**

Open a command prompt and run `oci fs snapshot list` to list all snapshots associated with a specific file system.

For example:

```
oci fs snapshot list --file-system-id <file_system_OCID>
```

**To get a specific snapshot**

Open a command prompt and run `oci fs snapshot get` to retrieve information about a specific snapshot.

For example:

```
oci fs snapshot get --snapshot-id <snapshot_OCID>
```

**To delete a snapshot**

Open a command prompt and run `oci fs snapshot delete` to delete a snapshot.

For example:

```
oci fs snapshot delete --snapshot-id <snapshot_OCID>
```
Using the API

- CreateSnapshot
- ListSnapshots
- GetSnapshot
- DeleteSnapshot

If you have issues managing snapshots, see Troubleshooting Snapshot Management on page 2022.

Using File Storage Parallel Tools

The Parallel File Tools suite provides parallel versions of `tar`, `rm`, and `cp`. These tools can run requests on large file systems in parallel, maximizing performance for data protection operations.

The toolkit includes:

- `partar`: Use this command to create and extract tarballs in parallel.
- `parrm`: You can use this command to recursively remove a directory in parallel.
- `parcp`: Use this command to recursively copy a directory in parallel.

Installing the Parallel File Tools

The tool suite is distributed as an RPM for Oracle Linux, Red Hat Enterprise Linux, and CentOS.

To install Parallel File Tools on Linux

To install Parallel File Tools on an Oracle Linux instance:

1. Open a terminal window on the destination instance.
2. Type the following command:


```
sudo yum install -y fss-parallel-tools
```

To install Parallel File Tools on CentOS and Red Hat 6.x

To install Parallel File Tools on CentOS and Red Hat 6.x:

1. Open a terminal window on the destination instance.
2. Type the following command:


```
sudo wget http://yum.oracle.com/RPM-GPG-KEY-oracle-ol6 -O /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
sudo yum --enablerepo=ol6_developer install fss-parallel-tools
```

To install Parallel File Tools on CentOS and Red Hat 7.x

To install Parallel File Tools on CentOS and Red Hat 7.x:

1. Open a terminal window on the destination instance.
2. Type the following command:


```
sudo wget http://yum.oracle.com/RPM-GPG-KEY-oracle-ol7 -O /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
sudo yum --enablerepo=ol7_developer install fss-parallel-tools
```

Oracle Cloud Infrastructure User Guide
Using the Tools - Simple Examples

Here are some simple examples of how the different tools are commonly used in Oracle Cloud Infrastructure File Storage.

To copy all files and folders from one directory to another

In this example, parcp is used to copy the contents of one folder to another. The -P option is used to set the number of parallel threads you want to use.

$parcp -P 16 /source/folder /destination/folder

To create a .TAR archive of a directory

The following command will create a .tar archive of the contents of the specified directory, and store it as a tarball in the directory. In the example below, the name of the directory that is being used to create the tarball is example.

$partar pcf example.tar example -P 16

You can also create a tarball and send it to a different directory. In the example below, the directory being used to create the tarball is example. The tarball is being created in the /test directory.

$partar pcf example.tar example -P 16 -C /test

Using the Tools - Advanced Examples

Here are some examples of how the different tools are used in more advanced scenarios.

To copy selected files or folders into a .TAR archive and exclude others

You can specify which files and folders are included when you create a .tar archive using partar. Let's say you have a directory that looks like this:

```
[opc@example sourcedir]$ ls -l
total 180
-rw-r----.  1 opc opc          0 Apr 15 02:55 example2020-04-15_02-55-33_217107549.error
-rw-r----.  1 opc opc         10 Apr 15 03:18 example2020-04-15_02-55-33_217107549.log
-rw-rw-r--.  1 opc opc         12 Apr 15 03:18 example2020-04-15_03-18-13_267771997.error
-rw-rw-r--.  1 opc opc         10 Apr 15 03:18 example2020-04-15_03-18-13_267771997.log
-rwxr-xr-x.  1 opc opc         37 Nov 30  2017 File1.txt
-rwxr-xr-x.  1 opc opc         15 Dec  1  2017 File2.txt
-rwxr-xr-x.  1 opc opc         39 Nov 30  2017 File3.txt
-rwxr-xr-x.  1 opc opc         57 Dec  1  2017 File4.txt
```

The following command creates a .tar archive that:

- Excludes all .log and .error files.
- Names the .tar archive mytar
- Sends the .tar ball from /sourcedir to /mnt/destinationdir
• Extracts the .tar archive

```
[opc@example sourcedir]$ partar cf - mytar '*.log*' --exclude '*.err*' |
                partar xf - -C /mnt/destinationdir
```

Performing `ls -l` on `/mnt/destinationdir/mytar` shows that only the desired files have been copied.

```
[opc@example mytar]$ ls -l
total 148
-rwxr-xr-x.  1 opc opc         37 Nov 30 2017 File1.txt
-rwxr-xr-x.  1 opc opc         15 Dec  1  2017 File2.txt
-rwxr-xr-x.  1 opc opc         39 Nov 30 2017 File3.txt
-rwxr-xr-x.  1 opc opc         57 Dec  1  2017 File4.txt
```

**To copy selected files or folders from one directory to another**

You can specify which files and folders are included when you use `parcp` to copy from one directory to another. Let's say you have a directory that looks like this:

```
[opc@example sourcedir]$ ls -l
total 180
-rw-r-----.  1 opc opc          0 Apr 15 02:55 example2020-04-15_02-55-33_217107549.error
-rw-r-----.  1 opc opc         10 Apr 15 03:18 example2020-04-15_02-55-33_217107549.log
-rw-r-r--.  1 opc opc         12 Apr 15 03:18 example2020-04-15_03-18-13_267771997.error
-rw-r-r--.  1 opc opc         10 Apr 15 03:18 example2020-04-15_03-18-13_267771997.log
-rwxr-xr-x.  1 opc opc         37 Nov 30 2017 File1.txt
-rwxr-xr-x.  1 opc opc         15 Dec  1  2017 File2.txt
-rwxr-xr-x.  1 opc opc         39 Nov 30 2017 File3.txt
-rwxr-xr-x.  1 opc opc         57 Dec  1  2017 File4.txt
```

First, create a `.txt` file containing a list of files you want to exclude. In this example, it's `/home/opc/list.txt`.

The following command copies the contents from `sourcedir` to `/mnt/destinationdir` and:

- Excludes `File4.txt` and the `.log` and `.error` files, as listed in `/home/opc/list.txt`.

```
[opc@example ~]$ cat /home/opc/list.txt
File4.txt
*.log*
*.err*

[opc@example ~]$ date; time sudo parcp --exclude-from=/home/opc/list.txt -P 16 --restore /sourcedir /mnt/destinationdir;
date Mon Jun  1 15:58:30 GMT 2020
real 9m55.820s
user 0m3.602s
sys 1m5.441s
Mon Jun  1 16:08:25 GMT 2020
```

Performing `ls -l` on `/mnt/destinationdir` shows that only the desired files have been copied.

```
[opc@example destinationdir]$ ls -l
total 91
-rwxr-xr-x.  1 opc opc         37 Nov 30 2017 File1.txt
-rwxr-xr-x.  1 opc opc         15 Dec  1  2017 File2.txt
```

Oracle Cloud Infrastructure User Guide 1996
To use PARCP as an effective alternative for RSYNC in parallel

The `--restore` option in parcp is similar to using the `-a` `-r` `-x` and `-H` options in rsync. (See [rsync(1)-Linux Man Page.](#) The `-P` option is used to set the number of parallel threads you want to use.

The `restore` option includes the following behavior:

- Recurse into directories
- Stop at file system boundaries
- Preserve hard links, symlinks, permissions, modification times, group, owners, and special files such as `named` sockets and `fifo` files

```
$parcp -P 16 --restore /source/folder/ /destination/folder/
```

You can use parcp with the `--restore` and `--delete` options to sync files between a source and target folder. This is a good substitute for using rsync in parallel. As files are added or removed from the source directory, you can run this command at regular intervals to add or remove the same files from the destination directory. You can automate syncing by using this command option in a cron job.

```
sudo parcp -P 32 --restore --delete /source/folder/ /destination/folder/
```

**File System Metrics**

You can monitor the health, capacity, and performance of your file systems and mount targets by using `metrics`, `alarms`, and `notifications`.

This topic describes the metrics emitted by the metric namespace `oci_filestorage` (the File Storage service).

**Overview of Metrics for oci_filestorage**

File Storage service metrics help you measure operations and throughput related to file systems and mount targets. The available metrics help you determine quickly if your file system is accessible, how much data is flowing through its associated mount target, and if operations are producing unexpected errors. You can get visibility into your workload IOPs and latency, and set up alarms to receive notifications if tolerance thresholds are exceeded.

File Storage metrics include these resources:

- **File system**: A high-performance shared storage entity made available to a network by an associated mount target.
- **Mount target**: An NFS endpoint that lives in a VCN subnet of your choice and provides network access for file systems.

Metrics provided for file systems can be filtered or grouped by their associated mount target.

**Raw Data Point Frequency**

For every 1-minute interval, the File Storage service posts one raw data point to the Monitoring service. The Monitoring service charts show data points at 1-minute, 5-minute, 1-hour (60-minute), and 1-day intervals. Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the `1h` or `1d` interval values are supported. The available statistics are calculated by using the count of 1-minute data points in the select interval. For example, for a given metric:

- The mean for each 5-minute interval is calculated over 5 raw data points.
- The mean for each 60-minute interval is calculated over 60 raw data points.
**Required IAM Policy**

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

**Available Metrics: oci_filestorage**

The metrics listed in the following table are automatically available for any file system or mount target. You do not need to enable monitoring on the resource to get these metrics.

You also can use the Monitoring service to create custom queries.

Each metric includes one or more of the following dimensions:

| RESOURCEID | The OCID of the file system or mount target. |
| MOUNTTARGETID | The OCID of the mount target exporting an associated file system. |

**THROUGHPUT**

The type of request throughput:

- ReadThroughput
- WriteThroughput

**SIZE**

The request size range:

- 0–8 KiB
- 8–64 KiB
- 64 KiB – 1 MiB

**HEALTHITEM**

The type of health rate item:

- SuccessRate
- ErrorRate

**File System Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileSystemReadThroughput</td>
<td>FilesystemRead</td>
<td>bytes</td>
<td>Read throughput for the file system. If the file system is exported through multiple mount targets, total throughput for all mount targets is displayed. Expressed as bytes read per second.</td>
<td>resourceId, mountTargetId, throughput</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>FileSystemWriteThroughput</td>
<td>Write Throughput</td>
<td>bytes</td>
<td>Write throughput for the file system. If the file system is exported through multiple mount targets, total throughput for all mount targets is displayed. Expressed as bytes written per second.</td>
<td></td>
</tr>
<tr>
<td>FileSystemReadRequestsbySize</td>
<td>Read Requests</td>
<td>operation</td>
<td>Read requests by size: 0–8 KiB, 8–64 KiB, 64 KiB – 1 MiB. Expressed as operation per second, grouped by size.</td>
<td>resourceId, mountTargetId, size</td>
</tr>
<tr>
<td>FileSystemWriteRequestsbySize</td>
<td>Write Requests</td>
<td>operation</td>
<td>Write requests by size: 0–8 KiB, 8–64 KiB, 64 KiB – 1 MiB. Expressed as operation per second, grouped by size.</td>
<td></td>
</tr>
<tr>
<td>FileSystemReadAverageLatencybySize</td>
<td>Read Latency</td>
<td>second</td>
<td>Read latency by size: 0–8 KiB, 8–64 KiB, 64 KiB – 1 MiB. Expressed as average read latency per second, grouped by size.</td>
<td></td>
</tr>
<tr>
<td>FileSystemWriteAverageLatencybySize</td>
<td>Write Latency</td>
<td>second</td>
<td>Write latency by size: 0–8 KiB, 8–64 KiB, 64 KiB – 1 MiB. Expressed as average write latency per second, grouped by size.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>MetadataRequestAverageLatency</td>
<td>Metadata Latency</td>
<td>second</td>
<td>Average metadata request latency for the following NFS operations: CREATE, GETATTR, SETATTR, ACCESS, LOOKUP, READLINK, and REMOVE. Expressed as average latency per second, grouped by operation.</td>
<td>resourceId, mountTargetId operation</td>
</tr>
<tr>
<td>MetadataIOPS</td>
<td>Metadata IOPs</td>
<td>operation</td>
<td>IOPs (Input/Output Operations Per Second) for the following NFS operations: CREATE, GETATTR, SETATTR, ACCESS, LOOKUP, READLINK, and REMOVE. Expressed as operations per second.</td>
<td></td>
</tr>
<tr>
<td>FileSystemUsage</td>
<td>Usage</td>
<td>bytes</td>
<td>Total space utilization for a file system. Expressed as GiB consumed per second.</td>
<td>resourceId, mountTargetId</td>
</tr>
</tbody>
</table>

**Mount Target Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MountTargetReadThroughput</td>
<td>Read Throughput</td>
<td>bytes</td>
<td>Read throughput for the mount target. If the mount target exports multiple file systems, total throughput for all file systems is displayed. Expressed as bytes read per interval.</td>
<td>resourceId, throughput</td>
</tr>
</tbody>
</table>
### File Storage

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MountTargetWriteThroughput</td>
<td>Write Throughput</td>
<td>bytes</td>
<td>Write throughput for the mount target. If the mount target exports multiple file systems, total throughput for all file systems is displayed. Expressed as bytes written per interval.</td>
<td></td>
</tr>
<tr>
<td>MountTargetConnections</td>
<td>Connections</td>
<td>count</td>
<td>Number of client connections for the mount target. Expressed as total connection count at the interval.</td>
<td>resourceId</td>
</tr>
<tr>
<td>MountTargetHealth</td>
<td>Health</td>
<td>percent</td>
<td>Number of successfully executed NFS API requests. Expressed as a percentage of total requests per interval.</td>
<td>resourceId, healthItem</td>
</tr>
</tbody>
</table>

### Tips for Working with File Storage Metrics

You can use the tables below to help interpret the data you see in File Storage metric charts. You can familiarize yourself with the typical metrics emitted by the File Storage service using the chart defaults.

### File System Charts

<table>
<thead>
<tr>
<th>This chart...</th>
<th>shows this information...</th>
<th>using these defaults...</th>
<th>that you can use to...</th>
</tr>
</thead>
</table>
| Read Throughput/Write Throughput | The read or write throughput of your file system in bytes per second. Read/write throughput is averaged across all mount targets that export the file system. Only the default mean statistic is meaningful. | • Statistic - mean  
• Interval - 1 minute  
• Time range - 3 hours  
• y-axis - bytes per second | • Ensure that your workloads have sufficient read/write bandwidth for maximum performance.  
• Identify which file systems have the highest and lowest throughput.  
• Receive notifications when read or write throughput is above or below tolerance, so you can take action. |
<table>
<thead>
<tr>
<th>This chart...</th>
<th>shows this information...</th>
<th>using these defaults...</th>
<th>that you can use to...</th>
</tr>
</thead>
</table>
| **Read Requests/Write Requests** | Read or write operation requests processed by your file systems in bytes per second. Each operation is placed in one of these three size groups:  
• 0–8 KiB  
• 8–64 KiB  
• 64 KiB - 1 MiB  
Only the default **mean** statistic is meaningful. | • Statistic - mean  
• Interval - 1 minute  
• Time range - 3 hours  
• Grouped by: size  
• y-axis - bytes per second | • See which file systems might have lower performance than expected.  
• Measure impact of operation size on file system and workload performance.  
• Identify and monitor file systems whose workloads are consistently receiving larger read or write requests and compare performance over time.  
• Receive notifications when operation bytes per second for a larger group size is too high. |
| **Read Latency/Write Latency** | Average latency of read or write operation requests processed by your file systems in bytes per second. Each operation is placed in one of these three size groups:  
• 0–8 KiB  
• 8–64 KiB  
• 64 KiB - 1 MiB  
These charts don't report zero latency, or periods when there are no read/write operations happening. Information is presented in the charts as individual data points. | • Statistic - mean  
• Interval - 1 minute  
• Time range - 3 hours  
• Grouped by: size | • See which file systems might have lower performance than expected due to operation latency.  
• Measure impact of operation latency on file system and workload performance.  
• Troubleshoot possible network or application issues that might increase file system latency.  
• Receive notifications when operation latency exceeds tolerance, so you can take action. |
<table>
<thead>
<tr>
<th>This chart...</th>
<th>shows this information...</th>
<th>using these defaults...</th>
<th>that you can use to...</th>
</tr>
</thead>
</table>
| **Metadata Latency** | Average latency of read or write metadata operation requests processed by your file systems in bytes per second. CREATE, GETATTR, SETATTR, ACCESS, LOOKUP, READLINK, and REMOVE operations are shown. Each operation is placed in one of these three size groups: | • Statistic - mean  
• Interval - 1 minute  
• Time range - 3 hours  
• Grouped by: size | • See which metadata operations requested by your workload have the highest and lowest latency.  
• Measure impact of metadata operation latency on file system and workload performance.  
• Receive notifications when a metadata operation exceeds tolerance.  
• Troubleshoot your application workloads. |
| **Metadata IOPs** | IOPs per second of read or write metadata operation requests processed by your file systems. CREATE, GETATTR, SETATTR, ACCESS, LOOKUP, READLINK, and REMOVE operations are shown. | • Statistic - rate  
• Interval - 1 minute  
• Time range - 3 hours  
• Grouped by: operation  
• y-axis - bytes per second | • See which metadata operations requested by your workload have the highest and lowest IOPs.  
• Identify specific operations that might consistently have higher or lower IOPs.  
• Receive notifications when IOPs for a metadata operation are below tolerance.  
• Troubleshoot your application workloads. |
**File Storage**

<table>
<thead>
<tr>
<th>This chart...</th>
<th>shows this information...</th>
<th>using these defaults...</th>
<th>that you can use to...</th>
</tr>
</thead>
</table>
| **Usage**     | The total space utilization for each file system per hour. The data in this chart is presented differently than the utilization value shown in the Details tab of the file system: | - Statistic - mean  
- Interval - 1 hour  
- Time range - 1 day | - See what the total space utilization is for all of your file systems.  
- Identify which of your file systems are consuming the most and least space.  
- Identify which of your file systems are incurring the most and least cost.  
- Use in conjunction with the information in File System Usage and Metering on page 2007 and receive notifications when usage is not within expectations. |
|               | - File system utilization is displayed in GiB. This chart displays GB.  
- File system utilization is captured once every hour. This chart captures one data point every minute.  
- There may be temporary discrepancies between the file system utilization value and the Usage chart. For example, if the usage for a file system briefly spikes during the file system's hourly update, the utilization value may temporarily appear higher than expected when compared to the Usage chart. |                          |                       |

**Mount Target Charts**

<table>
<thead>
<tr>
<th>This chart...</th>
<th>shows this information...</th>
<th>using these defaults...</th>
<th>that you can use to...</th>
</tr>
</thead>
</table>
| **Read Throughput/Write Throughput** | The read or write throughput of your mount target in bytes per second. Read/write throughput is averaged across all file systems exported by the mount target. Only the default mean statistic is meaningful. | - Statistic - mean  
- Interval - 1 minute  
- Time range - 3 hours  
- y-axis - bytes per second | - Ensure that your workloads have sufficient read/write bandwidth for maximum performance.  
- Identify which mount targets have the highest and lowest throughput.  
- Receive notifications when read or write throughput is below tolerance, so you can take action. |

---

Oracle Cloud Infrastructure User Guide 2004
This chart shows this information using these defaults that you can use to:

| Connections | The number of active connections for each mount target. Typically, one connection represents one NFS client. | • Statistic - sum  
• Interval - 1 minute  
• Time range - 3 hours | • See how many active connections each mount target has.  
• Measure impact of high connection count on file system and workload performance.  
• Decide if additional mount targets are required for your workload. |
| Health | The percentage of requests processed successfully by the mount target. | • Statistic - mean  
• Interval - 1 minute  
• Time range - 3 hours | • See which mount targets have the highest and lowest percentage of successfully processed requests.  
• Identify mount targets that are not performing well and troubleshoot possible causes.  
• Receive notifications when mount target health drops below tolerance, so you can take action. |

Using the Console

To view default metric charts for a single file system

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click File Systems.
2. Click the file system to view its details.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for a single mount target

1. Open the navigation menu. Under Core Infrastructure, click File Storage and then click Mount Targets.
2. Click the mount target to view its details.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for multiple file systems and mount targets

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that contains the file storage resource you're interested in.
3. For **Metric Namespace**, select **oci_filestorage**.
   The **Service Metrics** page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

**Paths in File Systems**

The File Storage service uses three kinds of paths:

1. **Export Paths** are part of the information contained in an export that makes a file system available through a mount target. The export path uniquely identifies the file system within the mount target, letting you associate up to 100 file systems behind a single mount target. The export path is used by an instance to mount (logically attach to) the file system. This path is unrelated to any path within the file system or the client instance. It exists solely as a way to distinguish one file system from another within a single mount target.

In this mount command example, `10.0.0.6` is the mount target IP address. `/FileSystem1` is the unique export path that was specified when the file system was associated with a mount target during creation.

```
sudo mount 10.0.0.6:/FileSystem1 /mnt/mountpointA
```

**Important:**

The export path must start with a slash (/) followed by a sequence of zero or more slash-separated elements. For multiple file systems associated with a single mount target, the export path sequence for the first file system cannot contain the complete path element sequence of the second file system export path sequence. Export paths cannot end in a slash. No export path element can be a period (.) or two periods in sequence (..). No export path can exceed 1024 bytes. Lastly, no export path element can exceed 255 bytes. For example:

**Acceptable:**

```
/example and /path
/example and /example2
```

**Not Acceptable:**

```
/example and /example/path
/ and /example
/example/
```
Caution:
If one file system associated to a mount target has `/` specified as an export path, you can't associate another file system with that mount target.

Note:
Export paths cannot be edited after the export is created. If you want to use a different export path, you must create a new export with the desired path. Optionally, you can then delete the export with the old path.

See Managing Mount Targets on page 1980 for more information about mount targets and exports.

2. **Mount Point Paths** are paths within a client instance to a locally accessible directory to which the remote file system is mounted.

   In this mount command example, `/mnt/mountpointA` is the path to the directory on the client instance on which the external file system is mounted.

   ```
   sudo mount 10.0.0.6:/FileSystem1 /mnt/mountpointA
   ```

   See Mounting File Systems on page 1954 for more information.

3. **File System Paths** are paths to directories within the file system, and contain the contents of the file system. When the file system is mounted, you can create any directory structure within it you like. Snapshots of the file system can be accessed using the file system path, under the file system's root directory at `.snapshot/name`.

   The following example shows the path to a snapshot called 'January 1' when navigating from the instance:

   ```
   /mountpointA/.snapshot/January1
   ```

### File System Usage and Metering

This topic describes how usage and metering are calculated for your file systems, to help you understand and manage your service costs. This topic also describes different ways to see your file system and snapshot utilization and the differences in reporting that can occur depending on which method you use.

#### Overview

File Storage service provisioning is fully managed and automatic as your utilization scales. For more information, see Space Allocation on page 2007.

Here are the methods you can use to view your file system and snapshot usage:

- The File Storage service reports metered file system utilization and updates hourly. The metered file system utilization comes from the `meteredBytes` value in the API, and represents the authoritative utilization value that is used to count your service cost. You can access the reported utilization for each of your file systems using the Console, the Command Line Interface (CLI), or the API. For more information, see the following section File System Metered Utilization on page 2008.

- The File Storage service supports Network File System (NFS) protocol, so you can use the `df` or `du` command from your instance command line tool to see usage for mounted file systems. However, the usage reported by `du` can differ from both the `meteredBytes` value and the `df` value. For more information, see Using DF and DU Commands on page 2008.

#### Space Allocation

The File Storage service allocates space in blocks of variable size in a way that minimizes total customer cost and optimizes performance. Other storage systems might allocate blocks differently than Oracle Cloud Infrastructure File Storage. If you copy files from another storage device to your Oracle Cloud Infrastructure file system, you might see minor differences when you compare the physical file size before and after copying.
**Metering and Service Cost**

This section describes aspects of file system usage and how they affect your overall service costs.

**File System Metered Utilization**

The File Storage service reports metered utilization size for each file system. The metered utilization size is updated on an hourly cycle. You can see the metered **Utilization** size in the Console on the **Details** page of the file system. This value comes from the File Storage service API `meteredBytes` property which is the total number of bytes consumed by the file system.

The `meteredBytes` value is updated asynchronously with respect to updates to the file system. Your usage charges are calculated based on the `meteredBytes` value.

You can also use the CLI or API to obtain this information. See Managing File Systems on page 1970 for instructions about how to view your file system utilization.

<table>
<thead>
<tr>
<th><strong>Important:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>When you add or remove files from your file system, it can take the File Storage service up to one hour to report the change in metered size.</td>
</tr>
</tbody>
</table>

**Snapshot Metered Utilization**

A snapshot is a point-in-time view of your file system. Snapshots initially consume no additional usage in the file system, because they reference the original data instead of duplicating it, limiting usage cost. A snapshot doesn't change which blocks it references after it's taken.

Snapshot data usage is metered against differentiated data only. If nothing has changed within the file system since the last snapshot was taken, a new snapshot does not consume more storage. The metered size of snapshots is included in the reported `meteredBytes` value of the file system it belongs to.

For example:

1. Let's say you create a file system called "MyFileSystem" and add "File1". The new file system now contains 1 GB including metadata. After the hourly update cycle is complete, the total `meteredBytes` shown by the File Storage service is 1 GB.
2. Next, you create a snapshot of "MyFileSystem" named "Snapshot1". After the hourly update cycle is complete, the total `meteredBytes` shown by the File Storage service remains at 1 GB, because there's no differentiated data yet.
3. You then overwrite the first 0.5 GB of "File1". Now, "MyFileSystem" has a file that is different than the version previously captured in "Snapshot1". The `meteredBytes` value is 1.5 GB, because the differentiated data between the live file system and the snapshot is 0.5 GB.
   
   $ 1 \text{ GB (snapshot)} + 0.5 \text{ GB (differentiated data)} = 1.5 \text{ GB}$
4. If you then delete "File1". "MyFileSystem" now has a `meteredBytes` value of 1 GB, which represents just the usage for "Snapshot1".
5. Finally, delete "Snapshot1". Deleting the snapshot removes its references to the file data. **Provided no other snapshots reference the file data**, the space is relinquished and utilization returns to zero.

**Metadata Metered Utilization**

Files in the file system require space to be allocated for metadata. 512 bytes are required for each directory entry, and 8192 bytes are required for each symlink. Multiple hardlinks to a file create multiple directory entries for the file, and increases the metadata utilization. This utilization is included in the `meteredBytes` value of the file system it belongs to.

**Using DF and DU Commands**

You can use `df` or `du` commands from your instance command-line application to view usage information about your file system. To use these commands to view file system usage, the file system must first be mounted to the instance. See Managing File Systems on page 1954 for instructions on mounting your file system.
How the Commands Work

- `df` provides the amount of storage metered for your file system. Results are returned quickly, but can be up to 1 hour out of date.
- `du` provides the storage used by a directory hierarchy. The `du` command walks the directory tree, and if your hierarchy is large, it can take a long time to run and return results.

How Results can Differ

DF and DU report snapshot utilization differently

A snapshot is a point-in-time view of a file system. Snapshots reference unchanged file system data instead of duplicating it. The file system blocks that the snapshot references don't count towards the snapshot utilization. Only differentiated data increases the snapshot utilization.

- The `df` command retrieves information provided by the File Storage service using the NFS FSSTAT call. The NFS FSSTAT call accounts correctly for the way that snapshots reference file system data. Only utilization caused by differentiated data is reported.
- The `du` command descends the file system tree and uses each file's size attribute to total up the space used. When you create a snapshot, it copies the original size attribute for each file. So, if you run the `du` command, the snapshot reports the file system's size at the time the snapshot was taken, not necessarily the snapshot's actual current utilization.

For example,

1. Let's say you create file system called "MyFileSystem". You then add a 1 GB file called "FileA" to the file system. Here's how each command would report size:

<table>
<thead>
<tr>
<th>For..</th>
<th>du reports...</th>
<th>df reports...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileA</td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>MyFileSystem</td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

2. You then create "Snapshot1". The snapshot is placed in the /.snapshot folder of MyFileSystem. Here's how each command would report size:

<table>
<thead>
<tr>
<th>For..</th>
<th>du reports...</th>
<th>df reports...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileA</td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>snapshot1</td>
<td>1 GB</td>
<td>0 GB</td>
</tr>
<tr>
<td>MyFileSystem</td>
<td>2 GB</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

- `df` reports 0 GB for Snapshot1 because the data hasn't changed yet, so there is no space allocated for differentiated data.
- `du` reports 1 GB for Snapshot1 because it reports the copied file size attribute of FileA, which is 1 GB.

**Important:**

Charges are calculated using the `meteredBytes` value. The utilization size reported by `du` can be much larger than `meteredBytes` value. `df` reports the same value as `meteredBytes`, so you can use it to accurately view the file system size.

DF and DU count hard links differently

- `df` counts each file only once.
- `du` may count files with hard links more than once.
DF and DU count symlinks and metadata differently

- `df` reports the utilization of bytes required by File Storage for metadata and symlinks, even on empty files.
- `du` reports empty files as using zero bytes. It doesn't accurately report the bytes being used by File Storage for metadata and symlinks.

Troubleshooting Your File System

These topics cover some common issues you may run into and how to address them.

File System Setup

- Mount Command Fails
- Mount Target Creation Fails on page 2012
- Mount Target is in a Failed State on page 2021
- Write to File System Fails on page 2013
- File Storage CREATE API Operations Fail on page 2011
- Creating a File System With an Assigned Key Fails on page 2011

File System Management

- Showmount Command Fails on page 2018
- Symbolic Links (Symlinks) Produce Errors on page 2018
- Removing File Locks from a Host that is No Longer Available on page 2017
- Cannot Delete VCN - Mount Target VNIC Still Attached
- Metadata Operations Are Very Slow or Fail on page 2016
- 409 Error Occurs When Creating or Moving a File System or Mount Target on page 2019
- Cannot Mount a File System after Instance Reboot on page 2014
- Cannot Unmount a File System: Device is Busy on page 2015
- DF Operation Reports File System as 100% Used (0% Free) on page 2015
- Removing Snapshots With RM -RF Fails on page 2022
- Mounted File System No Longer Accessible on page 2017
- RSYNC is Slow When Copying Files on page 2018
- Deleted Snapshots Still Appear in DF Output on page 2022

Mount Target Management

- Cannot Delete VCN- Mount Target VNIC Still Attached on page 2019
- Mount Target is in a Failed State on page 2021

Snapshot Management

- Deleted Snapshots Still Appear in DF Output on page 2022
- Removing Snapshots With RM -RF Fails on page 2022

Application Installation

- Application Installation Fails Due to Too Much or Too Little Available Capacity on page 2024
- Application Performance is Not as Expected on page 2024
- Apache Webserver Fails on page 2023
- Oracle E-Business Suite Concurrent Processing is Slow on page 2025
- Access to File System is Denied Due to Stale File Handle on page 2023
• **Sharing the Application Tier File System in Oracle E-Business Suite Release 12.2 or 12.1.3 Using the Oracle Cloud Infrastructure File Storage Service**

  Learn best practices for using a File Storage service shared application tier file system for Oracle E-Business Suite.

**Windows NFS Connections**

• **Create and Write to File System Fails using Windows NFS** on page 2027
• **Mounted Drive is Not Visible in File Explorer** on page 2030
• **Mounting from File Explorer Fails With "An Unexpected Error Occurred."** on page 2031
• **Access to File System using UNC Path is Slow or Fails** on page 2026

**Troubleshooting File System Setup**

Here are some issues you may run into when you set up your file system.

• **Creating a File System With an Assigned Key Fails** on page 2011
• **File Storage CREATE API Operations Fail** on page 2011
• **Mount Command Fails**
• **Mount Target Creation Fails** on page 2012
• **Write to File System Fails** on page 2013

**Creating a File System With an Assigned Key Fails**

How to resolve problems creating a file system with an assigned Oracle Cloud Infrastructure Vault key.

**Symptom:** Creating a file system with an assigned Oracle Cloud Infrastructure Vault key fails with the following exception:

```plaintext
com.oracle.bmc.model.BmcException: (401, NotAuthenticated, false) The required information to complete authentication was not provided or was incorrect.
```

**Cause:** The File Storage service requires authorization to use keys on your behalf. Additionally, you must also authorize users to delegate key usage to the service in the first place. Authorization is provided to the service and users using specific IAM policies.

**Solution:**

1. Create a policy in the tenancy to let a user group delegate key usage in a compartment. For example:

   ```plaintext
   Allow group FileWriters to use key-delegate in compartment ABC where target.key.id = '<key_OCID>'
   ```

2. Assign the user who is creating the file system to the group.

3. Create a policy in the tenancy to let the File Storage service use the key. For example:

   ```plaintext
   Allow service FssOciProd to use keys in compartment ABC where target.key.id = '<key_OCID>'
   ```

For more information, see **Assigning Keys** on page 3971.

**File Storage CREATE API Operations Fail**

**Symptom:** API resource create operations such as `createFileSystem` fail to create resources.

**Cause:** High volume can cause API calls to fail. If you haven't specified `retry` in your request, the operation isn't tried again, and the resource isn't created.

**Solution:** Retry the API operation. Use the `opc-retry-token` header in the create resource request. For example:

```plaintext
POST /20171215/fileSystems
```
See REST APIs on page 4368 for more information.

Mount Command Fails

This topic troubleshoots issues with file system mount commands.

Symptom: Mount command fails.

Cause: The information in the mount command is incorrect

Solution: Verify the information in your mount command, especially the export path information.

The export path is specified when you create an export for the file system in a mount target. It uniquely identifies the file system within the mount target, letting you associate multiple file systems to a single mount target. The export path is appended to the mount target IP address, and used to mount the file system.

```
sudo mount 10.0.0.6:/example/path /mnt/mountpointA
```

In this example, 10.0.0.6: is the mount target IP address, and /example/path is the export path. /mnt/mountpointA is the path to the directory on the client instance on which the external file system is mounted.

Tip:

You can find all the export paths for a file system in the Exports list shown in its Details page, together with associated mount target information.

- You can obtain the correct export path by copying mount commands directly from the file system export. These commands minimize the chance of a typing error. See To get mount command samples on page 1956 for more information.
- If one file system associated with a mount target uses an export path of '/', it will prevent you from associating more file systems with that mount target. No two file systems associated with the same mount target can have an export path that contains a complete path of the other.

See Paths in File Systems on page 2006 for more information.

Symptom: Mounting a file system using an FQDN in the mount command fails, but mounting with an IP address succeeds.

Cause: If the mount target has a hostname specified, the File Storage service creates an FQDN for it and includes it in the mount command sample for the file system. Be sure that the FQDN correctly resolves to the mount target's IP address. For more information about DNS resolution, see DNS in Your Virtual Cloud Network on page 2910.

Mount Target Creation Fails

Mount target creation can fail for various reasons:
• **You’ve exceeded your mount target limit.**

Each availability domain is limited to two mount targets by default. If you create both a file system and a mount target at the same time, it is possible for the file system to be successfully created but the mount target creation to fail because of this limitation.

This limitation can be avoided by reusing a previously created mount target for new file systems. You can reuse a single mount target to make as many file systems available on the network as you wish.

- To reuse a mount target when creating a new file system, select **Select an Existing Mount Target**. The workflow creates a new export for the file system in the existing mount target of your choice.
- To reuse a mount target for an existing file system, you must manually create a new export for the file system in the mount target. For more information, see **To create an export for a file system** on page 1972.

See **Service Limits** on page 215 for a list of applicable limits and instructions for requesting a limit increase.

• **There aren’t enough available IP addresses in your subnet.**

Each mount target requires three internal IP addresses in the subnet to function:

- Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.
- The third IP address is used to create a new VNIC for the mount target during failover. The original primary IP address is retained.
- The File Storage service doesn’t "reserve" the third IP address required for high availability failover.
- Use care to ensure that enough unallocated IP addresses remain available for your mount targets to use during failover.
- Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses for mount target creation.

**Write to File System Fails**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before proceeding with troubleshooting, be sure to implement the following prerequisites for connecting to file systems from Linux-style instances:</td>
</tr>
<tr>
<td>• Mount the file system. Follow the procedure found in <strong>Mounting File Systems From Unix-Style Instances</strong> on page 1957.</td>
</tr>
<tr>
<td>• Set up security rules to work with File Storage. Follow the procedure found in <strong>Configuring VCN Security Rules for File Storage</strong> on page 1927</td>
</tr>
</tbody>
</table>

**Symptom 1:** Writing to a file system from a mounted instance fails.

For example, open a terminal window on the instance and use the `touch` command to write a 'helloworld' file:

```bash
touch /mnt/yourmountpoint/helloworld
```

The write operation fails with the error:

```bash
touch: cannot touch '/mnt/yourmountpoint/helloworld': Permission denied
```

**Cause:** When a file system is created, the `root` user owns the root directory. If you're connecting from an Oracle-provided Linux or CentOS instance, the default user is `opc`. The default user is `ubuntu` when you connect from an Oracle-provided Ubuntu instance. These default users are not root users, so you can't initially write a file or directory to a new file system with these users.

**Solution:** You can implement one of the following solutions:

- Connect as the `root` user. Then, create files or directories in the new file system.
- Connect as the `root` user. Then, change the ownership or permissions of the file system root directory to allow other users (such as `opc` or `ubuntu`) to write to the file system.
• Connect as the root user. Then, create subdirectories with ownership or permissions that allow other users to write to the subdirectory.

Learn more about updating file and directory ownership and permissions.

• Connect as the default user. Then, use the **sudo** command to write or to change permissions or ownership of files or directories. The **sudo** command temporarily provides a regular user with root user permissions. Here's an example of using the **sudo** command to write to the file system:

```bash
sudo touch /mnt/yourmountpoint/helloworld
```

Learn more about the **sudo** command.

For more information on accessing Oracle-provided instances, see Connecting to an Instance on page 733.

**Troubleshooting File System Management**

Here are some issues you may run into while managing your file system.

- Showmount Command Fails on page 2018
- Symbolic Links (Symlinks) Produce Errors on page 2018
- Removing File Locks from a Host that is No Longer Available on page 2017
- Cannot Delete VCN - Mount Target VNIC Still Attached
- 409 Error Occurs When Creating or Moving a File System or Mount Target on page 2019
- Metadata Operations Are Very Slow or Fail on page 2016
- Cannot Mount a File System after Instance Reboot on page 2014
- Cannot Unmount a File System: Device is Busy on page 2015
- DF Operation Reports File System as 100% Used (0% Free) on page 2015
- Removing Snapshots With RM -RF Fails on page 2022
- Mounted File System No Longer Accessible on page 2017
- RSYNC is Slow When Copying Files on page 2018
- Deleted Snapshots Still Appear in DF Output on page 2022

**Cannot Mount a File System after Instance Reboot**

**Symptom:** Cannot re-mount a file system after rebooting the instance.

**Cause:** The NFS client services aren't running on the instance.

**More Information:** The rpcbind and nfslock services don't automatically start at reboot by default.

**Solution:**

1. Add the file system to the instance /etc/fstab file, so the file system is automatically remounted after reboot.
   a. See To auto-mount a file system on page 1961 for instructions.
2. Set the rpcbind and nfslock services to start automatically on every reboot.
   a. Use the following commands to start the rpcbind and nfslock services:

```bash
$ service rpcbind start
$ service nfslock start
```

b. Verify that the rpcbind and nfslock services are running:

```bash
$ service rpcbind status
$ service nfslock status
```

c. Enable the services to start automatically at reboot:

```bash
$ chkconfig rpcbind on
$ chkconfig nfslock on
```
**Cannot Unmount a File System: Device is Busy**

**Symptom:** Unmounting (`umount`) fails with a message: `device is busy`. For example:

```
sudo umount -f 10.x.x.x:/fs-export-path /mnt/yourmountpoint
device is busy
```

**Cause 1:** You're attempting to run the `umount` command from within the mountpoint directory.

**Solution 1:** Move to a directory outside the file system mount point, and retry the `umount` command.

**Cause 2:** An abrupt disconnect from the file system's mount target occurred.

**More Information:** An NFS message similar to the example below is displayed:

```
parrm: B cannot remove 'mnt/directory/.nfs <unique_id>':
Device or resource busy
```

**Solution 2:**

1. Use the `fuser` or `lsof` operation to find the process that has locked the file and note its ID.
   
   See `lsof(8)` - Linux Man Page for information about how to use `lsof`.
   
   See `fuser(1)` - Linux Man Page for information about how to use `fuser`.

2. After you've identified the process that has locked the file, stop the process using the `kill` command. For example:

   ```
   kill <process_id>
   ```

   See `kill(1)` - Linux Man Page for more information.

3. Retry the `umount` command.

**DF Operation Reports File System as 100% Used (0% Free)**

**Symptom:** Running the `df` command on a mounted file system unexpectedly reports zero available space (100% used, 0% free), rather than a realistic value.

**Cause:** The mount target that exports the file system has its `Reported Size` value set incorrectly.

**Solution:** Reset the mount target's `Reported Size (GiB)` to the default value of 8589934592 GiB. For instructions, see To set the file system reported size on page 1985.

**Important:**

Changing the `Reported Size` in the mount target affects all file systems exported through the mount target.

**File System Resources Aren't Visible in the Console**

Learn about why a file system resource might not be visible to you.

**Symptom:** You create a resource, but can't view it after it's created.

**Cause:** You don't have permission to work in the compartment that the resource resides in. Resources in a compartment that you don't have access to aren't visible to you.

When you create a resource, you can specify the compartment you want to create it in. The resource doesn't have to be in the same compartment as related file system resources. Another user might move the resource from one compartment (that you have access to) to another (that you don't).

**Solution 1:** Create the resource in a compartment you have permission to work in.

**Solution 2:** Obtain permission to work in the compartment that the resource resides in. For information about setting up user access, see Overview of Oracle Cloud Infrastructure Identity and Access Management on page 2124.
Metadata Operations Are Very Slow or Fail

**Symptom:** Metadata operations such as `ls -l`, `du`, or `find` are very slow.

**Causes:**

1. `ls`, `find`, and `du` are sequential operations. They create NFS `readdir` and `readdirplus` requests proportional to the number of entries in the directory. The service has high response latency on `readdir` and `readdirplus` requests. The severity of this performance issue can vary because of the directory size, number of files, or how busy the file system is.

2. If a client performs an `ls -l` operation while another client is writing to the file system, an issue with `READDIRPLUS` can cause looping behavior on the client instance.

**Solutions for Cause 1:**

- Use `ls -ld` or `stat` instead of `ls -l`. These operations are much quicker on large directories than `ls -l`.

  For example:

  ```bash
  [opc@instance01 dd]$ time ls -l | wc -l
  401425
  real 0m39.786s
  user 0m4.389s
  sys 0m5.403s
  [opc@instance01 dd]$ time ls -ld
  drwxrwxr-x. 4 opc opc 401424 Apr 17 14:18 .
  real 0m0.009s
  user 0m0.001s
  sys 0m0.003s
  [opc@instance01 dd]$ time stat . | grep Size
  Size: 401424 Blocks: 785 IO Block: 32768 directory
  real 0m0.010s
  user 0m0.002s
  sys 0m0.003s
  [opc@instance01 dd]$
  ```

- Redistribute your files to sub-directories instead of storing a large volume of files in a single directory.

**Solutions for Cause 2:**

- Disable the `READDIRPLUS` NFS operation on the instance:
  
  1. Open a terminal window on the instance.
  2. Unmount the file system with the `umount` command. For example:

     ```bash
     sudo umount 10.x.x.x:/fs-export-path /mnt/yourmountpoint
     ```

  3. Remount the file system, and include the `-o nordirplus` option to disable `READDIRPLUS`. For example:

     ```bash
     sudo mount -o nordirplus 10.x.x.x:/fs-export-path /mnt/yourmountpoint
     ```
• Apply a Linux kernel patch:

A Linux kernel patch is available that addresses this issue. The patch is available to install with Oracle Ksplice on Oracle Linux 7.x instances only. Oracle Ksplice lets you apply important security updates and other critical kernel updates without a reboot. The patch addressing this behavior was made available on April 17th, 2020.

Oracle Ksplice must be installed on the instance. After you install Ksplice, you can install available Ksplice patches.

See Installing and Running Oracle Ksplice on page 664 for instructions.

After you install the patch, you can verify the effective kernel version. Ksplice uptrack doesn't change the output of the uname command. uname continues to reflect the version of the kernel the instance was booted into. Instead, use uptrack-uname to see what effective kernel your instance is running. uptrack-uname has the same format as uname and supports the common uname flags, including \(-r\) and \(-a\).

For example:

```
$ uptrack-uname -r
4.14.35-1902.302.2.el7uek.x86_64
```

**Mounted File System No Longer Accessible**

**Symptom:** A file system that was previously mounted and available is no longer accessible.

**Cause:** The file system's mount target or export was deleted.

**More Information:** File systems are made available to the network using an associated mount target. An export controls how NFS clients access the file systems when they connect to the mount target. A file system needs at least one export in an associated mount target to be available for mounting. Deleting a mount target or an export of a file system makes the file system unavailable.

Even if the file system is exported through multiple mount targets, any instance that uses the deleted mount target or export information to mount the file system loses access. See Managing Mount Targets on page 1980.

**Solution:** Re-create the mount target and a new export for the file system.

1. Follow these instructions to re-create the mount target and export: To create an export for a file system on page 1972.
2. If the mount target still exists, choose Select an Existing Mount Target. If the mount target has been deleted, choose Create a New Mount Target.
3. If you're re-creating the mount target, you can re-use the same name, IP address, and hostname information as the old mount target. Click on Advanced Options to set the IP address and hostname.

**Removing File Locks from a Host that is No Longer Available**

The File Storage service supports the removal of file locks from any file system. To request the removal of file locks on a file system:

1. Go to My Oracle Support and sign in.
   
   If you are not signed in directly to Oracle Cloud Support, click Switch to Cloud Support at the top of the page.
2. Click Create Service Request.
3. Select the following from the displayed menus:
   
   • Service Type: Select Oracle Cloud Infrastructure from the list.
   • Service Name: Select the appropriate option for your organization.
   • Problem Type: FSS File System Lock Removal Request.
4. Enter your contact information.
5. Enter a Description, and then enter the following required fields specific to your issue. For most Oracle Cloud Infrastructure issues you need to include the OCID (Oracle Cloud Identifier) for each resource you need help with. See Locating Oracle Cloud Infrastructure IDs on page 128 for instructions on locating these.

- Tenancy OCID
- File System OCID
- Mount Target OCID
- Host IP Address

For help with any of the general fields in the service request or for information on managing your service requests, click Help at the top of the Oracle Cloud Support page.

**RSYNC is Slow When Copying Files**

**Symptom:** rsync runs very slowly against a file system.

**Cause:** rsync is a serial operation, so it is slow when copying a large file system, especially if snapshots are included in the process.

**Solution:** Use one of the following alternatives:

- GNU Parallel to run rsync in parallel. For example:

  ```
  time find /mnt/MyFileSystem -mindepth 1 -maxdepth 1 | parallel -P100 rsync --archive --perms --owner --group --xattrs --acls --recursive --delete --compress --exclude=.snapshot --ignore-errors --progress --log-file=$HOME/rsync/logs/test.log1 --quiet -e ssh () root@10.0.3.6:/mnt/rsync_target
  ```

  For more information, see GNU Parallel - GNU Project.

- File Storage Parallel Tools

  For more information and examples, see Using File Storage Parallel Tools on page 1994.

- The find command in combination with the xargs option. For example:

  ```
  find ${source_dir} -mindepth 1 -maxdepth 1 | xargs -P 24 -I {} rsync --archive --perms --owner --group --xattrs --acls --recursive --delete --compress --log-file=logfile_path -quiet -e ssh {} <destination_user>@<destination_instance>:<destination_dir>
  ```

  See find(1)- Linux Man Page and xargs(1)- Linux Man Page for more information.

**Showmount Command Fails**

The File Storage service supports the showmount -e command. You can use the showmount -e command to show a list of NFS exports available from a specific mount target IP address.

For example, `$ showmount -e 10.0.0.0`

To enable the command, you must create a security list rule in the subnet containing the mount target. The rule must be a stateful ingress rule for UDP traffic with a Destination Port Range of 111.

Click here for instructions about Configuring VCN Security Rules for File Storage on page 1927.

For more information about this command, see the Linux manual page about showmount.

**Important:**

Only showmount -e is supported. No other options are supported, and the -e option must be included.

**Symbolic Links (Symlinks) Produce Errors**

The File Storage service fully supports the use of symbolic links. However, symbolic links are interpreted by the client and symlinks that point outside of the mounted File Storage system may be interpreted differently by each client and lead to unexpected results, such as broken links or pointing to the wrong file. Symbolic link targets that
work on one client might be broken on another due to differences in file system layout or because clients mounted the
file system using different mount targets.

Snapshots can also break symbolic links that point to a target outside the file system’s root directory. This is because
when you create a snapshot of a file system, it becomes available as a subdirectory of the .snapshot directory.

To minimize these potential issues, use a relative path as the target path when creating a symbolic link to a file in the
network file system. Also, ensure that relative paths do not point to a target path outside the File Storage service root
directory except when the target is on the local machine. If you must use a symbolic link that points to a target path
outside the file system, use an absolute path starting with the client’s root directory.

For example:

- Pointing to "/user/bin/example" **works**.
- Pointing to "/yourmountpoint/..." does **not** work.
- Pointing to "/home/user/yourmountpoint/..." does **not** work.

### 409 Error Occurs When Creating or Moving a File System or Mount Target

**Symptom:** When creating or moving a file system or mount target from one compartment to another, you encounter a
409 error. For example:

```python
oci.exceptions.ServiceError: {'opc-request-id': '<<OPC REQUEST ID>>', 'code': 'Conflict', 'message': 'Another filesystem is currently being provisioned, try again later', 'status': 409}
```

**Cause:** There are constraints that limit the number of concurrent operations that a tenancy can perform on file system
and mount target resources in a region:

- Each tenancy in a region can have 1 CreateFileSystem or ChangeFilesystemCompartment
  operation in progress at a time.
- Each tenancy in a region can have 1 CreateMountTarget or ChangeMountTargetCompartment
  operation in progress at a time.

**Solution:** Retry the operation, either manually or programmatically. The default retry strategy for the OCI SDK is to
not retry 409 conflicts, so create a custom retry strategy that retries on 409.

For more information, see [409 error occurs when creating or moving a file system or mount target in Known Issues](#).

For more information about retry strategies, see [SDK Behaviors - Retries](#).

Several examples of building a custom retry strategy are provided at [https://github.com/oracle/oci-python-sdk/blob/master/examples/retries.py](https://github.com/oracle/oci-python-sdk/blob/master/examples/retries.py).

### Troubleshooting Mount Target Management

Troubleshooting topics about mount target management.

- [Cannot Delete VCN- Mount Target VNIC Still Attached](#) on page 2019
- [Mount Target is in a Failed State](#) on page 2021

**Cannot Delete VCN- Mount Target VNIC Still Attached**

A mount target is an NFS endpoint that lives in a VCN subnet of your choice and provides network access for the file
systems that it exports. Each mount target has a VNIC to enable network access. Mount target VNICs that remain in a
VCN must be deleted before you can delete the VCN.

Deleting a mount target also deletes all of the exports of associated file systems that exist in its export set. Data in
the file systems is not affected, but the file systems are no longer available through the deleted mount target. You can
create new exports for the file system in a different mount target and subnet.

For more information, see [Managing Mount Targets](#) on page 1980.
To resolve this issue using the Console

1. Note the OCID in the error message you receive when you attempt to delete the VCN. Mount target OCIDs contain the identifier mounttarget. For example:

   ocid1.mounttarget.oc1.phx.examplemounttargetid

2. Note the **Compartment** and **Subnet** information of the **VCN** you want to delete, and to assist navigation and choosing the correct mount target to delete.

3. Delete the mount target using the following steps:
   a. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **Mount Targets**.
   b. In the **List Scope** section, select a compartment.
   c. Find the mount target you want to delete.
   d. Click the Actions icon (three dots), and then click **Delete**.

   **Caution:**
   Deleting the mount target also deletes all of its exports of associated file systems. File systems are no longer available through the deleted mount target.

   **Tip:**
   In the Console, the mount target OCID can be seen in the mount target details page in the **Mount Target Information** tab. See Managing Mount Targets on page 1980 for more information about how to view the mount target details page. Be sure the mount target OCID seen on the details page matches the mount target OCID provided by the VCN delete process error message.

4. Delete the VCN.

To resolve this issue using the API

1. Note the OCID in the error message you receive when you attempt to delete the VCN. Mount target OCIDs contain the identifier mounttarget. For example:

   ocid1.mounttarget.oc1.phx.examplemounttargetid

2. Delete the mount target using the following steps:
   a. Use **DeleteMountTarget** to delete the mount target. For example:

   ```
   DELETE /20171215/mountTargets/
   ocid1.mounttarget.oc1.phx.examplemounttargetid
   Host: filestorage.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   ```

   b. You can use **GetMountTarget** to verify that the mount target has been deleted. For example:

   ```
   GET /20171215/mountTargets/
   ocid1.mounttarget.oc1.phx.examplemounttargetid?compartmentId=<compartmentId>
   Host: filestorage.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   ```

   The API should return **Status 404 Not Found**.

To resolve this issue using the CLI

For general information about using the CLI, see Command Line Interface (CLI) on page 4192.
1. Note the OCID in the error message you receive when you attempt to delete the VCN. Mount target OCIDs contain the identifier `mounttarget`. For example:

   `ocid1.mounttarget.oc1.phx.examplemounttargetid`

2. Delete the mount target using the following steps:
   a. Use `oci fs mount-target delete` to delete the mount target. For example:

   ```
   oci fs mount-target delete --mount-target-id ocid1.mounttarget.oc1.phx.examplemounttargetid
   ```
   
   b. You can use `oci fs export get` to verify that the mount target has been deleted. For example:

   ```
   oci fs export get --export-id ocid1.mounttarget.oc1.phx.examplemounttargetid
   ```

   The CLI should return a message indicating the mount target is not found. For example:

   ```
   {
     "code": "NotAuthorizedOrNotFound",
     "message": "Authorization failed or requested resource not found.",
     "opc-request-id": "<requestID>",
     "status": 404
   }
   ```

   If you still can't delete the VCN, be sure there are no other resources remaining in the VCN that might prevent it. For more information, see Subnet or VCN Deletion on page 3334.

**Mount Target is in a Failed State**

**Symptom:** A mount target reports a Failed state. File systems are not accessible using the mount target's IP address.

**Possible Cause:** There are insufficient unallocated IP addresses in the subnet. The mount target cannot fail over successfully.

Each mount target requires three internal IP addresses in the subnet to function:

- Two of the IP addresses are used during mount target creation. The third IP address must remain available for the mount target to use for high availability failover.
- The third IP address is used to create a new VNIC for the mount target during failover. The original primary IP address is retained.
- The File Storage service doesn't "reserve" the third IP address required for high availability failover.
- Use care to ensure that enough unallocated IP addresses remain available for your mount targets to use during failover.
- Do not use /30 or smaller subnets for mount target creation because they do not have sufficient available IP addresses for mount target creation.

**Solution:**

1. Delete the failed mount target.

   To delete a mount target on page 1986
2. Export the file system through an active mount target. You can create a replacement mount target and then create
an export for the file system, or create an export for the file system in a pre-existing mount target.
   • You can use the same export paths for the associated file systems as the previous mount target. However, the
     export path must be unique for each file system within the mount target.
   • If you create a replacement mount target, you can use the same IP address as the previous mount target, if
     available. Be sure to explicitly specify the desired IP address when you create the mount target.

To create a mount target on page 1983
To create an export for a file system on page 1972

3. If necessary, mount the file systems again.

   Mounting File Systems on page 1954

   | Note: |
   | If a replacement mount target uses exactly the same IP address and export paths as previously existed in the deleted mount target, mounted instances reconnect automatically. |

4. To prevent a recurrence of this issue, ensure that sufficient unallocated IP addresses remain available in the
   subnet.

Troubleshooting Snapshot Management
Troubleshooting topics about snapshot management.

   • Deleted Snapshots Still Appear in DF Output on page 2022
   • Removing Snapshots With RM -RF Fails on page 2022

Deleted Snapshots Still Appear in DF Output
Resolve an issue where deleted snapshots still appear in DF output with "stale file handle".

   Symptom: Previously deleted snapshots still appear in df output with the message stale file handle.

   Cause: When you use an NFSv3 client to perform operations such as ls, du, or find on the snapshot directory, the
     service automatically exports the directory. The client uses nfs_d_automount() to detect and mount the
     directory. After the directory is detected and mounted the first time, the client mounts the directory automatically.

     If you then delete the snapshot, the mount becomes disconnected. The client still holds an active reference to the
     snapshot, but can no longer access the snapshot itself, so it reports stale file handle.

   Solution: Manually unmount the snapshot. This might require using the -f flag in the umount command. For example:

     sudo umount -f 10.x.x.x:/fs-export-path /mnt/yourmountpoint

   | Note: |
   | If the umount command fails with the message device busy, see Cannot Unmount a File System: Device is Busy on page 2015 for a solution to this problem. |

Removing Snapshots With RM -RF Fails

   Symptom: Using the rm -rf .snapshot/<snapshot_folder> operation to delete a snapshot from a
   mounted file system fails.

   Cause: Snapshots are read-only and can't be deleted by running rm -rf .snapshot/<snapshot_folder>
   from a client instance. Snapshots must be deleted using the console, CLI, or API.

   Solution: Use one of these methods to delete the snapshot:

   • Use the Console
Troubleshooting Applications

Here are some issues you might run into when installing applications that use your file system.

- Application Installation Fails Due to Too Much or Too Little Available Capacity
- Application Performance is Not as Expected
- Apache Webserver Fails
- Oracle E-Business Suite Concurrent Processing is Slow
- Access to File System is Denied Due to Stale File Handle
- Sharing the Application Tier File System in Oracle E-Business Suite Release 12.2 or 12.1.3 Using the Oracle Cloud Infrastructure File Storage Service

Learn best practices for using a File Storage service shared application tier file system for Oracle E-Business Suite.

Access to File System is Denied Due to Stale File Handle

Symptom: Access to a file system fails with a message: stale file handle. For example:

```
[root@example]# /mnt/MyFileSystem
[root@example]# ls -l
ls: cannot access dbclient: Stale file handle
```

Cause: This issue happens when an application opens or creates a file, deletes and closes it, and then attempts to access or delete the same file again.

**Solution 1:** Restart the application.

**Solution 2:** If Solution 1 doesn't solve the issue, unmount and re-mount the file system. This might require using the -f flag in the `umount` command. For example:

```
sudo umount -f 10.x.x.x:/fs-export-path /mnt/yourmountpoint
sudo mount 10.x.x.x:/fs-export-path /mnt/yourmountpoint
```

**Note:**

If the `umount` command fails with the message `device busy`, see Cannot Unmount a File System: Device is Busy on page 2015 for a solution to this problem.

**Solution 3:** If the first two solutions don't solve the issue, reboot the instance.

Apache Webserver Fails

**Symptom 1:** When Apache webserver is installed on a File Storage file system, login to the web page fails and the Apache `error_log` contains messages like the following:

```
Permission denied: [client IP:port] AH00529: <FSS_mount_point>/public/.htaccess pcfg_openfile: unable to check htaccess file, ensure it is readable and that <FSS_mount_point>/public is executable

Permission denied: [client IP:port] AH00035: access to /index.php denied (filesystem path '<FSS_mount_point>/index.php') because search permissions are missing on a component of the path
```

**Additional Information:**

Permission checks show sufficient read and execute access on the directory and the files. Providing full access (777 permission) to the file storage mount point for testing purposes also fails.
Caution: The '777' permission is used strictly for testing purposes, and might compromise your security policy. Be sure to revert your file system mount point permissions to their previous state after testing is complete.

Cause: By default, the Apache webserver installation expects a local drive. You need to explicitly direct the installation to NFS.

Solution: Enable NFS compatibility for Apache.

Open a terminal on the instance and run:

```
$ sudo setsebool httpd_use_nfs on
```

Or:

```
$ sudo setsebool -P httpd_use_nfs 1
```

Application Installation Fails Due to Too Much or Too Little Available Capacity

The File Storage service reports file system capacity as 8589934592 gibibytes (GiB) and 8589934592 gibinodes (GiI) by default. Sometimes, application installers perform a space requirement check prior to running an installation process but cannot correctly interpret the reported size or reported inodes of the file system. When this occurs, you can define the file system size reported to the operating system by setting the **Reported Size** or **Reported Inodes** value in the export set of the file system's mount target.

Important:

Changing the **Reported Size** or **Reported Inodes** for a mount target affects all file systems exported by the mount target. Changing these values does not limit the amount of data you can store.

If your application installation is failing because of too little available space, you can expand the reported available free space. If your application installation is failing because of too much reported available free space, you can reduce it. Typically, setting the size to 1024 GiB and the inodes to 1024 GiI permits successful installation.

Important:

There can be a delay of up to 1 hour when reporting file system usage, either in the console or by using the `df` command.

To set the file system reported size on page 1985 in the Console

To set the file system reported size on page 1990 in the CLI

To set the reported free space in the API

You can use the `UpdateExportSet` operation to update the `MaxFsStatBytes`.

See REST APIs on page 4368 for more information.

Application Performance is Not as Expected

Several factors can impact application performance:

- **Available bandwidth**

  We recommend that you use bare metal Compute instances because instance bandwidth scales with the number of oCPU’s. Bare metal Compute instances provide the greatest bandwidth. Virtual machines (VMs) are bandwidth limited based on the number of CPUs consumed. Single oCPU VM Compute instances provide the least bandwidth.
• **Latency**

Subnets can be either AD-specific or regional. The type of subnet you choose to create your File Storage resources in can affect latency. You can create File Storage resources in either type of subnet.

Regional subnets allow Compute instances to connect to any mount target in the subnet regardless of AD, with no additional routing configuration. However, to minimize latency, place mount targets in the same AD as Compute instances just as you would in an AD-specific subnet.

For more information, see [VCNs and Subnets](#) on page 2821.

**Tip:**

If you want to verify that your instance and mount target are in the same availability domain, you can view the availability domain for any mount target in its **Details** page, in the **Mount Target Information** tab:

A file system is always in the same subnet as its associated mount target.

You can also view the availability domain for any instance in its **Details** page, in the **Instance Information** tab:

• **Mount options**

By not providing explicit values for mount options such as `rsize` and `wsize`, the client and server can negotiate the window size for read and write operations that provide the best performance.

**Oracle E-Business Suite Concurrent Processing is Slow**

**Symptom:** On an Oracle E-business Suite system that uses a shared application tier file system, EBS concurrent processing is slow.

**Cause:** The `APPLLDM` environment variable is referenced by `AutoConfig` and used to control the placement of concurrent processing logs. The placement of these files can have performance implications.
**Solution:** Set APPLLDM to a value *other* than *single*, so that there are multiple log and output directories instead of one large directory. See *Sharing the Application Tier File System in Oracle E-Business Suite Release 12.2 or 12.1.3 Using the Oracle Cloud Infrastructure File Storage Service* for instructions.

### Troubleshooting Windows NFS Connections

Here are some issues you may run into with Windows NFS Connections to your file system.

- **Create and Write to File System Fails using Windows NFS** on page 2027
- **Mounted Drive is Not Visible in File Explorer** on page 2030
- **Mounted Drive is Not Visible in PowerShell** on page 2030
- **Mounting from File Explorer Fails With "An Unexpected Error Occurred."** on page 2031
- **Access to File System using UNC Path is Slow or Fails** on page 2026

### Access to File System using UNC Path is Slow or Fails

**Important:**

Before proceeding with troubleshooting, be sure to implement the following prerequisites for connecting to file systems from Windows instances:

- Install the NFS Client. Follow the installation procedure found in *Mounting File Systems From Windows Instances* on page 1964.
- Set up security rules to work with File Storage. Follow the procedure found in *Configuring VCN Security Rules for File Storage* on page 1927

**Symptom 1:** Windows NFS connection to a file system using a Universal Naming Convention (UNC) path is significantly delayed or fails. The effect is intermittent.

**Symptom 2:** Mount fails using Windows NFS connection with "Network Error 53 "Network path not found".

**Cause:** By default, Windows network providers have higher priority than the client for NFS network provider. Initially, the delay as Windows tries each provider in the default order is significant. Subsequent attempts may be faster because the mount information is cached. After the cache times out, the delay increases again. The native Windows file system client called Distributed File System (DFS) is also given default priority over NFS client, increasing the delay.

**Solution:** Change the network provider order and disable the DFS client so that the client for NFS Network provider is tried first.

For reference, see:

- Support for UNC Naming and MUP
- Modify the protocol bindings and network provider order
- MUP and DFS Interactions

To change the network provider order and disable the DFS client on Windows 2012+

1. Click **Windows Search**.
2. Enter *regedit* in the **Search** field and press **Enter**.
3. Click **Yes** to allow changes to your device.
4. Click **HKEY_LOCAL_MACHINE**.
5. **Browse to:** System\CurrentControlSet\Control\NetworkProvider\Order
6. Change the Network Provider order from default to Nfsnp,RDPNP,LanmanWorkstation:
   a. Right-click **ProviderOrder**, and select **Modify**.
   b. In the **Value Data** field, enter Nfsnp,RDPNP,LanmanWorkstation. If there are any further items that exist in this field on your instance, enter them after LanmanWorkstation.
   c. Click **OK**.
7. **Browse to:** System\CurrentControlSet\Services\Mup.
8. Add a new DWORD32 registry entry for DisableDfs:
   a. Click Edit, and select New DWORD (32 bit) Value.
   b. In the Name field, enter DisableDfs.
   c. Right-click DisableDFS, and select Modify.
   d. In the Value Data field, enter 1.
   e. Click OK.
9. Restart the instance.

Create and Write to File System Fails using Windows NFS

**Important:** Before proceeding with troubleshooting, be sure to implement the following prerequisites for connecting to file systems from Windows instances:
- Install the NFS Client. Follow the installation procedure found in Mounting File Systems From Windows Instances on page 1964.
- Set up security rules to work with File Storage. Follow the procedure found in Configuring VCN Security Rules for File Storage on page 1927.

**Symptom:** After installing Windows NFS client, you can successfully mount the file system from Windows, but any attempt to create or update a file in the file system fails.

**Cause 1:** Registry entries that map the AnonymousGid and AnonymousUid to the root user are missing or in the wrong place.

Access to NFS file systems requires UNIX-style user and group identities, which are not the same as Windows user and group identities. To enable users to access NFS shared resources, Windows client for NFS accesses file systems anonymously, using AnonymousGid and AnonymousUid. On brand new file systems, write permissions are only granted to the root user.

**Solution:** Verify that the correct registry entries are located in HKEY_LOCAL_MACHINE\Software\Microsoft\ClientForNFS\CurrentVersion\Default. If not, add the AnonymousGid and AnonymousUid registry entries to map them to the root user, and then remount the file system with the new user privileges.

**Tip:**
You can verify the AnonymousGid and AnonymousUid are correctly set for a mounted file system by opening a Windows Command Line (CMD) window and typing the mount command without any arguments. A list of all mounted file systems and their properties is shown. The AnonymousGid (GID) and AnonymousUid (UID) values should appear as 0.

For example:
```
C:\>mount
Local    Remote    Properties
-----------------------------------------------
X:       \10.0.1.0\FileSystem
       UID=0, GID=0
       rsize=1048576, wsize=1048576
       mount=soft, timeout=0.8
       retry=1, locking=yes
       fileaccess=755, lang=ANSI
casesensitive=no
```
To map the AnonymousGid and AnonymousUid to the root user

1. In the Windows Command Line (CMD) window, unmount the file system by typing the following. Replace 10.x.x.x with the local subnet IP address assigned to your mount target, fs-export-path with the export path you specified when associating the file system with the mount target, and X with the drive letter of any available drive you want to map the file system to.

   umount 10.x.x.x:/fs-export-path X:

2. Open the registry editor (regedit):
   - Click Windows Search.
   - Enter regedit in the Search field and press Enter.
   - Click Yes to allow changes to your device.

3. Click HKEY_LOCAL_MACHINE. Then, browse to: Software\Microsoft\ClientForNFS \CurrentVersion\Default.

4. Add a new DWORD32 registry entry for AnonymousGid:
   - Click Edit, and select New DWORD (32 bit) Value.
   - In the Name field, enter AnonymousGid. Leave the value at 0.

5. Repeat step 3 to add a second DWORD32 registry entry named AnonymousUid with a value of 0.

6. Open Windows Command Line (CMD) and run as Administrator:
   - Go to Start and scroll down to Apps.
   - In the Windows System section, press Ctrl+Shift and click Command Prompt.
7. In the Windows Command Line (CMD) window, restart the NFS Client by typing the following:

```bash
nfsadmin client stop
nfsadmin client start
```

8. Close the Administrator: Windows Command Prompt (CMD) window. Open a **standard** Command Prompt Window:
   - Click **Start**, then click **Command Prompt**.

   **Important:**
   
   NFS file systems mounted as Administrator are not available to standard users.

9. In the standard Windows Command Line (CMD) window, mount the file system by typing the following. Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target, `fs-export-path` with the export path you specified when associating the file system with the mount target, and `X` with the drive letter of any available drive you want to map the file system to.

```bash
mount 10.x.x.x:/fs-export-path X:
```

**Cause 2:** A standard user is trying to access a file system that was mounted using the Administrator: Command Prompt (CMD). When mounting file systems, it isn’t necessary to run the Command Prompt as Administrator.

**Solution:** Unmount the file system and then remount the file system using a standard Command Prompt. (CMD)

**To remount a file system with a standard Command Prompt (CMD)**

1. Open Windows Command Line (CMD) and run as Administrator:
   - Go to **Start** and scroll down to **Apps**.
   - In the **Windows System** section, press **Ctrl+Shift** and click **Command Prompt**.

2. In the Administrator: Windows Command Line (CMD) window, **unmount** the file system by typing the following. Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target, `fs-export-path` with the export path you specified when associating the file system with the mount target, and `X` with the drive letter of any available drive you want to map the file system to.

   **Tip:**
   
   IP address and export path information is available in the **Details** page of the mount target associated with your file system. See **To view details of a mount target** on page 1984 for more information.

```bash
umount 10.x.x.x:/fs-export-path X:
```

3. **Close** the Administrator: Windows Command Line (CMD) window.

4. Open a **standard** Command Prompt Window:
   - Click **Start**, then click **Command Prompt**.

5. In the **standard** Command Line (CMD) window, mount the file system by typing the following. Replace `10.x.x.x:` with the local subnet IP address assigned to your mount target, `fs-export-path` with the export path you specified when associating the file system with the mount target, and `X` with the drive letter of any available drive you want to map the file system to.

```bash
mount 10.x.x.x:/fs-export-path X:
```
Mounted Drive is Not Visible in File Explorer

Important:
Before proceeding with troubleshooting, be sure to implement the following prerequisites for connecting to file systems from Windows instances:

- Install the NFS Client. Follow the installation procedure found in Mounting File Systems From Windows Instances on page 1964.
- Set up security rules to work with File Storage. Follow the procedure found in Configuring VCN Security Rules for File Storage on page 1927.

Symptom: After installing Windows NFS client, you can successfully mount the file system from Windows, but the file system drive is not visible in File Explorer.

Cause: A standard user is trying to access a file system that was mounted using the Administrator: Command Prompt (CMD). When mounting file systems, it isn't necessary to run the Command Prompt as Administrator.

Solution: Unmount the file system and then remount the file system using a standard Command Prompt (CMD). See To remount a file system with a standard Command Prompt (CMD) on page 2029.

Mounted Drive is Not Visible in PowerShell

Important:
Before proceeding with troubleshooting, be sure to implement the following prerequisites for connecting to file systems from Windows instances:

- Install the NFS Client. Follow the installation procedure found in Mounting File Systems From Windows Instances on page 1964.
- Set up security rules to work with File Storage. Follow the procedure found in Configuring VCN Security Rules for File Storage on page 1927.

Symptom: After installing Windows NFS client, you can successfully mount the file system from either Windows File Explorer or the Command Prompt (CMD) using mount or net use commands. However, the file system drive is not visible in PowerShell.

Cause: A known issue exists where drives mapped from outside PowerShell aren't visible from within PowerShell.

Solution: Unmount the file system and remount the file system within PowerShell, using options to make it visible in File Explorer and in the CMD application.

To unmount a file system using the CMD prompt

1. Open Windows Command Line (CMD) and run as Administrator:
   - Go to Start and scroll down to Apps.
   - In the Windows System section, press Ctrl-Shift and click Command Prompt.
2. In the Administrator: Windows Command Line (CMD) window, unmount the file system by typing the following. Replace 10.x.x.x: with the local subnet IP address assigned to your mount target, fs-export-path with the export path you specified when associating the file system with the mount target, and X with the drive letter of any available drive you want to map the file system to.

   Tip:
   IP address and export path information is available in the Details page of the mount target associated with your file system. See To view details of a mount target on page 1984 for more information.

   umount 10.x.x.x:/fs-export-path X:

To map a drive in PowerShell and make it visible

You can map a drive in PowerShell and then use options to make it visible from File Explorer and the Windows Command Line (CMD).

1. Open Windows PowerShell and run as Administrator:
   a. Go to Start and click the Windows PowerShell icon.
   b. In Windows PowerShell, type the following to run as Administrator:
      ```powershell
      Start-Process powershell -Verb runAs
      ```
   c. In the User Account Control window, click Yes. A new Administrator: PowerShell window opens. You can close the standard PowerShell window to avoid confusing them.

2. Type the following cmdlet. Replace 10.x.x.x: with the local subnet IP address assigned to your mount target, fs-export-path with the export path you specified when associating the file system with the mount target, and X with the drive letter of any available drive you want to map the file system to:
   ```powershell
   New-PSDrive X -PsProvider FileSystem -Root "\10.x.x.x\fs-export-path" -Persist
   ```

Mounting from File Explorer Fails With "An Unexpected Error Occurred."

**Important:**

Before proceeding with troubleshooting, be sure to implement the following prerequisites for connecting to file systems from Windows instances:

- Install the NFS Client. Follow the installation procedure found in Mounting File Systems From Windows Instances on page 1964.
- Set up security rules to work with File Storage. Follow the procedure found in Configuring VCN Security Rules for File Storage on page 1927

**Symptom:** The IP address and export path are correctly represented in the Folder field. When you click Finish, the system attempts to connect to the file system, but fails with an error: "The mapped network drive could not be created because the following error has occurred: An unexpected error occurred."

**Solution 1:** Reboot the instance, and mount the file system again using File Explorer.

**Solution 2:** Mount the file system using the Command Prompt.
Chapter 19

Functions

This chapter explains how to create, deploy, and invoke functions using Oracle Functions.

Overview of Functions

Oracle Functions is a fully managed, multi-tenant, highly scalable, on-demand, Functions-as-a-Service platform. It is built on enterprise-grade Oracle Cloud Infrastructure and powered by the Fn Project open source engine. Use Oracle Functions (sometimes abbreviated to just Functions) when you want to focus on writing code to meet business needs.

The serverless and elastic architecture of Oracle Functions means there's no infrastructure administration or software administration for you to perform. You don't provision or maintain compute instances, and operating system software patches and upgrades are applied automatically. Oracle Functions simply ensures your app is highly-available, scalable, secure, and monitored. With Oracle Functions, you can write code in Java, Python, Node, Go, and Ruby (and for advanced use cases, bring your own Dockerfile, and Graal VM). You can then deploy your code, call it directly or trigger it in response to events, and get billed only for the resources consumed during the execution.

Oracle Functions is based on Fn Project. Fn Project is an open source, container native, serverless platform that can be run anywhere - any cloud or on-premises. Fn Project is easy to use, extensible, and performant. You can download and install the open source distribution of Fn Project, develop and test a function locally, and then use the same tooling to deploy that function to Oracle Functions.

You can access Oracle Functions using the Console, a CLI, and a REST API. You can invoke the functions you deploy to Oracle Functions using the CLI or by making signed HTTP requests.

Oracle Functions is integrated with Oracle Cloud Infrastructure Identity and Access Management (IAM), which provides easy authentication with native Oracle Cloud Infrastructure identity functionality. See Overview of Oracle Cloud Infrastructure Identity and Access Management on page 2124.

To get set up and running quickly with Oracle Functions, see the Quick Start Guides. A number of related Developer Tutorials are also available.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

• Google Chrome 69 or later
• Safari 12.1 or later
• Firefox 62 or later

For general information about using the REST API, see REST APIs on page 4368.
Creating Automation with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

The following Oracle Functions resources emit events:

- applications
- functions

You can also have events in other services invoke functions in Oracle Functions. See Invoking Oracle Functions from Other Oracle Cloud Infrastructure Services on page 2095.

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Oracle Functions Capabilities and Limits

The number of functions and applications you can create in a region is controlled by Oracle Functions service limits (see Functions Limits on page 225). The default service limits vary according to your payment method. If you need more capacity, you can submit a request to increase the default service limits (see Requesting a Service Limit Increase on page 217).

The maximum amount of data you can send to a function (the function's request payload) is 6MB. The maximum amount of data a function can return in response to a request (the function's response payload) is 6MB. These limits are fixed and cannot be changed.

Some other Oracle Functions capabilities and limits are also fixed. However, there are also a number that you can change. See Changing Oracle Functions Default Behavior on page 2095.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies.

For more information about policies for Oracle Functions, see:

- Create Policies to Control Access to Network and Function-Related Resources on page 2041
- Details for Functions on page 2276
Oracle Functions Concepts

This topic describes key concepts you need to understand when using Oracle Functions.

Functions Developers

Oracle Cloud Infrastructure users who use Oracle Functions to create and deploy functions are referred to as 'functions developers'. To use Oracle Functions, functions developers must have Oracle Cloud Infrastructure user accounts. Their user accounts must belong to groups to which appropriate policies grant access to function-related resources.

See Create Groups and Users to use with Oracle Functions, if they don't exist already on page 2039.

Applications

In Oracle Functions, an application is:

• a logical grouping of functions
• a way to allocate and configure resources for all functions in the application
• a common context to store configuration variables that are available to all functions in the application
• a way to ensure function runtime isolation

When you define an application in Oracle Functions, you specify the subnets in which to run the functions in the application. You also specify whether to enable logging for the functions in the application.

When functions from different applications are invoked simultaneously, Oracle Functions ensures these function executions are isolated from each other.

Best practice is to group multiple functions in a single application for better efficiency and performance.

Oracle Functions shows applications and their functions in the Console.

See Creating Applications on page 2061.

Functions

In Oracle Functions, functions are:

• small but powerful blocks of code that generally do one simple thing
• grouped into applications
• stored as Docker images in a specified Docker registry
• invoked in response to a CLI command or signed HTTP request

When you deploy a function to Oracle Functions using the Fn Project CLI, the function is built as a Docker image and pushed to a specified Docker registry.

A definition of the function is stored as metadata in the Oracle Functions server. The definition describes how the function is to be executed and includes:

• the Docker image to pull when the function is invoked
• the maximum length of time the function is allowed to execute for
• the maximum amount of memory the function is allowed to consume

Oracle Functions shows functions, and the applications into which they are grouped, in the Console.

See Creating, Deploying, and Invoking a Helloworld Function on page 2059.

Invocations

In Oracle Functions, a function's code is run (or executed) when the function is called (or invoked). You can invoke a function that you've deployed to Oracle Functions from:

• The Fn Project CLI.
Functions

- The Oracle Cloud Infrastructure SDKs.
- Signed HTTP requests to the function's invoke endpoint. Every function has an invoke endpoint.
- Other Oracle Cloud services (for example, triggered by an event in the Events service) or from external services.

When a function is invoked for the first time, Oracle Functions pulls the function's Docker image from the specified Docker registry, runs it as a Docker container, and executes the function. If there are subsequent requests to the same function, Oracle Functions directs those requests to the same container. After a period being idle, the Docker container is removed.

Oracle Functions shows information about function invocations in metric charts.

See Invoking Functions on page 2071.

Triggers

A trigger is the result of an action elsewhere in the system, that sends a request to invoke a function in Oracle Functions. For example, an event in the Events service might cause a trigger to send a request to Oracle Functions to invoke a function. Alternatively, a trigger might send regular requests to invoke a function on a defined, time-based schedule.

A function might not be associated with any triggers, or it can be associated with one or multiple triggers.

How Oracle Functions Works

This topic describes how Oracle Functions works when you deploy a function, and when you invoke a function.

What Happens When You Deploy a Function to Oracle Functions?

When you have written the code for a function and it's ready to deploy, you can use a single Fn Project CLI command to perform all the deploy operations in sequence:

- building a Docker image from the function
- providing a definition of the function in a func.yaml file that includes:
  - the maximum length of time the function is allowed to execute for
  - the maximum amount of memory the function is allowed to consume
- pushing the image to the specified Docker registry
- uploading function metadata (including the memory and time restrictions, and a link to the image in the Docker registry) to the Fn Server
- adding the function to the list of functions shown in the Console

The above process of deploying a function to Oracle Functions is shown in the diagram.
What Happens When You Invoke a Function?

You can invoke a function that you've deployed to Oracle Functions from:

- The Fn Project CLI.
- The Oracle Cloud Infrastructure SDKs.
- Signed HTTP requests to the function's invoke endpoint. Every function has an invoke endpoint.
- Other Oracle Cloud services (for example, triggered by an event in the Events service) or from external services.

When a function is invoked for the first time, Oracle Functions first verifies the request with the IAM service. Assuming the request passes authentication and authorization checks, Oracle Functions then passes the request to the Fn Server, which uses the function definition to:

- identify the Docker image of the function to pull from the Docker registry
- execute the function by running the function’s image as a container on an instance in a subnet associated with the application to which the function belongs

When the function is executing inside the container, the function can read from and write to other resources and services running in the same subnet (for example, Database as a Service). The function can also read from and write to other shared resources (for example, Object Storage), and other Oracle Cloud Services. You can specify the maximum length of time the function is allowed to execute by setting a timeout in the func.yaml file or in the Console.

Oracle Functions stores the function's logs in Oracle Cloud Infrastructure or in an external logging destination.

When the function has finished executing and after a period being idle, the Docker container is removed. If Oracle Functions receives another call to the same function before the container is removed, the second request is routed to the same running container. If Oracle Functions receives a call to a function that is currently executing inside a running container, Oracle Functions scales horizontally to serve both incoming requests and a second Docker container is started.

Oracle Functions shows information about function invocations in metric charts.

The above process of invoking a function is shown in the diagram.
Functions

Oracle Functions Resiliency, Availability, Concurrency, and Scalability

Resiliency and Availability

Resiliency and availability refers to the ability of a system to continue operating, despite the failure or sub-optimal performance of some of its components.

In the case of Oracle Functions:

- The control plane is a set of components that manages function definitions.
- The data plane is a set of components that executes functions in response to invocation requests.

For resiliency and high availability, both the control plane and data plane components are distributed across different availability domains and fault domains in a region. If one of the domains ceases to be available, the components in the remaining domains take over to ensure that function definition management and execution are not disrupted.

When functions are invoked, they run in the subnets specified for the application to which the functions belong. For resiliency and high availability, best practice is to specify a regional subnet for an application (or alternatively, multiple AD-specific subnets in different availability domains). If an availability domain specified for an application ceases to be available, Oracle Functions runs functions in an alternative availability domain.

Concurrency and Scalability

Concurrency refers to the ability of a system to run multiple operations in parallel using shared resources. Scalability refers to the ability of the system to scale capacity (both up and down) to meet demand.

In the case of Functions, when a function is invoked for the first time, the function's image is run as a container on an instance in a subnet associated with the application to which the function belongs. When the function is executing inside the container, the function can read from and write to other shared resources and services running in the same subnet (for example, Database as a Service). The function can also read from and write to other shared resources (for example, Object Storage), and other Oracle Cloud Services.

If Oracle Functions receives multiple calls to a function that is currently executing inside a running container, Oracle Functions automatically and seamlessly scales horizontally to serve all the incoming requests. Oracle Functions starts multiple Docker containers, up to the limit specified for your tenancy. The default limit is 60 GB of RAM reserved for function execution per availability domain, although you can request an increase to this limit. Provided the
When a tenancy is configured, you will have access, via a suitable policy and user account, to a compartment that has a VCN with at least one public subnet (and an internet gateway) or at least one private subnet (and a service gateway). For more information about these network components, see Networking on page 2746.

You will also have access to a Docker registry in which to store images. This documentation assumes you will be using Oracle Cloud Infrastructure Registry as your Docker registry and provides instructions accordingly. For more information, see Overview of Registry on page 3506.

• You must have configured your client environment for functions development. There are a number of different client environment configuration tasks to complete. For more information, see Configuring Your Client Environment for Function Development on page 2045.

To get set up and running quickly with Oracle Functions, see the Quick Start Guides.

### Availability by Region

Oracle Functions is available in the Oracle Cloud Infrastructure regions listed at Regions and Availability Domains on page 180. Refer to that topic to see region identifiers, region keys, and availability domain names.

### Configuring Your Tenancy for Function Development

Before you can start using Oracle Functions to create and deploy functions, you have to set up your tenancy for function development.

When a tenancy is created, an Administrators group is automatically created for the tenancy. Users that are members of the Administrators group can perform any operation on resources in the tenancy. Oracle Functions users are typically not members of the Administrators group, and do not have to be. However, a member of the Administrators group does need to perform a number of administrative tasks to enable users to use Oracle Functions.

To set up your tenancy for function development, you have to complete the following tasks in the order shown in this checklist (the instructions in the topics below assume that you are a tenancy administrator):

<table>
<thead>
<tr>
<th>Task #</th>
<th>Tenancy Configuration Task</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Create Groups and Users to use with Oracle Functions, if they don't exist already</strong> on page 2039</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Create Compartments to Own Network Resources and Oracle Functions Resources in the Tenancy, if they don't exist already</strong> on page 2039</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><strong>Create the VCN and Subnets to Use with Oracle Functions, if they don't exist already</strong> on page 2040</td>
<td></td>
</tr>
</tbody>
</table>
Click each of the links in turn, and follow the instructions.

When you have set up your tenancy for function development, the next step is to set up your client development environment (see Configuring Your Client Environment for Function Development on page 2045).

Create Groups and Users to use with Oracle Functions, if they don't exist already

Before users can start using Oracle Functions to create and deploy functions, as a tenancy administrator you have to create Oracle Cloud Infrastructure user accounts, along with a group to which the user accounts belong. Later on, you'll define policies to give the group (and the user accounts that belong to it) access to function-related resources. If a suitable group and user accounts already exist, there's no need to create new ones.

To create groups and users to use with Oracle Functions:

1. Log in to the Console as a tenancy administrator.
2. If a suitable group for Oracle Functions users doesn't exist already, create such a group as follows:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups. A list of the groups in your tenancy is displayed.
   b. Click Create Group and create a new group (see To create a group on page 2420). Give the group a meaningful name (for example, acme-functions-developers) and description. Avoid entering confidential information.
3. If suitable user accounts for Oracle Functions users don't exist already, create users as follows:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
   b. Click Create User and create one or more new users (see To create a user on page 2417).
4. If they haven't been added already, add users to the group to use Oracle Functions as follows:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
   b. Select one or more users and add them to the group authorized to use Oracle Functions (see To add a user to a group on page 2417).

Create Compartments to Own Network Resources and Oracle Functions Resources in the Tenancy, if they don't exist already

Before users can start using Oracle Functions to create and deploy functions, as a tenancy administrator you have to create:

- a compartment to own network resources (a VCN, a public or private subnet, and other resources such as an internet gateway or service gateway, a route table, security lists)
• a compartment to own function-related resources (functions, applications)

Note that the same compartment can own both network resources and function-related resources. Alternatively, you can create two separate compartments for network resources and function-related resources.

If suitable compartments already exist, there’s no need to create new ones.

To create a compartment to own network resources and/or function-related resources in the tenancy:

1. Log in to the Console as a tenancy administrator.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A list of the compartments in your tenancy is displayed.
3. Click Create Compartment and create a new compartment (see To create a compartment on page 2442). Give the compartment a meaningful name (for example, acme-network, acme-functions-compartment) and description. Avoid entering confidential information.

Create the VCN and Subnets to Use with Oracle Functions, if they don’t exist already

Before users can start using Oracle Functions to create and deploy functions, a VCN containing the subnets in which to create functions and applications must already exist. The VCN can be, but need not be, owned by the same compartment to which other function-related resources will belong.

Each subnet in the VCN must have a CIDR block that provides at least a certain minimum number of free IP addresses, as follows:

• AD-specific subnets must have a minimum of 12 free IP addresses
• regional subnets must have a minimum of 32 free IP addresses

Note that Oracle strongly recommends each subnet has a CIDR block that provides more than the minimum number of free IP addresses.

To support the largest possible number of concurrent connections, Oracle also strongly recommends that the security lists used by subnets in the VCN only have stateless rules.

If a suitable VCN already exists, there's no need to create a new one.

If you do decide to create a new VCN, you have several options, including the following:

• You can create the new VCN and have related resources created automatically at the same time, using one of the VCN wizards. For example, this topic describes how to use the VCN with Internet Connectivity wizard to create a VCN. As well as creating the VCN, the VCN with Internet Connectivity wizard creates a public regional subnet and a private regional subnet, along with an internet gateway, a NAT gateway, and a service gateway. The VCN with Internet Connectivity wizard also creates route tables and security lists. For more information about the VCN wizards, see Virtual Networking Quickstart on page 2820.
• You can create just the VCN initially, and then create the related resources yourself later (see VCNs and Subnets on page 2821). In this case, you can choose which of the following to create:
  
  • Public subnets and an internet gateway (see Internet Gateway on page 3243). In this case, a route table must include a route rule that targets the internet gateway, with its Destination CIDR Block property set to 0.0.0.0/0. A security list must include a stateful egress rule that allows access to Oracle Cloud Infrastructure Registry (for example, with its Destination Type property set to Service, its Destination Service property set to All <region> services In Oracle Services Network, and its IP Protocol property set to All).
  
  • Private subnets and a service gateway (see Access to Oracle Services: Service Gateway on page 3256). In this case, the service gateway must be set up to allow access to All <region> Services In Oracle Services Network. A route table must include a route rule that targets the service gateway, with its Destination Service property set to All <region> Services In Oracle Services Network. A security list must include a stateful egress rule that allows access to Oracle Cloud Infrastructure Registry (for example, with its Destination Type property set to Service, its Destination Service property set to
All <region> services In Oracle Services Network, and its IP Protocol property set to All).

For example, if you don't want to expose traffic over the public internet, create private subnets and a service gateway (see Oracle Functions Support for Private Network Access on page 2094).

Note that to use an external logging destination like Papertrail, you have to create a VCN with public subnets (see Storing and Viewing Function Logs on page 2078).

To create a VCN to use with Oracle Functions, using the VCN with Internet Connectivity wizard to create related resources automatically:

1. Log in to the Console as a tenancy administrator.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
3. Choose the compartment that will own the network resources (on the left side of the page). For example, acme-network.

The VCN can be, but need not be, owned by the same compartment to which other function-related resources will belong. The page updates to display only the resources in that compartment.

4. Click Start VCN Wizard to create a new VCN.
5. In the Start VCN Wizard dialog box, select VCN with Internet Connectivity and click Start VCN Wizard.

Note that the following instructions assume that you select the VCN with Internet Connectivity wizard to create the VCN and related resources automatically. However, if a different VCN wizard is a better fit for your requirements, select that wizard instead and configure it appropriately (see Virtual Networking Quickstart on page 2820).

6. On the Configuration page, enter:
   - **Name**: A meaningful name for the cloud network, such as acme-functions-vcn. The name doesn't have to be unique, but it cannot be changed later in the Console. Avoid entering confidential information.
   - **Compartment**: The compartment that will own the network resources (by default, the compartment you selected earlier is shown). For example, acme-network.
   - **VCN CIDR Block, Public Subnet CIDR Block, and Private Subnet CIDR Block**: CIDR blocks for the VCN, and the public and private regional subnets. The CIDR blocks you specify for the regional subnets must not overlap, and must have a minimum of 32 free IP addresses.
   - **Use DNS Hostnames in this VCN**: Select this option.
7. Click Next and on the Review and Create page, verify the details of the VCN and related resources that will be created.
8. Click Create to create the VCN, along with the related resources.
9. Click View Virtual Cloud Network to see details of the VCN and the related resources that have been created.

**Create Policies to Control Access to Network and Function-Related Resources**

Before users can start using Oracle Functions to create and deploy functions, as a tenancy administrator you have to create a number of Oracle Cloud Infrastructure policies to grant access to function-related and network resources. You have to:

- Create a Policy to Give Oracle Functions Users Access to Oracle Cloud Infrastructure Registry Repositories on page 2043
- Create a Policy to Give Oracle Functions Users Access to Function-Related Resources on page 2043
- Create a Policy to Give Oracle Functions Users Access to Logging Resources on page 2044
- Create a Policy to Give Oracle Functions Users Access to Network Resources on page 2045

See Details for Functions on page 2276 for more information about policies.

**Tip:**

As an alternative to creating separate policies to grant access to network and function-related resources, you can create a single policy containing all the necessary policy statements. A quick way to create such a policy is to use
the Policy Builder and select the policy template Let users create, deploy,
and manage functions and applications using Cloud Shell on page 2158.
This policy template contains all the policy statements required to use Oracle
Functions. See Writing Policy Statements with the Policy Builder on page
2451.

### Summary of Policies to Create for Oracle Functions

<table>
<thead>
<tr>
<th>Policy to give:</th>
<th>Where to create the policy:</th>
<th>Statement:</th>
<th>More information and examples:</th>
</tr>
</thead>
</table>
| Users access to repositories in Oracle Cloud Infrastructure Registry | Root compartment | Allow group <group-name> to manage repos in tenancy  
Allow group <group-name> to read objectstorage-namespaces in tenancy | Create a Policy to Give Oracle Functions Users Access to Oracle Cloud Infrastructure Registry Repositories on page 2043 |
| Users access to function-related resources | Compartment that owns function-related resources | Allow group <group-name> to manage functions-family in compartment <compartment-name>  
Allow group <group-name> to read metrics in compartment <compartment-name> | Create a Policy to Give Oracle Functions Users Access to Function-Related Resources on page 2043 |
| Users access to logging resources | Root compartment | Allow group <group-name> to read logging-family in tenancy  
Allow group <group-name> to manage logging-family in compartment <compartment-name> | Create a Policy to Give Oracle Functions Users Access to Logging Resources on page 2044 |
| Users access to network resources | Compartment that owns network resources | Allow group <group-name> to use virtual-network-family in compartment <compartment-name> | Create a Policy to Give Oracle Functions Users Access to Network Resources on page 2045 |
Create a Policy to Give Oracle Functions Users Access to Oracle Cloud Infrastructure Registry Repositories

When Oracle Functions users work with functions, they have to access repositories in Oracle Cloud Infrastructure Registry. Users can only access repositories that the groups to which they belong have been granted access. To enable users to access a repository, you must create an identity policy to grant the groups access to that repository.

To create a policy to give Oracle Functions users access to repositories in Oracle Cloud Infrastructure Registry:

1. Log in to the Console as a tenancy administrator and create a new policy in the root compartment:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
   b. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acme-functions-developers-ocir-access).

2. Specify a policy statement to enable the group to obtain the auto-generated Object Storage namespace string of the tenancy (required to log in to Oracle Cloud Infrastructure Registry):

   ```
   Allow group <group-name> to read objectstorage-namespaces in tenancy
   ```

   where `<group-name>` is the name of the group to which users using Oracle Functions belong.

   For example:

   ```
   Allow group acme-functions-developers to read objectstorage-namespaces in tenancy
   ```

   The above policy statement also provides access to function logs stored in a storage bucket in Oracle Cloud Infrastructure Object Storage (see Storing and Viewing Function Logs on page 2078).

3. Specify a policy statement to give the group access to repositories in Oracle Cloud Infrastructure Registry:

   ```
   Allow group <group-name> to manage repos in tenancy
   ```

   where `<group-name>` is the name of the group to which users using Oracle Functions belong.

   For example:

   ```
   Allow group acme-functions-developers to manage repos in tenancy
   ```

   The above policy statement gives the group permission to manage all repositories in the tenancy. If you consider this to be too permissive, then you can restrict the repositories to which the group has access by including a where clause in the manage repos statement. Note that if you do include a where clause, you must also include a second statement in the policy to enable the group to inspect all repositories in the tenancy (when using the Console).

   For example, the following policy statements restrict the group to accessing only repositories with names that start 'acme-web-app', but also enables the group to inspect all repositories in the tenancy:

   ```
   Allow group acme-functions-developers to inspect repos in tenancy
   Allow group acme-functions-developers to manage repos in tenancy where all {target.repo.name=/acme-web-app*/ }
   ```

4. Click Create.

Create a Policy to Give Oracle Functions Users Access to Function-Related Resources

When Oracle Functions users create functions and applications, they have to specify a compartment for those function-related resources (including for metrics emitted by Oracle Functions). Users can only specify a compartment that the groups to which they belong have been granted access. To enable users to specify a compartment, you must create an identity policy to grant the groups access to that compartment.
To create a policy to give Oracle Functions users access to function-related resources in the compartment that will own those resources:

1. Log in to the Console as a tenancy administrator and create a new policy in the compartment that will own Oracle Functions resources:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
   b. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acme-functions-developers-manage-access).

2. Specify a policy statement to give the group access to all function-related resources in the compartment:

   Allow group <group-name> to manage functions-family in compartment <compartment-name>

   For example:

   Allow group acme-functions-developers to manage functions-family in compartment acme-functions-compartment

3. Specify a second policy statement to give the group access to metrics emitted by Oracle Functions:

   Allow group <group-name> to read metrics in compartment <compartment-name>

   For example:

   Allow group acme-functions-developers to read metrics in compartment acme-functions-compartment

4. Click Create.

Create a Policy to Give Oracle Functions Users Access to Logging Resources

When Oracle Functions users define an application, they can enable logging to store and view function logs in the Oracle Cloud Infrastructure Logging service. Users can only view logs that the groups to which they belong have been granted access. To enable users to store and view function logs in the Oracle Cloud Infrastructure Logging service, you must create an identity policy to grant the groups access to logging resources.

To create a policy to enable Oracle Functions users to store and view function logs in the Oracle Cloud Infrastructure Logging service:

1. Log in to the Console as a tenancy administrator and create a new policy in the tenancy:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
   b. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acme-functions-developers-logging-access).

2. Specify a policy statement to give the group read access to all logging resources in the tenancy:

   Allow group <group-name> to read logging-family in tenancy

   For example:

   Allow group acme-functions-developers to read logging-family in tenancy
3. Specify a policy statement to give the group full access to logging resources in the compartment that will own logging resources:

```
Allow group <group-name> to manage logging-family in compartment <compartment-name>
```

For example:

```
Allow group acme-functions-developers to manage logging-family in compartment acme-functions-compartment
```

4. Click Create.

**Create a Policy to Give Oracle Functions Users Access to Network Resources**

When Oracle Functions users create a function or application, they have to specify a VCN and a subnet in which to create them. Users can only specify VCNs and subnets in compartments that the groups to which they belong have been granted access. To enable users to specify a VCN and subnet, you must create an identity policy to grant the groups access to the compartment.

To create a policy to give Oracle Functions users access to network resources:

1. Log in to the Console as a tenancy administrator and create a new policy in the compartment that will own network resources:
   
a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
   
b. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acme-functions-developers-manage-network-access).

2. Specify a policy statement to give the group access to the network resources in the compartment:

```
Allow group <group-name> to use virtual-network-family in compartment <compartment-name>
```

For example:

```
Allow group acme-functions-developers to use virtual-network-family in compartment acme-network
```

3. Click Create.

**Configuring Your Client Environment for Function Development**

Before you can start using Oracle Functions to create and deploy functions, you have to set up your client environment for function development. Note that prior to setting up your client environment, you must already have set up your tenancy (see Configuring Your Tenancy for Function Development on page 2038).

**Different Options for Function Development Environments**

When setting up your Oracle Functions development environment, you have different options:

- **Option 1: Setting up Cloud Shell. (Recommended)** For users trying out Oracle Functions for the first time, this is the recommended way to get started quickly. By copying and pasting a few commands from the Console into the Cloud Shell window, you can set up an Oracle Functions development environment in just a few minutes.

  This option enables you to experiment creating, deploying, and invoking new functions. You can also explore Oracle Functions using the samples on Git Hub (see Oracle Functions Samples). If you want to set up Cloud Shell as your Oracle Functions development environment, see the instructions in the Oracle Functions on Cloud Shell Quick Start Guide.
Functions

- **Option 2: Setting up a local machine.** For most users (especially Mac and Linux users), this will be the way to work with Oracle Functions. If you set up a local machine, you'll have to specify `--provider oracle` when you create a new Fn Project CLI context.

  This option enables Oracle Functions to perform authentication and authorization using Oracle Cloud Infrastructure request signing, private keys, user groups, and policies that grant permissions to those user groups.

  This documentation assumes you want to set up a local machine as your client environment, and provides instructions accordingly (see Setting up a Local Machine as a Development Environment on page 2046). Instructions for setting up a local machine are also included in the Oracle Functions in a Local Dev Environment Quick Start Guide.

- **Option 3: Setting up an Oracle Cloud Infrastructure compute instance.** For some users, this will be more convenient than setting up a local machine. If you set up an Oracle Cloud Infrastructure compute instance, you'll have to specify `--provider oracle-ip` when you create a new Fn Project CLI context.

  This option enables Oracle Functions to perform authentication and authorization using instance OCIDs, dynamic groups, and policies granting permissions to those dynamic groups. This approach removes the requirement for users to manage private keys. Note that to set up an Oracle Functions development environment on an Oracle Cloud Infrastructure compute instance, you must:
  
  - have permission to create dynamic groups
  - create a new dynamic group that includes the compute instance's OCID
  - create a policy to give the new dynamic group access to function resources, network resources, and Oracle Cloud Infrastructure Registry
  - specify `--provider oracle-ip` when you create a new Fn Project CLI context

  If you want to set up an Oracle Cloud Infrastructure compute instance as your Oracle Functions development environment, see the instructions in the Oracle Functions on an OCI Compute Instance Quick Start Guide.

### Setting up a Local Machine as a Development Environment

To set up a local machine as your client environment for function development, you have to complete the following tasks in the order shown in this checklist:

<table>
<thead>
<tr>
<th>Task #</th>
<th>Development Environment Configuration Task</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions on page 2047</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3. Create and Configure a Copy of oci-curl on page 2050</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4. Install Docker for Use with Oracle Functions on page 2052</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5. Install the Fn Project CLI on page 2053</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7. Set the Context for the Fn Project CLI Using the oracle.profile Parameter on page 2055</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8. Generate an Auth Token to Enable Login to Oracle Cloud Infrastructure Registry on page 2056</td>
<td></td>
</tr>
</tbody>
</table>
Click each of the links in the checklist in turn, and follow the instructions.

When you have completed all of the development environment configuration tasks, confirm your configuration is correct (see Verifying Your Configuration for Function Development on page 2058).

1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions

Before using Oracle Functions, you have to set up an Oracle Cloud Infrastructure API signing key.

The instructions in this topic assume:

- you are using Linux
- you are following Oracle's recommendation to provide a passphrase to encrypt the private key

For more information and other options, see Required Keys and OCIDs on page 4179.

The instructions below describe how to create a new ~/.oci directory, how to generate a new private key file and public key file in that ~/.oci directory, how to upload the public key to Oracle Cloud Infrastructure to create a new API signing key, and how to obtain a fingerprint for the public API key. Be aware that instructions and examples elsewhere in this documentation assume the ~/.oci directory exists and contains the private and public key files.

If your user account already has an API signing key, create the ~/.oci directory if it doesn't exist, and then go straight to 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049.

If your user account doesn't already have an API signing key, follow the steps below, but note the following:

- If the ~/.oci directory doesn't exist, create it.
- If the ~/.oci directory already exists, go straight to the step below that instructs you to generate a private key file.
- If the ~/.oci directory already exists and already contains a private key file and public key file, and you know the passphrase that was used to encrypt the existing private key file, there's no need to create new private and public key files. Instead, go straight to the step below that instructs you to create a new API signing key and upload the public key value to Oracle Cloud Infrastructure to obtain a fingerprint.
- If you already have a private key file and public key file but they are not in the ~/.oci directory, and you know the passphrase that was used to encrypt the existing private key file, there's no need to create new private and public key files. Having created the ~/.oci directory if it doesn't exist, go straight to the step below that instructs you to create a new API signing key and upload the public key value to Oracle Cloud Infrastructure to obtain a fingerprint.

To set up an API signing key:

1. Log in to your development environment as a functions developer.
2. In a terminal window, confirm that the ~/.oci directory does not already exist. For example, by entering:

   ```bash
   ls ~/.oci
   ```

3. Assuming the ~/.oci directory does not already exist, create it. For example, by entering:

   ```bash
   mkdir ~/.oci
   ```
4. Generate a private key encrypted with a passphrase that you provide by entering:

```bash
openssl genrsa -out ~/.oci/<private-key-file-name>.pem -aes128 2048
```

where `<private-key-file-name>` is a name of your choice for the private key file (for example, `john_api_key_private.pem`).

For example:

```bash
openssl genrsa -out ~/.oci/john_api_key_private.pem -aes128 2048
```

The output from the above command shows the status of the private key generation operation, and prompts you for a passphrase:

```bash
Generating RSA private key, 2048 bit long modulus
....+++ .................................................................+++ 
```

```bash
e is 65537 (0x10001) 
```

```bash
Enter pass phrase for /Users/johndoe/.oci/john_api_key_private.pem: 
```

5. When prompted, enter a passphrase to encrypt the private key file. Be sure to make a note of the passphrase you enter, as you will need it later.

6. When prompted, re-enter the passphrase to confirm it.

7. Confirm that the private key file has been created in the directory you specified. For example, by entering:

```bash
ls -l ~/.oci/john_api_key_private.pem
```

The output from the above command confirms the creation of the private key file.

```bash
-rw-r--r-- 1 johndoe staff 1766 Jul 14 00:24 /Users/johndoe/.oci/john_api_key_private.pem
```

8. Change permissions on the file to ensure that only you can read it. For example, by entering:

```bash
chmod go-rwx ~/.oci/john_api_key_private.pem
```

9. Generate a public key (in the same location as the private key file) by entering:

```bash
openssl rsa -pubout -in ~/.oci/<private-key-file-name>.pem -out ~/.oci/<public-key-file-name>.pem
```

where:

- `<private-key-file-name>` is what you specified earlier as the name of the private key file (for example, `john_api_key_private.pem`)
- `<public-key-file-name>` is a name of your choice for the public key file (for example, `john_api_key_public.pem`)

For example:

```bash
openssl rsa -pubout -in ~/.oci/john_api_key_private.pem -out ~/.oci/john_api_key_public.pem
```

The output from the above command shows the status of the public key generation operation, and prompts you for a passphrase:

```bash
Enter pass phrase for /Users/johndoe/.oci/john_api_key_private.pem: 
```

10. When prompted, enter the same passphrase you previously entered to encrypt the private key file.
11. Confirm that the public key file has been created in the directory you specified. For example, by entering:

```
ls -l ~/.oci/
```

The output from the above command confirms the creation of the public key file.

```
-rw------- 1 johndoe staff 1766 Jul 14 00:24 john_api_key_private.pem
-rw-r----- 1 johndoe staff 451 Jul 14 00:55 john_api_key_public.pem
```

12. Copy the contents of the public key file you just created. For example, by entering:

```
cat ~/.oci/john_api_key_public.pem | pbcopy
```

13. Having created the API key pair, upload the public key value to Oracle Cloud Infrastructure:

   a. Log in to the Console as the Oracle Cloud Infrastructure user who will be using Oracle Functions to create and deploy functions.
   
   b. In the top-right corner of the Console, open the Profile menu (👤) and then click User Settings to view the details.
   
   c. On the API Keys page, click Add Public Key.
   
   d. Paste the public key's value into the window and click Add.
   
   e. (Optional) Note the fingerprint value. You'll use the fingerprint in a subsequent configuration task, so you might want to copy it to a convenient and secure location.

When you have completed the steps in this topic, go on to 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049.

2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File

Before using Oracle Functions, you must have an Oracle Cloud Infrastructure CLI configuration file that contains the credentials of the user account that you will be using to create and deploy functions. These user account credentials are referred to as a 'profile'.

By default, the Oracle Cloud Infrastructure CLI configuration file is located at `~/.oci/config`. You might already have a configuration file as a result of installing the Oracle Cloud Infrastructure CLI. However, you don't need to have installed the Oracle Cloud Infrastructure CLI in order to use Oracle Functions.

The Oracle Cloud Infrastructure CLI configuration file can contain several profiles. If you already have a configuration file containing one or more profiles, you have to add a new profile to the existing file for the Oracle Cloud Infrastructure user who will be using Oracle Functions to create and deploy functions.

The instructions in this topic assume:

- you are using Linux
- you have already completed the steps in 1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions on page 2047

To create a profile in the Oracle Cloud Infrastructure CLI configuration file for the user account that you will be using to create and deploy functions:

1. Log in to your development environment as a functions developer.
2. In a terminal window, confirm the contents of the `~/.oci` directory. For example, by entering:

```
ls -l ~/.oci/
```

The output from the above command shows the contents of the `~/.oci` directory:

```
-rw------- 1 johndoe staff 1766 Jul 14 00:24 john_api_key_private.pem
```
3. Do one of the following, depending on whether the ~/.oci directory already contains a file called config:
   • If the ~/.oci directory already contains a file called config, open the file in a text editor.
   • If the ~/.oci directory doesn't yet contain a file called config, create the file and open it in a text editor. For example, by entering:

     vim ~/.oci/config

4. Add a new profile to the ~/.oci/config file as follows:

   [<profile-name>]
   user=<user-ocid>
   fingerprint=<public-key-fingerprint>
   key_file=<full-path-to-private-key-pem-file>
   tenancy=<tenancy-ocid>
   region=<region-identifier>
   pass_phrase=<passphrase>

where:

   • <profile-name> is a name of your choosing for the profile.
   • <user-ocid> is the OCID of the Oracle Cloud Infrastructure user account you will be using to create and deploy functions. See Where to Get the Tenancy's OCID and User's OCID on page 4184.
   • <public-key-fingerprint> is the fingerprint of the public API key value that you uploaded in the Console in 1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions on page 2047.
   • <full-path-to-private-key-pem-file> is the full path to the private key file that you created in 1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions on page 2047.
   • <tenancy-ocid> is the OCID of the tenancy in which you will be creating and deploying functions. See Where to Get the Tenancy's OCID and User's OCID on page 4184.
   • <region-identifier> is the identifier of the Oracle Cloud Infrastructure region in which you will be creating and deploying functions. For example, us-phoenix-1. See Availability by Region on page 2038.
   • <passphrase> is the passphrase you entered in 1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions on page 2047).

For example:

   [john-oci-profile]
   user=ocid1.user.oc1..aaaaaaaas...7ap
   key_file=~/.oci/john_api_key_private.pem
   tenancy=ocid1.tenancy.oc1..aaaaaaap...keq
   region=us-phoenix-1
   pass_phrase=<your-passphrase>

When you have completed the steps in this topic, go on to 3. Create and Configure a Copy of oci-curl on page 2050.

**3. Create and Configure a Copy of oci-curl**

You can use a bash script provided by Oracle (commonly referred to as oci-curl) to invoke a function. The oci-curl script creates a signed request, based on credentials you provide in the body of the script. For more information about oci-curl, see Request Signatures - Bash.

To use oci-curl to invoke a function, you must provide the credentials of an Oracle Cloud Infrastructure user that has been granted access to resources in the same tenancy and belonging to the same compartment as the function (see Create Policies to Control Access to Network and Function-Related Resources on page 2041).
Typically you'll want to invoke a function as the functions developer that's configured for your development environment. The instructions below assume that is the case.

The instructions in this topic assume you have already completed the steps in 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049.

To create and configure a copy of oci-curl:

1. Log in to your development environment as a functions developer.
2. Create a copy of the oci-curl script file in your development environment and add your credentials to the file as follows:
   a. In a browser navigate to https://docs.cloud.oracle.com/iaas/Content/Resources/Assets/signing_sample_bash.txt to see the oci-curl code as raw text.
   b. Select all the text and copy it.
   c. In a text editor, open a new file in a convenient location. For example, in a terminal window, you might create a new subdirectory in your home directory and open a new file in that directory by entering:

```
$ cd ~
$ mkdir oci-curl
$ vim ~/oci-curl/oci-curl.sh
```

The name and location of the new file is up to you, but the following instructions assume `~/oci-curl/oci-curl.sh`.

   d. Paste the oci-curl script code that you copied earlier into the new file.
   e. Save the file but leave it open so you can add your credentials.
3. Replace the sample credentials in the oci-curl.sh file with those of the user account that you want to invoke functions, as follows:
   a. Locate the following lines in the oci-curl.sh file that contain sample credential values:

```
# TODO: update these values to your own
local tenancyId="ocid1.tenancy.oc1..aaaaaaaab______dsq";
local authUserId="ocid1.user.oc1..aaaaaaaas______o3r";
local privateKeyPath="/Users/someuser/.oci/oci_api_key.pem";
```

   Tip:

Typically you'll want to invoke a function as the functions developer that's configured for your development environment. If that's the case,
open the ~/.oci/config file so you can easily copy values from there to replace the sample values in the oci-curl.sh file.

b. Change the value of the tenancyId parameter in the oci-curl.sh file by replacing the sample value in quotes with the OCID of the tenancy in which the function has been deployed. For example:

```
local tenancyId="ocid1.tenancy.oc1..aaaaaaaap______keq";
```

c. Change the value of the authUserID parameter in the oci-curl.sh file by replacing the sample value in quotes with the OCID of the user account that you want to run the function. The user account must have access to resources in the same tenancy and belonging to the same compartment as the function. For example:

```
local authUserId="ocid1.user.oc1..aaaaaas______7ap";
```

d. Change the value of the keyFingerprint parameter in the oci-curl.sh file by replacing the sample value in quotes with the fingerprint of the user's public key uploaded to Oracle Cloud Infrastructure. For example:

```
```

e. Change the value of the privateKeyPath parameter in the oci-curl.sh file by replacing the sample value in quotes with the full path to the private key file that is paired with the public key for which you provided the fingerprint. For example:

```
local privateKeyPath="/Users/johndoe/.oci/john_api_key_private.pem";
```

4. Save and close the oci-curl.sh file.

**Note:**

When you've deployed functions to Oracle Functions and you want to use oci-curl to invoke them, you will first have to run the `source` command to set up the current shell environment for oci-curl. See Invoking Functions on page 2071.

When you have completed the steps in this topic, go on to 4. Install Docker for Use with Oracle Functions on page 2052.

4. **Install Docker for Use with Oracle Functions**

Before using Oracle Functions, a version of Docker supported by Fn Project must be installed in your development environment. If Docker is not already installed, or the installed version of Docker is not supported, you'll have to install or upgrade Docker.

The instructions in this topic assume you have already completed the steps in 3. Create and Configure a Copy of oci-curl on page 2050.

To confirm that a supported version of Docker is installed in your development environment:

1. Log in to your development environment as a functions developer.
2. In a terminal window, confirm that Docker is installed by entering:

```
docker version
```

3. Do one of the following, depending on the message you see:

- If you see an error message indicating that Docker is not installed, you have to install Docker before proceeding to the next step. See the Docker documentation for information about installing Docker on your platform. If your platform is Oracle Linux, see Oracle Container Runtime for Docker User's Guide.
- If you see a message indicating the version of Docker that's installed, go to the next step.
4. Assuming Docker is installed, go to the Fn Project home page on GitHub to confirm that the installed version of Docker is at least the minimum version specified in the Pre-requisites section. If the installed version of Docker is not supported by Fn Project, you have to upgrade the version of Docker before proceeding. See the Docker documentation for information about upgrading Docker on your platform. If your platform is Oracle Linux, see Oracle Container Runtime for Docker User's Guide.

When you have completed the steps in this topic, go on to 5. Install the Fn Project CLI on page 2053.

5. Install the Fn Project CLI

Before using Oracle Functions, the Fn Project CLI must be installed in your development environment. You can install the Fn Project CLI in a number of different ways according to your environment. The instructions in this topic assume you have already completed the steps in 4. Install Docker for Use with Oracle Functions on page 2052.

To install the Fn Project CLI:

1. Log in to your development environment as a functions developer.
2. Open the README.md file in the fnproject/cli repository on GitHub and follow the appropriate instructions for installing the Fn Project CLI in your development environment. As a convenient overview, the instructions are summarized below:
   • In a MacOS environment using Homebrew, install the Fn Project CLI by entering:
     `brew install fn`
   • In a Linux or MacOS environment, install the Fn Project CLI by entering:
     `curl -LSs https://raw.githubusercontent.com/fnproject/cli/master/install | sh`
     If prompted for a password, enter the superuser's password.
   • In a Linux, MacOS, or Windows environment, install the Fn Project CLI by downloading the binary from the Releases page and running it.
3. In a terminal window, confirm that the CLI has been installed by entering:
   `fn version`

Assuming the Fn Project CLI has been installed correctly, you'll see a message indicating the version of the CLI that has been installed.

When you have completed the steps in this topic, go on to 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053.

6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure

Before using Oracle Functions, you have to configure the Fn Project CLI to connect to your Oracle Cloud Infrastructure tenancy. When the Fn Project CLI is initially installed, it's configured for a local development 'context'. To configure Fn Project CLI to connect to your Oracle Cloud Infrastructure tenancy instead, you have to create a new context. The context specifies Oracle Functions endpoints, the OCID of the compartment to which deployed functions will belong, and the address of the Docker registry to and from which to push and pull images.

You can define multiple contexts, each stored in a different context file in .yaml format. By default, the individual context files are stored in the `~/.fn/contexts` directory. The `~/.fn/config.yaml` file specifies which context file Fn Project uses.

To create a new context, you can create a new context file manually and edit the `~/.fn/config.yaml` file by hand to point to that file. Alternatively, you can use the Fn Project CLI to interactively create the new context file and instruct the Fn Project CLI to start using that file, as described below.
The instructions in this topic assume you have already completed the steps in 5. Install the Fn Project CLI on page 2053.

To create a new context file using the Fn Project CLI:

1. Log in to your development environment as a functions developer.
2. In a terminal window, create the new Fn Project CLI context for Oracle Cloud Infrastructure by entering:

   `fn create context <my-context> --provider oracle`

   where `<my-context>` is a name of your choosing. For example:

   `fn create context johns-oci-context --provider oracle`

3. Specify that the Fn Project CLI is to use the new context by entering:

   `fn use context <my-context>`

   where `<my-context>` is the name you specified in the previous step. For example:

   `fn use context johns-oci-context`

4. Configure the new context with the OCID of the compartment that you want to own the deployed functions (you might have created a new compartment specifically for this purpose, see Create Compartments to Own Network Resources and Oracle Functions Resources in the Tenancy, if they don't exist already on page 2039) by entering:

   `fn update context oracle.compartment-id <compartment-ocid>`

   For example:

   `fn update context oracle.compartment-id ocid1.compartment.oc1..aaaaaaaarvdfa72n...`

5. Configure the new context with the api-url endpoint to use when calling the API by entering:

   `fn update context api-url <api-endpoint>`

   where `<api-endpoint>` is one of the endpoints in the list of Functions endpoints in Functions API, in the format https://functions.<region-identifier>.oci.oraclecloud.com. The `<region-identifier>` in `<api-endpoint>` is the identifier of the Oracle Cloud Infrastructure region in which you'll be creating and deploying functions. For example, us-phoenix-1.

   For example:

   `fn update context api-url https://functions.us-phoenix-1.oci.oraclecloud.com`
6. Configure the new context with the address of the Docker registry that you want to use with Oracle Functions by entering:

```
fn update context registry <region-key>.ocir.io/<tenancy-namespace>/<repo-name>
```

where:

- `<region-key>` is the key of the Oracle Cloud Infrastructure Registry region. For example, `phx` for Phoenix. See Availability by Region on page 3508.
  
  Oracle recommends that the Docker registry you specify is in the same region as the subnet on which you intend functions to run.

- `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy in which to create repositories (as shown on the Tenancy Information page). For example, the namespace of the `acme-dev` tenancy might be `ansh81vru1zp`. Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, `acme-dev`).

- `<repo-name>` is a repository name to pre-pend to the names of functions that you deploy.

  For example:

```
fn update context registry phx.ocir.io/ansh81vru1zp/acme-repo
```

7. (Optional) Verify the Fn Project CLI context you've created by viewing the context file. For example, by entering:

```
more ~/.fn/contexts/johns-oci-context.yaml
```

The context file contains:

```
api-url: https://functions.us-phoenix-1.oci.oraclecloud.com
provider: oracle
registry: phx.ocir.io/ansh81vru1zp/acme-repo
```

When you have completed the steps in this topic, go on to 7. Set the Context for the Fn Project CLI Using the oracle.profile Parameter on page 2055.

**7. Set the Context for the Fn Project CLI Using the oracle.profile Parameter**

Before using Oracle Functions, you have to configure the Fn Project CLI to use the new profile you added to the Oracle Cloud Infrastructure CLI configuration file `~/.oci/config` (see 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049). The profile you added contains the credentials of the user account you'll be using to create and deploy functions.

Note that unless you specify otherwise, the Fn Project CLI will attempt to use a profile in the `~/.oci/config` file named `default`.

The instructions in this topic assume you have already completed the steps in 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053.

To configure the Fn Project CLI to use the profile you've created for use with Oracle Functions:

1. Log in to your development environment as a functions developer.

2. In a terminal window, configure the Fn Project CLI context with the name of the profile you've created for use with Oracle Functions by entering:

```
fn update context oracle.profile <profile-name>
```

For example:

```
fn update context oracle.profile john-oci-profile
```
When you have completed the steps in this topic, go on to 8. Generate an Auth Token to Enable Login to Oracle Cloud Infrastructure Registry on page 2056.

8. Generate an Auth Token to Enable Login to Oracle Cloud Infrastructure Registry

Before using Oracle Functions, the user account you'll be using to create and deploy functions must have an Oracle Cloud Infrastructure auth token. You use the auth token as the password when logging Docker in to Oracle Cloud Infrastructure Registry

The instructions in this topic assume you have already completed the steps in 7. Set the Context for the Fn Project CLI Using the oracle.profile Parameter on page 2055.

If the user account already has an auth token, go straight on to 9. Start Docker on page 2056. Otherwise, if the user account does not have an auth token, generate an auth token now.

To generate an auth token for the user account you'll be using to create and deploy functions:

1. Log in to the Console as a functions developer.
2. In the top-right corner of the Console, open the Profile menu ( ) and then click User Settings to view the details.
3. On the Auth Tokens page, click Generate Token.
4. In the Generate Token dialog:
   a. Enter a meaningful description for the auth token. For example, John's auth token for use with Oracle Functions. Avoid entering confidential information.
   b. Click Generate Token. The new auth token is displayed. For example, 6<!)N___________6MqX.
5. Copy the auth token immediately to a secure location from where you can retrieve it later, because you won't see the auth token again in the Console.
6. Close the Generate Token dialog.

When you have completed the steps in this topic, go on to 9. Start Docker on page 2056.

9. Start Docker

Before using Oracle Functions, Docker must be running in your development environment. If it is not running, you must start Docker before proceeding.

The instructions in this topic assume you have already completed the steps in 8. Generate an Auth Token to Enable Login to Oracle Cloud Infrastructure Registry on page 2056.

To verify that Docker is running:

1. Log in to your development environment as a functions developer.
2. In a terminal window, launch the standard hello-world Docker image as a container to confirm that Docker is running by entering:
   
   docker run hello-world

3. Do one of the following, depending on the message you see:
   - If you see an error message indicating that Docker is not running, you have to start the Docker daemon before proceeding. See the Docker documentation for information about starting Docker on your platform.
   - If you see an error message indicating that the network timed out while trying to connect and advising you to check your internet connection or whether you are behind a proxy, your development environment might be behind a corporate proxy server or firewall. In which case, you will probably need to set the http_proxy, https_proxy, and no_proxy environment variables. Ask your network administrator for advice.
   - If you see a message like the one shown below, Docker is already running and you can proceed:

```
Hello from Docker.
This message shows that your installation appears to be working correctly.
```
When you have completed the steps in this topic, go on to 10. Log in to Oracle Cloud Infrastructure Registry on page 2057.

### 10. Log in to Oracle Cloud Infrastructure Registry

Before using Oracle Functions, you have to log Docker in to the Docker registry in which you are going to store your functions as Docker images. This is the Docker registry specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

You can store functions in public and private repositories in Oracle Cloud Infrastructure Registry, an Oracle-managed registry built on top of Oracle Cloud Infrastructure.

When you log Docker into a Docker registry, you have to provide the appropriate authentication details. For example, in the case of Oracle Cloud Infrastructure Registry, you have to provide the tenancy Object Storage namespace, the user name, and the user's auth token.

The instructions in this topic assume you have already completed the steps in 9. Start Docker on page 2056.

To log Docker into Oracle Cloud Infrastructure Registry:

1. **Log in to your development environment as a functions developer.**
2. **In a terminal window, log in to Oracle Cloud Infrastructure Registry by entering:**
   ```
docker login <region-key>.ocir.io
   ```
   where `<region-key>` is the key for the Oracle Cloud Infrastructure Registry region specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053). For example, `phx` for Phoenix. See Availability by Region on page 3508.
   
   For example:
   ```
docker login phx.ocir.io
   ```
3. **When prompted for **Username**, enter the name of the user you will be using with Oracle Functions to create and deploy functions, in the format:**
   ```
   <tenancy-namespace>/<username>
   ```
   where `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy in which to create repositories (as shown on the **Tenancy Information** page). For example, `ansh81vrulzp/jdoe@acme.com`.
   
   Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, `acme-dev`).
   
   If your tenancy is federated with Oracle Identity Cloud Service, use the format `<tenancy-namespace>/oracleidentitycloudservice/<username>`.
   
   You must have already generated an Oracle Cloud Infrastructure auth token for the user you specify (see 8. Generate an Auth Token to Enable Login to Oracle Cloud Infrastructure Registry on page 2056).
4. **When prompted for **Password**, enter the user's Oracle Cloud Infrastructure auth token.** Having entered the password, Docker might warn you that the password is stored unencrypted in the Docker configuration file. The warning includes a link to the Docker documentation where you can find out how to configure a credential helper. Oracle recommends you review the information in the Docker documentation and consider using an external credentials store for increased security.

When you have completed the steps in this topic, you have completed the configuration tasks for your client environment. Go on to Verifying Your Configuration for Function Development on page 2058 to confirm that the Fn Project CLI can communicate with the API endpoint.
Verifying Your Configuration for Function Development

Before using Oracle Functions, it's a good idea to confirm that you have successfully completed:

- the tasks for Configuring Your Tenancy for Function Development on page 2038
- the tasks for Configuring Your Client Environment for Function Development on page 2045

If you have successfully completed the configuration tasks, the Fn Project CLI will be able to communicate with the API endpoint.

To confirm that the Fn Project CLI can communicate with the API endpoint:

1. Log in to your development environment as a functions developer.
2. In a terminal window, try and view a list of applications that have been defined in Oracle Functions by entering:

   ```
   fn list apps
   ```

3. If you see either of the following, you can proceed to create and deploy functions because your system is configured correctly:
   - A message indicating that no applications have been found, which is expected if this is the first time the tenancy has been configured for Oracle Functions.
   - A list of applications that have already been created, which is expected if other users are already using the tenancy for functions development.

4. If you see an error message, it's likely that the Fn Project CLI cannot communicate with the API endpoint due to some incorrect configuration. Do the following:
   - Review the configuration tasks to confirm you completed them as instructed (see Configuring Your Tenancy for Function Development on page 2038 and Configuring Your Client Environment for Function Development on page 2045).
   - Review the solutions for common problems (see Troubleshooting Oracle Functions on page 2097).

Using the Fn Project CLI with Oracle Functions

Oracle Functions is powered by the Fn Project open source engine. As a result, you can use the Fn Project CLI to perform create, read, update, and delete operations on Oracle Functions.

To enable you to use the Fn Project CLI with Oracle Functions, you perform a number of preparatory tasks. See Configuring Your Client Environment for Function Development on page 2045.

Most Fn Project CLI commands have a similar syntax:

```
fn [global options] <command> [command options] [subcommands] [arguments]
```

For example, to:

- list all the available applications, use the command:

  ```
  fn list apps
  ```

- create an application, use a command like:

  ```
  fn create app acmeapp --annotation oracle.com/oci/subnetIds='["ocid1.subnet.oc1.phx.aaaaaaaacnh..."]'
  ```

- invoke a function, use a command like:

  ```
  fn invoke helloworld-app helloworld-func
  ```

- change the profile that the Fn Project CLI uses for its context, use a command like:

  ```
  fn update context oracle.profile john-oci-profile
  ```
To see a complete list of Fn Project CLI commands, you can:

- Log in to your development environment as a functions developer and enter `fn --help` or `fn -h` in a terminal window.
- In a web browser, go to the Fn Project CLI documentation.

To see detailed information about individual Fn Project CLI commands, you can:

- Log in to your development environment as a functions developer and enter `fn <command> [subcommand] --help` or `fn <command> [subcommand] -h` in a terminal window. For example:

```
fn create --help
```

```
fn update app -h
```

- In a web browser, go to the Fn Project CLI documentation and select the command from the list.

From time to time, new versions of the Fn Project CLI are released. To:

- See which version of the Fn Project CLI is currently installed and whether it is the most recent version, log in to your development environment as a functions developer and enter `fn version` in a terminal window. The Fn Project CLI version number is displayed. If a more recent version of the Fn Project CLI is available, the number of the latest available version is also displayed.
- Upgrade the Fn Project CLI to the most recent version, reinstall the Fn Project CLI by following the instructions in 5. Install the Fn Project CLI on page 2053.

### Creating, Deploying, and Invoking a HelloWorld Function

You can start off using Oracle Functions by using Fn Project CLI commands to:

- create a simple helloworld function written in java
- push the image to the Docker registry that's configured for Oracle Functions
- deploy the function to an application in Oracle Functions
- invoke the function

**Tip:**

If you aren't able to successfully complete one of the steps in this topic, review the solutions for common problems (see Troubleshooting Oracle Functions on page 2097).

To get started with Oracle Functions:

1. **Confirm that you have completed the prerequisite steps for using Oracle Functions, as described in Preparing for Oracle Functions on page 2038.** Specifically, that you have:
   - set up your tenancy (see Configuring Your Tenancy for Function Development on page 2038)
   - set up your development environment (see Configuring Your Client Environment for Function Development on page 2045)
2. Log in to the Console as a functions developer.
3. Use the Console to create a new application in Oracle Functions:
   
a. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.

b. Select the region you intend to use for Oracle Functions. Oracle recommends that you use the same region as the Docker registry specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

c. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

   The **Applications** page shows the applications already defined in the compartment.

d. Click **Create Application** and specify:
   
   • The name for the new application as helloworld-app.
   • The VCN and subnet (or subnets, up to a maximum of three) in which to run the function. For example, a VCN called acme-vcn-01 and a public subnet called Public Subnet IHsY:US-PHOENIX-AD-1. If a regional subnet has been defined, best practice is to select that subnet to make failover across availability domains simpler to implement. If a regional subnet has not been defined and you need to meet high availability requirements, select multiple subnets. Oracle recommends that subnets are in the same region as the Docker registry specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

   e. Click **Create**.

4. Log in to your development environment as a functions developer.

5. In a terminal window, create a helloworld java function by entering:

   ```
   fn init --runtime java helloworld-func
   ```

   A directory called helloworld-func is created, containing:
   
   • A function definition file called func.yaml, containing the minimum amount of information required to build and run the function. See the Fn Project documentation to find out about the additional parameters you can include in a func.yaml file.
   • A /src directory containing source files and directories for the helloworld function (including /src/main/java/com/example/fn/HelloFunction.java).
   • A Maven configuration file called pom.xml that specifies the project artifacts and dependencies required to compile the function from the source files.

6. Change directory to the newly created helloworld-func directory.

7. Enter the following single Fn Project command to build the function and its dependencies as a Docker image called helloworld-func, push the image to the specified Docker registry, and deploy the function to Oracle Functions in the helloworld-app:

   ```
   fn -v deploy --app helloworld-app
   ```

   The -v option simply shows more detail about what Fn Project commands are doing (see Using the Fn Project CLI with Oracle Functions on page 2058).
8. (Optional) Assuming the specified Docker registry is Oracle Cloud Infrastructure Registry, use the Console to confirm that the helloworld-func image has been pushed to Oracle Cloud Infrastructure Registry successfully:
   a. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Container Registry**.
   b. Choose the registry’s region.
      You see all the repositories in the registry to which you have access. The image you pushed is in a new repository with a name constructed from:
      - the repository name in the address of the Docker registry in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053)
      - the name of the helloworld-func image
      For example, the new repository might be called `acme-repo/helloworld-func`.
   c. Click the name of the new repository. You see details of the helloworld-func image that's been pushed to Oracle Cloud Infrastructure Registry.

9. (Optional) Use the Console to confirm that the function has been deployed to Oracle Functions successfully:
   a. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.
   b. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
      The **Applications** page shows that an application called helloworld-app has been created.
   c. Click the helloworld-app application to see the functions within it.
      The **Functions** page shows that the helloworld-func function has been deployed to Oracle Functions.

10. In a terminal window, invoke the helloworld-func function by entering:
    ```
    fn invoke helloworld-app helloworld-func
    ```
    The 'Hello World !' message is displayed.

Congratulations! You've successfully created and deployed your first function to Oracle Functions!

**Creating Applications**

You can create applications in Oracle Functions in readiness for deploying functions. An application need not contain any functions.

You can create applications using the Console, the Fn Project CLI, and the API.

For more information about applications, see **Applications** on page 2034.

**Using the Console**

To create a new application in Oracle Functions using the Console:

1. Confirm that you have completed the prerequisite steps for using Oracle Functions, as described in **Preparing for Oracle Functions** on page 2038. Specifically, that you have:
   - set up your tenancy (see **Configuring Your Tenancy for Function Development** on page 2038)
   - set up your development environment (see **Configuring Your Client Environment for Function Development** on page 2045)
2. Log in to the Console as a functions developer.
3. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.
4. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
5. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

The Applications page shows the applications already defined in the compartment.

6. Click Create Application and specify:
   - A name for the new application (for example, acmeapp). Avoid entering confidential information.
   - The VCN and subnet (or subnets, up to a maximum of three) in which to run functions. For example, a VCN called acme-vcn-01 and a public subnet called Public Subnet IHsY:US-PHOENIX-AD-1). If a regional subnet has been defined, best practice is to select that subnet to make failover across availability domains simpler to implement. If a regional subnet has not been defined and you need to meet high availability requirements, select multiple subnets. Oracle recommends that the subnets are in the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

7. Click Create.

The new application appears in the list of applications.

Using Fn Project CLI Commands

To create a new application in Oracle Functions using the Fn Project CLI:

1. Log in to your development environment as a functions developer.
2. In a terminal window, create a new application by entering:

   ```
   fn create app <app-name> --annotation oracle.com/oci/subnetIds='["<subnet-ocid>"]'
   ```

   where:
   - `<app-name>` is the name of the new application. Avoid entering confidential information.
   - `<subnet-ocid>` is the OCID of the subnet (or subnets, up to a maximum of three) in which to run functions. If a regional subnet has been defined, best practice is to select that subnet to make failover across availability domains simpler to implement. If a regional subnet has not been defined and you need to meet high availability requirements, specify multiple subnets (enclose each OCID in double quotes separated by commas, in the format '"<subnet-ocid>"'). Oracle recommends that the subnets are in the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

   For example:

   ```
   fn create app acmeapp --annotation oracle.com/oci/subnetIds='["ocid1.subnet.oc1.phx.aaaaaacnh..."]'
   ```

   An application is created in Oracle Functions, in the tenancy and region implied by the subnet OCID and belonging to the compartment specified in the Fn Project CLI context file.

3. Verify that the new application has been created by entering:

   ```
   fn list apps
   ```

   For example:

   ```
   $ fn list apps
   acmeapp
   ```
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage applications:

- CreateApplication
- DeleteApplication
- GetApplication
- UpdateApplication

Creating and Deploying Functions

You use Fn Project CLI commands to create and deploy functions to Oracle Functions.

Tip:

If you aren't able to successfully complete one of the steps in this topic, review the solutions for common problems (see Troubleshooting Oracle Functions on page 2097).

Using Fn Project CLI Commands

To create and deploy a function to Oracle Functions using Fn Project CLI commands:

1. Confirm that you have completed the prerequisite steps for using Oracle Functions, as described in Preparing for Oracle Functions on page 2038. Specifically, that you have:
   - set up your tenancy (see Configuring Your Tenancy for Function Development on page 2038)
   - set up your development environment (see Configuring Your Client Environment for Function Development on page 2045)
2. If the application to which you want to add the function doesn't yet exist in Oracle Functions, create it now using the Fn Project CLI or the Console. For example, you might create a new application called acmeapp. See Creating Applications on page 2061.
3. Log in to your development environment as a functions developer.
4. In a terminal window, change directory to the directory containing the function code.
5. Initialize the function by entering:

```bash
fn init --runtime <runtime-language> <function-name>
```

where:

- `<runtime-language>` is one of the supported runtime languages (currently go, java, node, python, and ruby are supported)
- `<function-name>` is the name to use as the function name. If you don't specify a function name, the name of the current directory (in lower case) is used. Avoid entering confidential information.

For example:

```bash
fn init --runtime java acme-func
```

A directory is created with the function name you specified, containing:

- A function definition file called func.yaml, containing the minimum amount of information required to build and run the function. See the Fn Project documentation to find out about the additional parameters you can include in a func.yaml file.
- A `src` directory containing source files and directories.
- A Maven configuration file called pom.xml that specifies the project artifacts and dependencies required to compile the function from the source files.

Note that depending on the runtime language you specify, the `fn init` command might create an `/example` directory containing code for a helloworld application. As a matter of good practice, you'll probably want to delete the `/example` directory.

6. Change directory to the newly created directory.

7. Enter the following single Fn Project command to build the function and its dependencies as a Docker image, push the image to the specified Docker registry, and deploy the function to Oracle Functions:

```bash
fn -v deploy --app <app-name>
```

where `<app-name>` is the name of the application in Oracle Functions to which you want to add the function.

For example:

```bash
fn -v deploy --app acmeapp
```

The `-v` option simply shows more detail about what Fn Project commands are doing (see Using the Fn Project CLI with Oracle Functions on page 2058).

Note that you can build, push, and deploy the function using separate Fn Project commands, instead of the single `fn deploy` command.

8. (Optional) Assuming the specified Docker registry is Oracle Cloud Infrastructure Registry, use the Console to confirm that the image has been pushed to Oracle Cloud Infrastructure Registry successfully:

a. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.

b. Choose the registry's region.

You see all the repositories in the registry to which you have access. The image you pushed is in a new private repository with a name constructed from:

- the repository name in the address of the Docker registry in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053)
- the name of the image you pushed

For example, the new repository might be called `acme-repo/acme-func`.

c. Click the name of the new repository. You see details of the image that's been pushed to Oracle Cloud Infrastructure Registry.
9. (Optional) Use the Console to confirm that the function has been deployed to Oracle Functions successfully:

   a. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.

   b. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

      The **Applications** page shows the applications in the compartment, including the one you specified in the `fn deploy` command.

   c. Click the name of the application you specified in the `fn deploy` command to see the functions within it.

      The **Functions** page shows that the function has been deployed to Oracle Functions.

### Using Custom Dockerfiles

When you build or deploy a function with Oracle Functions, a Docker image is created and pushed to a Docker registry. As with any Docker image, the instructions to build the image are contained in a Dockerfile.

If the function is written in one of the languages supported by an Fn Project FDK (Functions Development Kit), Oracle Functions uses the `runtime:`, `build_image:`, and `run_image:` settings in a `func.yaml` file to determine the language (and therefore the build-time and run-time dependencies) to include in the Docker image. If you use the `fn init` command to initialize the function, a `func.yaml` file is created for you. For example, a `func.yaml` might look like:

```yaml
schema_version: 20180708
name: hello-java
version: 0.0.1
runtime: java
build_image: fnproject/fn-java-fdk-build:jdk11-1.0.116
run_image: fnproject/fn-java-fdk:jre11-1.0.116
cmd: com.example.fn.HelloFunction::handleRequest
```

When you build or deploy the function, Oracle Functions uses the settings in the `func.yaml` file to create a temporary Dockerfile containing the instructions from which to build the Docker image. For example, a temporary Dockerfile is shown below.

```bash
FROM fnproject/fn-java-fdk-build:jdk11-1.0.116 as build-stage
WORKDIR /function
ENV MAVEN_OPTS -Dhttp.proxyHost= -Dhttp.proxyPort= -Dhttps.proxyHost= -Dhttps.proxyPort= -Dhttp.nonProxyHosts= -Dmaven.repo.local=/usr/share/maven/ref/repository
ADD pom.xml /function/pom.xml
ADD src /function/src
RUN ["mvn", "package"]
FROM fnproject/fn-java-fdk:jre11-1.0.116
WORKDIR /function
COPY --from=build-stage /function/target/*.jar /function/app/
CMD ["com.example.fn.HelloFunction::handleRequest"]
```

Having created the Docker image, Oracle Functions deletes the temporary Dockerfile.

If you want more control over the Docker image that is created, you can modify the Dockerfile that Oracle Functions creates. Alternatively, you can create your own Dockerfile entirely from scratch. In both cases, the Dockerfile is referred to as a 'custom Dockerfile'. This workflow is sometimes referred to as Bring-Your-Own-Dockerfile, or BYOD.

When you build or deploy the function, Oracle Functions uses the instructions in the custom Dockerfile to build the Docker image.
To have Oracle Functions use a custom Dockerfile when building a Docker image:

1. Make a copy of the Dockerfile you want to use as a custom Dockerfile.
2. Save the new file to the directory containing the func.yaml file.
3. Give the new file the name Dockerfile.

Note that you must name the file Dockerfile.
4. Open the file named Dockerfile in an editor of your choice.

For example, the Dockerfile file might contain the following lines to install the Oracle Instant Client from an oraclelinux:7-slim base image:

```
FROM oraclelinux:7-slim
RUN yum -y install oracle-release-el7 oracle-nodejs-release-el7 && \
    yum-config-manager --disable ol7_developer_EPEL && \
    yum -y install oracle-instantclient19.3-basiclite nodejs && \
    rm -rf /var/cache/yum
WORKDIR /function
ADD . /function/
RUN npm install
CMD exec node func.js
```

5. Include the following lines in the file named Dockerfile (as described in Permissions Granted to Containers Running Functions on page 2094):

```
groupadd --gid 1000 fn && \
adduser --uid 1000 --gid fn fn
```

For example:

```
FROM oraclelinux:7-slim
RUN yum -y install oracle-release-el7 oracle-nodejs-release-el7 && \
    yum-config-manager --disable ol7_developer_EPEL && \
    yum -y install oracle-instantclient19.3-basiclite nodejs && \
    rm -rf /var/cache/yum && \
groupadd --gid 1000 fn && \
adduser --uid 1000 --gid fn fn
WORKDIR /function
ADD . /function/
RUN npm install
CMD exec node func.js
```

6. Save the file named Dockerfile. You can now use the Dockerfile file as a custom Dockerfile.
7. In the func.yaml file, change the value of the runtime: parameter to runtime: docker.

For example, if the func.yaml file contains runtime: java, change it to runtime: docker.
8. Use the fn build or fn deploy commands to build or deploy the function.

Oracle Functions uses the instructions in the custom Dockerfile (the file named Dockerfile) to build the Docker image for the function, and push it to the Docker registry.

**Creating Functions from Existing Docker Images**

You can create a new function definition in the Oracle Functions server in different ways:

- Using the Console or the Fn Project CLI command fn create function to create a new function based on an existing Docker image that has already been pushed to the Docker registry (as described in this topic).
• Using the single Fn Project CLI command `fn deploy` to build a new Docker image, push the image to the Docker registry, and create a new function based on the image in one step (as described in Creating and Deploying Functions on page 2063).
• Using the API (see CreateFunction).

When using the Console or the `fn create function` command to create a new function based on an existing Docker image, you specify function metadata to store in the Oracle Functions server. For example, the maximum length of time the function is allowed to execute for.

The existing image on which you base a new function must be suitable for use with Oracle Functions. Typically, to build and push a suitable image, you or somebody else will use Fn Project CLI commands and/or Docker CLI commands. For example, having written your function code and a `func.yaml` file containing function metadata (perhaps based on the template `helloworld` function and `func.yaml` created using `fn init`), you can:

• Use `fn build` to build a new Docker image from the function.
• Use `docker push` to push the image to the Docker registry.

With the image in the Docker registry, you can then use the Console to create a function based on the image, as described in this topic.

**Using the Console**

To use the Console to create a new function in the Oracle Functions server from an existing Docker image that has already been pushed to the Docker registry:

1. Log in to the Console as a functions developer.
2. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.
3. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
4. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

   The **Applications** page shows the applications defined in the compartment.
5. Click the name of the application in which you want to create the new function.
6. Click **Create Function** and specify:
   • **Name**: A name for the new function. Avoid entering confidential information.
   • **Image**: The existing image in the Oracle Cloud Infrastructure Registry in your currently selected region. You first select the image repository, and then the image version.
   • **Memory**: The maximum amount of memory the function can use during execution.
   • **Timeout**: The maximum amount of time the function will be allowed to run for.
   • **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click **Create** to create the new function in the Oracle Functions server.

The new function is shown in the Console, in the list of functions in the application you selected.

**Using Fn Project CLI Commands**

To use the Fn Project CLI to create a new function in the Oracle Functions server from an existing Docker image that has already been pushed to the Docker registry:

1. Log in to your development environment as a functions developer.
2. In a terminal window, create a new function by entering:

```
fn create function <app-name> <function-name> <image-name>
```

where:
- `<app-name>` is the name of an existing application in which to create the new function.
- `<function-name>` is the name of the new function you want to create. Avoid entering confidential information.
- `<image-name>` is the name of the existing image in the Docker registry on which to base the new function.

For example:

```
fn create function acmeapp acme-func phx.ocir.io/ansh81vrlzp/acme-repo/acme-func:0.0.3
```

A new function is created in Oracle Functions, based on the existing image and with the name you specified.

3. Verify that the new function has been created by entering:

```
fn list functions <app-name>
```

For example:

```
$ fn list functions acme-app
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>IMAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>acme-func</td>
<td>phx.ocir.io/ansh81vrlzp/acme-repo/acme-func:0.0.3</td>
</tr>
</tbody>
</table>

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage functions:
- `CreateFunction`
- `DeleteFunction`
- `GetFunction`
- `UpdateFunction`

**Sample Functions, Solution Playbooks, Reference Architectures, and Developer Tutorials**

**Sample Functions**

When you set up your development environment for Oracle Functions, simple helloworld functions are included by default. These sample functions enable you to get up and running quickly with Oracle Functions.

In addition, a number of how-to's, patterns, use cases, and other samples are available in the Oracle Functions samples repository on GitHub. These include:
- examples of how to interact with other Oracle Cloud Infrastructure services
- examples of how to optimally connect to databases
- examples of how to use Cloud Events to trigger functions
- use cases for IT Governance, Data Processing, SaaS Application Extensions, and more
Solution Playbooks

Solution playbooks are targeted, cross-product explanations and architectures showing how to handle or implement a specific scenario on Oracle Cloud Infrastructure. They are available from the Oracle Cloud Infrastructure Architecture Center.

Extend SaaS Applications with a Cloud Native Approach

The Extend SaaS Applications with a Cloud Native Approach solution playbook shows how to design a SaaS extension for Oracle Fusion Applications Cloud Service using a Cloud Native approach.

In this high-level design, Oracle Functions serves as the back-end implementation of a REST API, secured by Oracle Identity Cloud Service. Authentication is handled by Oracle Cloud Infrastructure API Gateway.

Reference Architectures

Reference architectures are architectures, configurations, and best practices for deploying on Oracle Cloud Infrastructure. They are available from the Oracle Cloud Infrastructure Architecture Center.

Automate Loading Data to a Data Warehouse Using a Serverless Application

The Automate Loading Data to a Data Warehouse Using a Serverless Application reference architecture shows how to use a serverless function to automate the process of extracting data from files generated by various databases or applications and loading the data into a data warehouse for analysis.

In this architecture, the Events service is triggered when zipped CSV files are uploaded to a specific bucket in Oracle Cloud Infrastructure Object Storage. The emitted event invokes a function in Oracle Functions, which extracts the data from the uploaded files and loads the data into an Oracle Autonomous Data Warehouse instance. After the data is loaded to the data warehouse, the processed CSV files are moved to a different bucket in Object Storage.

Developer Tutorials

Developer Tutorials show you how to complete development-related tasks with step-by-step instructions. Developer Tutorials for Oracle Functions are available in the Oracle Cloud Infrastructure documentation.

Viewing Functions and Applications

Having deployed functions to Oracle Functions, you'll typically want to view the functions you've deployed, along with other functions in the same application and different applications. For example, you might want to see:

- all the applications in a compartment
- details of the image for a given function

You can view applications and functions using the Console, the Fn Project CLI, and the API.

Using the Console

To view details of applications and functions deployed to Oracle Functions using the Console:

1. Log in to the Console as a functions developer.
2. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Functions.
3. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
4. Select the compartment containing the applications and functions that you want to see information about.

The Applications page shows all the applications in the compartment you selected.
5. Click the name of an application to see the functions within it.

The **Functions** page shows details for all the functions within the application you selected, including:

- the Docker image created for each function
- when the function was last updated

6. Click the name of a function on the **Functions** page to see additional information about that function, including the values of timeout and memory configuration parameters.

**Using Fn Project CLI Commands**

To view details of applications and functions deployed to Oracle Functions using the Fn Project CLI:

1. Log in to your development environment as a functions developer.

2. If you want to see details about applications, in a terminal window:

   - Enter the following command to see a simple list of applications:
   ```
   fn list apps
   ```
   For example:
   ```
   $ fn list apps
   acme-app
   ```
   - Enter the following command to see more detail about a particular application:
   ```
   fn inspect app <app-name>
   ```
   For example:
   ```
   $ fn inspect app acme-app
   {
   "annotations": {
      "oracle.com/oci/appCode": "fht7ns4mn2q",
      "oracle.com/oci/compartmentId": "ocid1.compartment.oc1..aaaaaaaaw______nyq",
      "oracle.com/oci/subnetIds": [
         "ocid1.subnet.oc1.phx.aaaaaaaaao...
      ],
      "oracle.com/oci/tenantId": "oci1.tenancy.oc1..aaaaaaap...keq",
      "created_at": "2018-07-13T17:54:34.000Z",
      "id": "ocid1.fnapp.oc1.phx.aaaaaaaaaf______r3ca",
      "name": "acme-app",
      "updated_at": "2018-07-13T17:54:34.000Z"
   }
   ```

3. If you want to see details about functions, in a terminal window:

   - Enter the following command to see a simple list of functions in a particular application:
   ```
   fn list functions <app-name>
   ```
   For example:
   ```
   $ fn list functions acme-app
   NAME            IMAGE
   acme-func       phx.ocir.io/ansh81vrulzp/acme-repo/acme-func:0.0.3
   ```
Functions

- Enter the following command to see more detail about a particular function:

  $ fn inspect function <app-name> <function-name>

For example:

  $ fn inspect function acme-app acme-func

  {
    "annotations": {
      "fnproject.io/fn/invokeEndpoint": "https://fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke",
      "oracle.com/oci/compartmentId": "ocid1.compartment.oc1..aaaaaaaaw______nyq"
    },
    "app_id": "ocid1.fnapp.oc1.phx.aaaaaaaaaf______r3ca",
    "created_at": "2018-07-26T12:50:53.000Z",
    "format": "default",
    "id": "ocid1.fnfunc.oc1.phx.aaaa___uxoa",
    "image": "phx.ocir.io/ansh81vru1zp/acme-repo/acme-func:0.0.3",
    "memory": 128,
    "name": "acme-func",
    "timeout": 30,
    "updated_at": "2018-07-26T13:59:18.000Z"
  }

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to see details about applications and functions:

- ListApplications
- ListFunctions

Invoking Functions

You can invoke a function that you've deployed to Oracle Functions in different ways:

- Using the Fn Project CLI.
- Using the Oracle Cloud Infrastructure CLI.
- Using the Oracle Cloud Infrastructure SDKs.
- Making a signed HTTP request to the function's invoke endpoint. Every function has an invoke endpoint.

Each of the above invokes the function via requests to the API. Any request to the API must be authenticated by including a signature and the OCID of the compartment to which the function belongs in the request header. Such a request is referred to as a 'signed' request. The signature includes Oracle Cloud Infrastructure credentials in an encrypted form.

If you use the Fn Project CLI or the Oracle Cloud Infrastructure CLI to invoke a function, authentication is handled for you. See Using the Fn Project CLI to Invoke Functions on page 2072 and Using the Oracle Cloud Infrastructure CLI to Invoke Functions on page 2072.

If you use an Oracle Cloud Infrastructure SDK to invoke a function, you can use the SDK to handle authentication. See Using SDKs to Invoke Functions on page 2073.
If you make a signed HTTP request to a function's invoke endpoint, you'll have to handle authentication yourself by including a signature and the OCID of the compartment to which the function belongs in the request header. You can do this in different ways:

- Using the Oracle Cloud Infrastructure CLI `raw-request` command. See Sending a Signed Request to a Function's Invoke Endpoint (using the Oracle Cloud Infrastructure CLI raw-request command) on page 2074.
- Using a bash script provided by Oracle (commonly referred to as oci-curl). See Sending a Signed Request to a Function's Invoke Endpoint (using oci-curl) on page 2075.
- Writing code to programmatically sign requests. For information about the required credentials and how to sign the requests, see Request Signatures on page 4383.

Tip:
If you aren't able to successfully complete one of the steps in this topic, review the solutions for common problems (see Troubleshooting Oracle Functions on page 2097).

Using the Fn Project CLI to Invoke Functions

To invoke a function deployed to Oracle Functions using the Fn Project CLI:

1. Log in to your development environment as a functions developer.
2. In a terminal window, enter:

   ```
   fn invoke <app-name> <function-name>
   ```

   where:
   - `<app-name>` is the name of the application containing the function you want to invoke
   - `<function-name>` is the name of the function you want to invoke

   For example:

   ```
   fn invoke helloworld-app helloworld-func
   ```

   Output:

   ```
   Hello World !
   ```

   Tip:
   If you want to pass arguments and values to a function, prefix the `fn` `invoke` command with `echo -n "<argument>=<value>" |`

   If the function is expecting the argument and value as JSON, use a valid JSON format. For example:

   ```
   echo -n '{"name":"John"}' | fn invoke helloworld-app helloworld-func
   ```

   Output:

   ```
   Hello John !
   ```

Using the Oracle Cloud Infrastructure CLI to Invoke Functions

If you have installed the Oracle Cloud Infrastructure CLI, you can use it to send API requests to invoke functions. Among other things, the Oracle Cloud Infrastructure CLI will facilitate Oracle Cloud Infrastructure authentication. For information about using the Oracle Cloud Infrastructure CLI, see Command Line Interface (CLI) on page 4192.
These instructions assume:

- you have already installed and configured the Oracle Cloud Infrastructure CLI
- you want to invoke a function as the functions developer that's configured for your development environment

To invoke a function using the Oracle Cloud Infrastructure CLI:

1. Log in to your development environment as a functions developer.
2. In a terminal window, enter:

   ```
   oci fn function invoke <function-ocid> --file "<output-filepath>" --body "<request-parameters>"
   ```

   where:

   - `<function-ocid>` is the OCID of the function you want to invoke. To find out a function's OCID, use the `fn inspect` command to see the value of the function's `id` property (see Viewing Functions and Applications on page 2069).
   - `<output-filepath>` is the path and name of a file to write the response to. To write the response to stdout, specify `--file "-"`
   - `<request-parameters>` are optionally arguments and values to pass to the function. If the function is expecting arguments and values as JSON, use a valid JSON format. For example, `--body '{"name":"John"}'`. Note that you must include `--body ""` in the request, even if there are no request parameters to pass.

   For example:

   - ```
   oci fn function invoke --function-id ocid1.fnfunc.oc1.phx.aaaa___uxoa --file "-" --body ""
   ```

   Output:

   ```
   Hello World !
   ```

   - ```
   oci fn function invoke --function-id ocid1.fnfunc.oc1.phx.aaaa___uxoa --file "-" --body '{"name":"John"}'
   ```

   Output:

   ```
   Hello John !
   ```

### Using SDKs to Invoke Functions

If you're writing a program to invoke a function in a language for which an Oracle Cloud Infrastructure SDK exists, Oracle recommends you use that SDK to send API requests to invoke the function. Among other things, the SDK will facilitate Oracle Cloud Infrastructure authentication.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the `InvokeFunction` API operation to invoke functions.

### Obtaining a Function's Invoke Endpoint

When invoking a function using oci-curl or the Oracle Cloud Infrastructure CLI `raw-request` command, you have to specify the function's invoke endpoint.

To obtain a function's invoke endpoint:

1. Log in to your development environment as a functions developer.
2. In a terminal window, enter:

```bash
fn inspect function <app-name> <function-name>
```

where:
- `<app-name>` is the name of the application containing the function for which you want to obtain the invoke endpoint
- `<function-name>` is the name of the function for which you want to obtain the invoke endpoint

For example:

```bash
fn inspect function helloworld-app helloworld-func
```

Output:

```json
{
   "annotations": {
      "fnproject.io/fn/invokeEndpoint": "https://fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke",
      ...
   }
}
```

The function's invoke endpoint is the value of "fnproject.io/fn/invokeEndpoint". For example, "https://fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke" (abbreviated for readability).

**Sending a Signed Request to a Function's Invoke Endpoint (using the Oracle Cloud Infrastructure CLI raw-request command)**

If you have installed the Oracle Cloud Infrastructure CLI, you can use it to send API requests to invoke functions. Among other things, the CLI will facilitate Oracle Cloud Infrastructure authentication. For more information about using the Oracle Cloud Infrastructure CLI, see Command Line Interface (CLI) on page 4192.

These instructions assume:
- you have already installed and configured the Oracle Cloud Infrastructure CLI
- you want to invoke a function as the functions developer that's configured for your development environment

To invoke a function deployed to Oracle Functions by sending a signed request to the function's invoke endpoint using the Oracle Cloud Infrastructure CLI raw-request command:

1. Log in to your development environment as a functions developer.
2. Obtain the function's invoke endpoint (see Obtaining a Function's Invoke Endpoint on page 2073).

   For example, "fnproject.io/fn/invokeEndpoint": "https://fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke" (abbreviated for readability).
3. Use the Oracle Cloud Infrastructure CLI raw-request command to invoke the function by sending a signed POST request to the function's invoke endpoint by entering:

```
oci raw-request --http-method POST --target-uri <invoke-endpoint> --request-body "<request-parameters>"
```

where:

- `<invoke-endpoint>` is the endpoint you obtained in the earlier step.
- `<request-parameters>` are optionally arguments and values to pass to the function. If the function is expecting arguments and values as JSON, use a valid JSON format. Note that you must include `--request-body ""` in the request, even if there are no request parameters to pass.

For example:

```
```

Output:

```
Hello World!
```

```
```

Output:

```
Hello John!
```

4. Assuming a passphrase was provided to encrypt the API signing key (as recommended by Oracle), enter the passphrase when prompted.

**Sending a Signed Request to a Function's Invoke Endpoint (using oci-curl)**

When you followed the instructions to prepare your client environment for Oracle Functions, you installed and configured oci-curl in readiness for using it to invoke functions. Among other things, oci-curl will facilitate Oracle Cloud Infrastructure authentication.

These instructions assume:

- you have already configured oci-curl appropriately (see 7. Set the Context for the Fn Project CLI Using the oracle.profile Parameter on page 2055)
- you want to invoke a function as the functions developer that’s configured for your development environment

To invoke a function deployed to Oracle Functions by sending a signed request to the function's invoke endpoint using oci-curl:

1. Log in to your development environment as a functions developer.
2. Obtain the function's invoke endpoint (see Obtaining a Function's Invoke Endpoint on page 2073).

For example, "fnproject.io/fn/invokeEndpoint": "https://fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa____uxoa/actions/invoke" (abbreviated for readability).
3. In a terminal window, use the `source` command to set up the current shell environment for oci-curl by entering:

```
source <path-to-script>/oci-curl.sh
```

where `<path-to-script>` is the path to the location of the oci-curl.sh script (see 3. Create and Configure a Copy of oci-curl on page 2050). For example:

```
source ~/oci-curl/oci-curl.sh
```

4. In the same terminal window in which you entered the `source` command, use oci-curl to invoke the function by sending a signed POST request to the function's invoke endpoint by entering:

```
oci-curl "<invoke-endpoint-host>" post <filename> "<invoke-endpoint-path>"
```

where:

- `<invoke-endpoint-host>` is the first half of the endpoint you obtained in the earlier step, excluding `https://` and up to (and including) `.oraclecloud.com`. For example, `fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com`
- `<filename>` is the name of a file containing data to pass to the function (you must specify a file, even if it's empty). For example, `payload.json`
- `<invoke-endpoint-path>` is the second half of the endpoint you obtained in the earlier step, from (but not including) `.oraclecloud.com` onwards. For example, `/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke`

For example, combining the previous examples, you might enter:

```
oci-curl "fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com" post payload.json "/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke"
```

5. Assuming a passphrase was provided to encrypt the API signing key (as recommended by Oracle), enter the passphrase when prompted.

## Controlling Access to Invoke and Manage Functions

When configuring a tenancy for function development, the steps in Create a Policy to Give Oracle Functions Users Access to Function-Related Resources on page 2043 instruct you to specify the following identity policy:

```
Allow group <group-name> to manage functions-family in compartment <compartment-name>
```

This identity policy enables authenticated users in the specified group to manage (that is, create, update, and delete) functions and applications in the named compartment, and also enables those users to invoke functions in the compartment. This policy typically meets the requirements of functions developers developing and testing multiple functions in your organization.

However, this identity policy might be too permissive to meet your security requirements to control the invocation and management of functions in production environments. For example, in a production environment you might want to prevent users from invoking functions completely, or restrict users to invoking just functions in a specific application, or to invoking just a particular function.

To control the functions that users in a group can invoke and manage, set up identity policies:

1. To control the functions that a user can invoke and manage, confirm that they are not in a group that has been given the manage functions-family permission.
2. If you want to enable users in a group to create, update, and delete applications and functions in a compartment, but to be unable to invoke functions, enter the following policy statements:

```plaintext
Allow group <group-name> to manage fn-app in compartment <compartment-name>

Allow group <group-name> to manage fn-function in compartment <compartment-name>
```

3. If you want to allow invocations of particular functions only, or invocations of functions in particular applications only, include the appropriate function and application OCIDs in suitable policy statements. For example:

- To enable users to invoke all the functions in a specific application, enter a policy statement in the following format:

  ```plaintext
  Allow group <group-name> to use fn-invocation in compartment <compartment-name> where target.app.id = '<application-OCID>'
  ```

- To enable users to invoke one specific function, enter a policy statement in the following format:

  ```plaintext
  Allow group <group-name> to use fn-invocation in compartment <compartment-name> where target.function.id = '<function-OCID>'
  ```

- To enable users to invoke all the functions in all applications except for functions in one specific application, enter a policy statement in the following format:

  ```plaintext
  Allow group <group-name> to use fn-invocation in compartment <compartment-name> where target.app.id != '<application-OCID>'
  ```

- To enable users to invoke all the functions in a compartment except for one specific function, enter a policy statement in the following format:

  ```plaintext
  Allow group <group-name> to use fn-invocation in compartment <compartment-name> where target.function.id != '<function-OCID>'
  ```

- To enable users to invoke two specific functions, enter a policy statement in the following format:

  ```plaintext
  Allow group <group-name> to use fn-invocation in compartment <compartment-name> where ANY {target.function.id='<function-OCID>', target.function.id='<function-OCID>'}
  ```

- To enable users to invoke one specific function along with all the functions in a specific application, a policy statement in the following format:

  ```plaintext
  Allow group <group-name> to use fn-invocation in compartment <compartment-name> where ANY {target.function.id='<function-OCID>', target.app.id='<application-OCID>'}
  ```
4. If you want to allow function invocation and management requests only from particular IP addresses:
   a. Create a network source to specify the allowed IP addresses, if a suitable network source doesn't exist already (see Managing Network Sources on page 2427).
   b. Add a policy statement to enable only those IP addresses in the network source to invoke or manage functions. For example:
      - To only allow function invocation requests from IP addresses defined in a network source named corpnet, enter a policy statement in the following format:
        
        ```
        Allow group <group-name> to use fn-invocation in compartment <compartment-name> where request.networkSource.name='corpnet'
        ```
      - To only allow function management requests from IP addresses defined in a network source named corpnet, enter a policy statement in the following format:
        
        ```
        Allow group <group-name> to manage functions-family in compartment <compartment-name> where request.networkSource.name='corpnet'
        ```

Storing and Viewing Function Logs

When a function is invoked, you'll typically want to access the function's logs for troubleshooting. The Oracle Cloud Infrastructure Logging service is the default and recommended option for accessing, searching, and storing function logs. See Using the Console to Enable and View Function Logs in Oracle Cloud Infrastructure Logging on page 2078. For more information about the contents of function logs, see Details for Functions on page 2603.

Alternatively, there might be occasions when you want to send function logs to an external logging destination like Papertrail. To send logs to an external logging destination instead of the Oracle Cloud Infrastructure Logging service, you use the Fn Project CLI to specify a syslog URL. See Using Fn Project CLI Commands to Specify a syslog URL on page 2079.

Note that to store and view logs for a function, the function must include print statements. For example:

- For node.js: `console.log('Entering Hello Node.js function');`
- For java: `System.err.println("Entering Java Hello World Function");`
- For go: `fmt.Println("Entering Hello Go function")`

Using the Console to Enable and View Function Logs in Oracle Cloud Infrastructure Logging

To enable and view function logs in the Oracle Cloud Infrastructure Logging service:

1. Log in to the Console as a functions developer.
2. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Functions.
3. Select the region and compartment containing the application with functions for which you want to create, enable, and view logs.
   The Applications page shows all the applications in the compartment you selected.
4. Select the application with functions for which you want to enable, view, and log.
5. To create and enable a new function log in the Oracle Cloud Infrastructure Logging service:
   a. Under Resources, click Logs, click the Actions icon (three dots), and then click Enable Log and specify:
      • **Compartment:** The compartment in which to create the new log. By default, the current compartment.
      • **Log Group:** The log group in which to create the new log. Select an existing log group, or select:
         • **Auto-create a default log group** to create a default log group with a default name (DEFAULT_GROUP), if one doesn't exist already.
         • **Create a new log group** to create a new log group with a name and description that you provide.
      • **Log Name:** The name of the new log. By default, `<application-name>_invoke`.
      • **Log Retention:** The length of time to retain log data.
   b. Click Enable Log to create the new log (and the new log group, if you specified one).

   For more information, see Enabling Logging for a Resource on page 2591.

6. To enable an existing function log, under Resources, click Logs, click the Actions icon (three dots), and then click Enable Log.

7. To view the data in an existing function log, under Resources, click Logs, and then click the name of the log you want to view in the Log Name column.

   The log opens in the log group's Log Details page, enabling you to sort and filter log data by time.

**Using Fn Project CLI Commands to Specify a syslog URL**

The Oracle Cloud Infrastructure Logging service is the default and recommended option for accessing, searching, and storing function logs.

Alternatively, you can send function logs to an external logging destination like Papertrail instead by using the Fn Project CLI to specify a syslog URL. Note that to use an external logging destination, you must have set up a VCN with public subnets and an internet gateway (see Create the VCN and Subnets to Use with Oracle Functions, if they don't exist already on page 2040).

To send function logs to an external logging destination by setting the syslog URL:

1. Log in to your development environment as a functions developer.
2. To create a new application and specify that all functions in the application send their logs to an external logging destination, enter:

   ```
   fn create app <app-name> --syslog-url <logging-service-url> --annotation oracle.com/oci/subnetIds='["<subnet-ocid>"]'
   ```

   where:
   • `<app-name>` is the name of the new application. Avoid entering confidential information.
   • `<logging-service-url>` is the syslog URL to which to send logs.
   • `<subnet-ocid>` is the OCID of the public subnet (or subnets, up to a maximum of six) in which to run functions. If a regional subnet has been defined, best practice is to select that subnet to make failover across availability domains simpler to implement. If a regional subnet has not been defined and you need to meet high availability requirements, select multiple subnets (enclose each OCID in double quotes separated by commas, in the format '"<subnet-ocid>" ,"<subnet-ocid>"'). Oracle recommends that the public subnets
Functions

are in the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

For example:

```shell
fn create app acmeapp --syslog-url tcp://my.papertrail.com:4242 --
annotation oracle.com/oci/
subnetIds='["ocid1.subnet.oc1.phx.aaaaaaaacnh..."]'
```

Note that if you subsequently set up Oracle Cloud Infrastructure Logging to store logs, the existing syslog URL details are retained. So if you later decide to resume sending function logs to the external logging destination, you simply have to disable Oracle Cloud Infrastructure Logging and logs will be sent to the syslog URL again.

3. To update an existing application and specify that all functions in the application send their logs to an external logging destination, enter:

```shell
fn update app <app-name> --syslog-url <logging-service-url>
```

where:
- `<app-name>` is the name of the application to update
- `<logging-service-url>` is the syslog URL to which to send logs

For example:

```shell
fn update app acmeapp --syslog-url tcp://my.papertrail.com:4242
```

4. To update an existing application and remove the external logging destination specified for the syslog URL, enter:

```shell
fn update app <app-name> --syslog-url ''
```

where:
- `<app-name>` is the name of the application to update

For example:

```shell
fn update app acmeapp --syslog-url ''
```

### Previously Supported Logging Options

In earlier Oracle Functions releases (prior to the release of the Oracle Cloud Infrastructure Logging service), you could specify where Oracle Functions stores a function's logs by setting up a 'logging policy' for the application containing the function. Previously, you could use the Console to set up a logging policy to:

- Store logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage by selecting the OCI **Logging** option.
  
  To view function logs in a storage bucket, the group to which you belong must have been granted access with the following identity policy statements:

  ```
  • Allow group <group-name> to manage object-family in compartment <compartment-name>
  • Allow group <group-name> to read objectstorage-namespaces in compartment <compartment-name>
  ```

  (Usually created when configuring your tenancy for function development. See Create a Policy to Give Oracle Functions Users Access to Oracle Cloud Infrastructure Registry Repositories on page 2043.)

- Store logs by sending them to an external logging destination like Papertrail by selecting the **Syslog URL** option.

For an existing application where you have previously already set up a logging policy, the above functionality is still supported and the existing logging policy is applied. However, note the following:

- You cannot use the Console to set up a new logging policy or edit an existing logging policy.
• If the existing logging policy specified storing function logs as objects in a storage bucket in Oracle Cloud Infrastructure Object Storage:
  • The ability to store logs in Object Storage will be deprecated in a future release.
  • Oracle recommends you switch to storing logs using Oracle Cloud Infrastructure Logging.
  • If you do switch to using Oracle Cloud Infrastructure Logging to store logs, you cannot revert to storing the logs in Object Storage.
  • Logs stored in Object Storage will continue to exist (with each log name including the OCID of the associated function, as before).
• If the existing logging policy specified a syslog URL:
  • If you switch to using Oracle Cloud Infrastructure Logging to store logs, the existing syslog URL details are retained. So if you later decide to resume sending function logs to the external logging destination, you simply have to disable Oracle Cloud Infrastructure Logging and logs will be sent to the syslog URL again.
  • If you want to change the syslog URL in the existing logging policy, you have to use the Fn Project CLI to change it.

Updating Functions

Having previously created a function definition in the Oracle Functions server, you can change some, but not all, of the function's properties. For example, you can change the maximum length of time a function is allowed to execute for, but you cannot change the function's name.

You can change the Docker image on which a function is based. If you do want to change the image, the replacement image must be suitable for use with Oracle Functions, and must have already been pushed to the Docker registry. With the replacement image in the Docker registry, you can then update a function's definition so that it is based on the replacement image, as described in this topic. If the replacement image has the same name and tag as the image on which the function was originally based, see Notes About Image Digests on page 2083.

You can update functions using the Console, the Fn Project CLI, and the API.

Using the Console to update an existing function

To use the Console to update an existing function in the Oracle Functions server:

1. Log in to the Console as a functions developer.
2. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Functions.
3. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
4. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

The Applications page shows the applications defined in the compartment.
5. Click the name of the application containing the existing function that you want to update.
6. Click the name of the function that you want to update.
7. Click Edit and update some or all of the following properties:
  • Image: The existing image in the Oracle Cloud Infrastructure Registry in your currently selected region. You first select the image repository, and then the image version. If the image has the same name and tag as the image on which the function was originally based, see Notes About Image Digests on page 2083.
  • Memory: The maximum amount of memory the function can use during execution.
  • Timeout: The maximum amount of time the function will be allowed to run for.
8. Click Save to update the function in the Oracle Functions server.

The function's updated properties are shown in the Console.
Using Fn Project CLI Commands

To use the Fn Project CLI to update an existing function in the Oracle Functions server:

1. Log in to your development environment as a functions developer.
2. In a terminal window, update properties of an existing function by entering:

   ```
   fn update function <app-name> <function-name> --image <image-name> --
   <property> <value>
   ```

   where:
   - `<app-name>` is the name of an existing application containing the existing function.
   - `<function-name>` is the name of the existing function you want to update.
   - `--image <image-name>` (optionally) is the name of an existing image in the Docker registry that you now want to base the function on, instead of the previously specified image. If the image has the same name and tag as the image on which the function was originally based, see Notes About Image Digests on page 2083.
   - `--<property> <value>` (optionally) is the property you want to update, and the new value you want it to have. Enter `fn update function --help` to see a list of properties and valid values.

   For example:

   ```
   fn update function acmeapp acme-func --image phx.ocir.io/ansh81vrlzpsi
   acme-repo/acme-func:0.0.4 --timeout 60
   ```

   ```
   fn update function acmeapp acme-func --memory 256
   ```

   The properties of the existing function are updated with the values you specified.

3. Verify that the function has been updated by entering:

   ```
   fn inspect function <app-name> <function-name>
   ```

   For example:

   ```
   fn inspect function acme-app acme-func
   ```

   Output:

   ```
   {
     "annotations": {
       "fnproject.io/fn/invokeEndpoint": "https://fht7ns4mn2q.us-
phoenix-1.functions.oci.oraclecloud.com/20181201/functions/
ocid1.fnfunc.oc1.phx.aaaa____uxoa/actions/invoke",
       "oracle.com/oci/compartmentId": "ocid1.compartment.oc1..aaaaaaaaw______nyq"
     },
     "app_id": "ocid1.fnapp.oc1.phx.aaaaaaaaaf______r3ca",
     "created_at": "2018-07-26T12:50:53.000Z",
     "format": "default",
     "id": "ocid1.fnfunc.oc1.phx.aaaa____uxoa",
     "image": "phx.ocir.io/ansh81vrlzpsi/acme-repo/acme-func:0.0.4",
     "memory": 256,
     "name": "acme-func",
     "timeout": 60,
     "updated_at": "2018-07-26T13:59:18.000Z"
   }
```
Functions

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the UpdateFunction API operation to update functions.

Notes About Image Digests

Images in a Docker registry are identified by repository, name, and a tag. In addition, Docker gives each version of an image a unique alphanumeric digest. When pushing an updated Docker image, it's recommended best practice to give the updated image a new tag to identify it, rather than reusing an existing tag. However, even if you push an updated image and give it the same name and tag as an earlier version, the newly pushed version will have a different digest to the earlier version.

When you create a function with Oracle Functions, you specify the name and tag of a particular version of an image on which to base the function. To avoid later inconsistencies, Oracle Functions also records the unique digest of that particular version of the image.

By default, if you push an updated version of an image to the Docker registry with the same name and tag as the original version of the image on which a function is based, Oracle Functions continues to use the original digest to pull the original version of the image. This might be the behavior you require. However, if you want Oracle Functions to pull the later version of the image, you can explicitly change the digest that Oracle Functions uses to identify which version of the image to pull in one of the following ways:

- Use the `fn update function` command and specify the original name and tag of the version of the image on which you want the function to be based. For example:

```
fn update function acmeapp acme-func --image phx.ocir.io/ansh81vrulzp/acme-repo/acme-func:0.0.4 --annotation oracle.com/oci/imageDigest="""'
```

Oracle Functions will update the digest recorded for the image on which the function is based to be the digest of the image in the Docker registry that has the name and tag you specify.

- Use the `fn update function` command and specify the digest of the version of the image on which you want the function to be based. For example:

```
fn update function acmeapp acme-func --annotation oracle.com/oci/imageDigest='sha256:8af7cb8d7______c498c0'
```

Oracle Functions will update the digest recorded for the image on which the function is based to be the digest you specify.

- Use the Console and click Edit Function on the Function Information tab, re-select the original name and tag of the version of the image on which the function is currently based, and click Save Changes. Oracle Functions will update the digest recorded for the image on which the function is based.

- Use the Oracle Cloud Infrastructure API or an Oracle Cloud Infrastructure SDK (for more information, see REST APIs on page 4368 and Software Development Kits and Command Line Interface on page 4225).

Deleting Applications and Functions

You can delete applications and functions in Oracle Functions that you or other functions developers have created, provided you have been granted the necessary permission (FN_APP_DELETE or FN_FUNCTION_DELETE as appropriate).

Note the following:

- Deleting a function does not delete the Docker image on which the function is based. To delete the image, you have to delete it explicitly (see Deleting and Undeleting an Image on page 3520).

- Deleting applications and functions is permanent. You cannot undelete an application or function that you've deleted.
Functions

• Deleting a function does not necessarily enable you to immediately delete the subnet and VCN in which the function runs. Expect to wait up to five minutes after the function was last invoked before you can delete the associated network resources.

You can delete applications and functions using the Console, the Fn Project CLI, and the API.

Using the Console

When using the Console to delete applications and functions, note that:

• when you delete an application, all of its functions are also deleted
• you're always prompted to confirm deletion because you cannot undelete an application or function later

To delete applications and functions using the Console:

1. Log in to the Console as a functions developer.
2. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Functions.
3. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
4. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
   The Applications page shows the applications defined in the compartment.
5. To delete an application, and all of its functions:
   a. Click the name of the application you want to delete.
   b. On the Application Detail page, click Delete and confirm you want to delete the application as follows:
      • If the application does not have functions within it, click Delete to confirm that you want to delete the application.
      • If the application does have functions within it, you are shown a list of the functions in the application. To delete the application, enter DELETE <APPLICATION-NAME> in the text box, and click Delete.
   Note that deleting an application and all of its functions does not delete the Docker images on which the functions are based. To delete the images, you have to delete them explicitly (see Deleting and Undeleting an Image on page 3520).
6. To delete a function:
   a. Click the name of the application containing the function you want to delete.
   b. On the Application Detail page, click the name of the function you want to delete.
   c. On the Function Detail page, click Delete and confirm you want to delete the function.
   Note that deleting a function does not delete the Docker image on which the function is based. To delete the image, you have to delete it explicitly (see Deleting and Undeleting an Image on page 3520).

Using Fn Project CLI Commands

When using the Fn Project CLI to delete applications and functions, note that you cannot delete an application if it contains functions (you must delete the functions first).

To delete applications and functions in Oracle Functions using the Fn Project CLI:

1. Log in to your development environment as a functions developer.
2. To delete an application:
   a. In a terminal window, enter:

   ```bash
   fn delete app <app-name>
   ```

   where `<app-name>` is the name of the application to delete.

   For example:

   ```bash
   fn delete app acmeapp
   ```

   b. Verify that the application has been deleted by entering:

   ```bash
   fn list apps
   ```

3. To delete a function:
   a. In a terminal window, enter:

   ```bash
   fn delete function <app-name> <function-name>
   ```

   where:
   - `<app-name>` is the name of the application containing the function you want to delete.
   - `<function-name>` is the name of the function you want to delete.

   For example:

   ```bash
   fn delete function acmeapp acme-func
   ```

   b. Verify that the function has been deleted by entering:

   ```bash
   fn list functions <app-name>
   ```

   For example:

   ```bash
   fn list functions acmeapp
   ```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to delete applications and functions:

- DeleteApplication
- DeleteFunction

Passing Custom Configuration Parameters to Functions

The code in functions you deploy to Oracle Functions will typically require values for different parameters. Some pre-defined parameters are available to your functions as environment variables. But you’ll often want your functions to use parameters that you’ve defined yourself. For example, you might create a function that reads from and writes to a database. The function will require a database connect string, comprising a username, password, and hostname. You’ll probably want to define username, password, and hostname as parameters that are passed to the function when it’s invoked.

To pass user-defined parameters to a function deployed in Oracle Functions, you create key-value pairs known as custom configuration parameters. You can create custom configuration parameters that are:

- application-wide, meaning they are passed to every function in an application
function-specific, meaning they are passed to the particular function for which they are defined (function-specific parameters override application-wide parameters with the same name)

To create custom configuration parameters, you can use:

- the `config:` section of a function's `func.yaml` file, to define function-specific custom configuration parameters
- the Console and the Fn Project CLI, to define both application-wide and function-specific custom configuration parameters

Oracle Functions combines all the custom configuration parameters (both application-wide and function-specific) in the application into a single, serially-encoded configuration object with a maximum allowable size of 4Kb.

**Using the Console**

To specify custom configuration parameters to pass to functions using the Console:

1. Log in to the Console as a functions developer.
2. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.
3. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
4. Select the compartment specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

   The **Applications** page shows the applications defined in the compartment.
5. Click the name of the application containing functions to which you want to pass custom configuration parameters:
   - To pass one or more custom configuration parameters to every function in the application, click **Configuration** to see the **Configuration** section for the application.
   - To pass one or more custom configuration parameters to a particular function, click the function's name to see the **Configuration** section for the function.
6. In the **Configuration** section, specify details for the first custom configuration parameter:
   - **Key**: The name of the custom configuration parameter. The name must only contain alphanumeric characters and underscores, and must not start with a number. For example, `username`
   - **Value**: A value for the custom configuration parameter. The value must only contain printable unicode characters. For example, `jdoe`
7. Click the plus button to save the new custom configuration parameter.

   Oracle Functions combines the key-value pairs for all the custom configuration parameters (both application-wide and function-specific) in the application into a single, serially-encoded configuration object with a maximum allowable size of 4Kb. You cannot save the new custom configuration parameter if the size of the serially-encoded configuration object would be greater than 4Kb.
8. (Optional) Enter additional custom configuration parameters as required.

**Using Fn Project CLI Commands**

To specify custom configuration parameters to pass to functions using the Fn Project CLI:

1. Log in to your development environment as a functions developer and open a terminal window.
2. To specify one or more custom configuration parameters to pass to every function in an existing application, enter:

```
fn config app <app-name> <key> <value>
```

where:

- `<app-name>` is the name of the application containing the functions to which you want to pass the custom configuration parameter.
- `<key>` is the name of the custom configuration parameter. The name must only contain alphanumeric characters and underscores, and must not start with a number.
- `<value>` is the value to give to the custom configuration parameter. The value must only contain printable unicode characters.

For example:

```
fn config app acmeapp username jdoe
```

Note the following:

- You can also define application-wide custom configuration parameters when you create a new application using the `fn create app` command.
- Oracle Functions combines the key-value pairs for all the custom configuration parameters (both application-wide and function-specific) in the application into a single, serially-encoded configuration object with a maximum allowable size of 4Kb.

3. To specify one or more custom configuration parameters to pass to a particular function, enter:

```
fn config function <app-name> <function-name> <key> <value>
```

where:

- `<app-name>` is the name of the application containing the function to which you want to pass the custom configuration parameter.
- `<function-name>` is the name of the function to which to pass the custom configuration parameter.
- `<key>` is the name of the custom configuration parameter. The name must only contain alphanumeric characters and underscores, and must not start with a number.
- `<value>` is the value to give to the custom configuration parameter. The value must only contain printable unicode characters.

For example:

```
fn config function acmeapp acme-func username jdoe
```

Note the following:

- You can also define function-specific custom configuration parameters when you create a new function using the `fn create function` command.
- Oracle Functions combines the key-value pairs for all the custom configuration parameters (both application-wide and function-specific) in the application into a single, serially-encoded configuration object with a maximum allowable size of 4Kb.

### Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use these API operations to define custom configuration parameters:

- `CreateFunction`
- `UpdateFunction`
- `CreateApplication`
Functions

- UpdateApplication

Accessing File Systems from Running Functions

A function you've deployed to Oracle Functions can access the file system of the container in which it's running as follows:

- the function can read files from all directories
- the function can write files to the /tmp directory

For example, you might want a function to download an Excel file and then read its contents. To meet this requirement, you might create a function that writes the file to the /tmp directory in the container's filesystem, and then subsequently reads the file.

When writing files to the /tmp directory, the /tmp directory is generally always writable. However, the maximum allowable size of the /tmp directory depends on the maximum memory threshold specified for the function:

<table>
<thead>
<tr>
<th>Maximum memory threshold for the function (MB)</th>
<th>Maximum allowed size of /tmp (MB)</th>
<th>Maximum allowed number of files (inodes) in /tmp</th>
</tr>
</thead>
<tbody>
<tr>
<td>128MB</td>
<td>32MB</td>
<td>1024</td>
</tr>
<tr>
<td>256MB</td>
<td>64MB</td>
<td>2048</td>
</tr>
<tr>
<td>512MB</td>
<td>128MB</td>
<td>4096</td>
</tr>
<tr>
<td>1024MB</td>
<td>256MB</td>
<td>8192</td>
</tr>
</tbody>
</table>

Note that the /tmp directory might be shared by multiple invocations of the function. A file written by an earlier invocation of a function could still exist when the function is invoked a second time. It is your responsibility to delete any files to avoid unexpected behavior.

Integrating Oracle Functions with Other Oracle Products

You can integrate functions you've deployed to Oracle Functions with other Oracle products, as described in the following topics:

- Accessing Other Oracle Cloud Infrastructure Resources from Running Functions on page 2088
- Connecting to Oracle Autonomous Database Instances from Running Functions on page 2093

Accessing Other Oracle Cloud Infrastructure Resources from Running Functions

When a function you've deployed to Oracle Functions is running, it can access other Oracle Cloud Infrastructure resources. For example:

- You might want a function to get a list of VCNs from the Networking service.
- You might want a function to read data from an Object Storage bucket, perform some operation on the data, and then write the modified data back to the Object Storage bucket.

To enable a function to access another Oracle Cloud Infrastructure resource, you have to include the function in a dynamic group, and then create a policy to grant the dynamic group access to that resource. For more information about dynamic groups, including the permissions required to create them, see Managing Dynamic Groups on page 2422.

Having set up the policy and the dynamic group, you can then include a call to a 'resource principal provider' in your function code. The resource principal provider uses a resource provider session token (RPST) that enables the function to authenticate itself with other Oracle Cloud Infrastructure services. The token is only valid for the resources to which the dynamic group has been granted access.

Note also that the token is cached for 15 minutes. So if you change the policy or the dynamic group, you will have to wait for 15 minutes to see the effect of your changes.
Oracle recommends that you use the resource principal provider included in the Oracle Cloud Infrastructure SDK. However, you might be writing a function in a language that the Oracle Cloud Infrastructure SDK does not support. Or you might simply not want to use the Oracle Cloud Infrastructure SDK. In either case, you can write your own custom resource principal provider to enable a function to authenticate itself with other Oracle Cloud Infrastructure services, using files and environment variables in the container in which the function is executing.

Using the Console
To enable a running function to access other Oracle Cloud Infrastructure resources:

1. Log in to the Console and create a new dynamic group:

   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Dynamic Groups.

   b. Follow the instructions in To create a dynamic group on page 2423, and give the dynamic group a name (for example, acme-func-dyn-grp).

   c. When specifying a rule for the dynamic group, consider the following examples:

      • If you want all functions in a compartment to be able to access a resource, enter a rule similar to the following that adds all functions in the compartment with the specified compartment OCID to the dynamic group:

        ```
        ALL {resource.type = 'fnfunc', resource.compartment.id = 'ocid1.compartment.oc1..aaaaaaaa23______smwa'}
        ```

      • If you want a specific function to be able to access a resource, enter a rule similar to the following that adds the function with the specified OCID to the dynamic group:

        ```
        resource.id = 'ocid1.fnfunc.oc1.iad.aaaaaaaaacq______dnya'
        ```

      • If you want all functions with a specific defined tag to be able to access a resource, enter a rule similar to the following that adds all functions with the defined tag to the dynamic group:

        ```
        ALL {resource.type = 'fnfunc', tag.department.operations.value = '45'}
        ```

      Note that free-form tags are not supported. For more information about tagging, see Resource Tags on page 211.

   d. Click Create Dynamic Group.

   Having created a dynamic group that includes the function, you can now create a policy to give the dynamic group access to the required Oracle Cloud Infrastructure resource.
Functions

2. Create a new policy:
a. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
b. Follow the instructions in To create a policy on page 2454, and give the policy a name (for example, acmefunc-dyn-grp-policy).
c. When specifying a policy statement, consider the following examples:
•

If you want functions in the acme-func-dyn-grp to be able to get a list of all the VCNs in the tenancy,
enter a rule similar to the following:
allow dynamic-group acme-func-dyn-grp to inspect vcns in tenancy

•

If you want functions in the acme-func-dyn-grp to be able to read and write to a particular Object
Storage bucket, enter a rule similar to the following:
allow dynamic-group acme-func-dyn-grp to manage objects
in compartment acme-storage-compartment where all
{target.bucket.name='acme-functions-bucket'}

•

If you want functions in the acme-func-dyn-grp to be able to read and write to all resources in a
compartment, enter a rule similar to the following:
allow dynamic-group acme-func-dyn-grp to manage all-resources in
compartment acme-storage-compartment

d. Click Create to create the new policy.
3. Include a resource principal provider in the function code to enable the function to authenticate with other Oracle
Cloud Infrastructure services. See:
•
•

Example: Adding the Oracle Resource Principal Provider to a Python Function to Get a List of VCNs from the
Networking Service on page 2090
Example: Adding a Custom Resource Principal Provider to a Function on page 2091

Example: Adding the Oracle Resource Principal Provider to a Python Function to Get a List of
VCNs from the Networking Service
Having added a function to a dynamic group, and created a policy that allows the dynamic group to list the VCNs
in the tenancy, you could include code similar to the following example to get a list of VCNs from the Networking
service. This example uses the Oracle resource principal provider to extract credentials from the RPST token.
import io
import json
from fdk import response
import oci
def handler(ctx, data: io.BytesIO=None):
signer = oci.auth.signers.get_resource_principals_signer()
resp = do(signer)
return response.Response(ctx,
response_data=json.dumps(resp),
headers={"Content-Type": "application/json"} )
def do(signer):
# List VCNs -------------------------------------------------------client = oci.core.VirtualNetworkClient({}, signer=signer)
try:
vcns = client.list_vcns(signer.compartment_id)
vcns = [[v.id, v.display_name] for v in vcns.data]
except Exception as e:
vcns = str(e)
return {"vcns": vcns, }

Oracle Cloud Infrastructure User Guide

2090


Example: Adding a Custom Resource Principal Provider to a Function

Oracle recommends that you use the resource principal provider included in the Oracle Cloud Infrastructure SDK. However, you might be writing a function in a language that the Oracle Cloud Infrastructure SDK does not support. Or you might simply not want to use the Oracle Cloud Infrastructure SDK. In either case, you can write your own custom resource principal provider to enable a function to authenticate itself with other Oracle Cloud Infrastructure services, using files and environment variables in the container in which the function is executing.

The container in which a function executes includes a directory tree that holds Oracle Cloud Infrastructure compatible credentials, specifically:

- A resource principal session token (RPST) in a file named `rpst`. The RPST token is formatted as a JWT token, and includes claims that identify the function's host tenancy and compartment.
- A private key for use in making requests to Oracle Cloud Infrastructure services on behalf of the function, in a file named `private.pem`.

The following environment variables are set inside the container in which the function executes:

- `OCIRESOURCEPRINCIPALVERSION`, containing the value `2.2`.
- `OCIRESOURCEPRINCIPALRPST`, containing the absolute path to the `rpst` file (including the filename).
- `OCIRESOURCEPRINCIPALPRIVATEPEM`, containing the absolute path to the `private.pem` file (including the filename).
- `OCIRESOURCEPRINCIPALREGION`, containing the region identifier in which the function is deployed (for example, `us-phoenix-1`).

To enable a function to access another Oracle Cloud Infrastructure service, add code to the function so that it can authenticate itself with the other resource:

1. Add code that loads the RPST token from the path in the `OCIRESOURCEPRINCIPALRPST` environment variable.
2. Add code that loads the private key from the path in the `OCIRESOURCEPRINCIPALPRIVATEPEM` environment variable.
3. Add code that uses the RPST token and the private key to create an Oracle Cloud Infrastructure request signature (see Request Signatures on page 4383).
4. Add code that constructs the request to the other Oracle Cloud Infrastructure resource.

If necessary, you can identify:

- The endpoints of other Oracle Cloud Infrastructure services in the same (local) region as the function, using the region identifier in the `OCIRESOURCEPRINCIPALREGION` environment variable.
- The function's host tenancy and compartment, using the `res_tenant` and `res_compartment` claims in the RPST token.

For example, the sample Python function below includes a custom resource principal provider that extracts credentials from the RPST token. It then submits a GET request to the IAM API's getTenancy operation to return the OCID of the function's tenancy.

```python
#!/usr/bin/env python3
import base64
import email.utils
import hashlib
import httpsig_cffi.sign
import json
import logging
import os.path
import re
import requests.auth
import urllib.parse

LOG = logging.getLogger(__name__)
```
The following class is derived from the Python section in https://docs.cloud.oracle.com/iaas/Content/API/Concepts/signingrequests.htm:

class SignedRequestAuth(requests.auth.AuthBase):
    """A requests auth instance that can be reused across requests""
    generic_headers = [
        "date",
        "(request-target)",
        "host"
    ]
    body_headers = [
        "content-length",
        "content-type",
        "x-content-sha256",
    ]
    required_headers = {
        "get": generic_headers,
        "head": generic_headers,
        "delete": generic_headers,
        "put": generic_headers + body_headers,
        "post": generic_headers + body_headers,
    }

    def __init__(self, key_id, private_key):
        # Build a httpsig_cffi.requests_auth.HTTPSignatureAuth for each
        # HTTP method's required headers
        self.signers = {}
        for method, headers in self.required_headers.items():
            signer = httpsig_cffi.sign.HeaderSigner(
                key_id=key_id, secret=private_key,
                algorithm="rsa-sha256", headers=headers[:]
            )
            use_host = "host" in headers
            self.signers[method] = (signer, use_host)

    def inject_missing_headers(self, request, sign_body):
        # Inject date, content-type, and host if missing
        request.headers.setdefault("date", email.utils.formatdate(usegmt=True))
        request.headers.setdefault("content-type", "application/json")
        request.headers.setdefault("host", urllib.parse.urlparse(request.url).netloc)

        # Requests with a body need to send content-type,
        # content-length, and x-content-sha256
        if sign_body:
            body = request.body or ""
            if "x-content-sha256" not in request.headers:
                m = hashlib.sha256(body.encode("utf-8"))
                base64digest = base64.b64encode(m.digest())
                base64string = base64digest.decode("utf-8")
                request.headers["x-content-sha256"] = base64string
                request.headers.setdefault("content-length", len(body))

    def __call__(self, request):
        verb = request.method.lower()
        # nothing to sign for options
        if verb == "options":
            return request
        signer, use_host = self.signers.get(verb, (None, None))
        if signer is None:
            raise ValueError("Don't know how to sign request verb ".format(verb))
# Inject body headers for put/post requests, date for all requests

```python
sign_body = verb in \["put", "post"]
self.inject_missing_headers(request, sign_body=sign_body)
```

```python
if use_host:
    host = urllib.parse.urlparse(request.url).netloc
else:
    host = None

signed_headers = signer.sign(
    request.headers, host=host,
    method=request.method, path=request.path_url)
request.headers.update(signed_headers)
return request
```

```python
def rp_auther():
    if os.environ['OCI_RESOURCE_PRINCIPAL_VERSION'] != "2.2":
        raise EnvironmentError('{} must be set to the value "2.2"'.format('OCI_RESOURCE_PRINCIPAL_VERSION'))
    rpst = os.environ['OCI_RESOURCE_PRINCIPAL_RPST']
    if os.path.isabs(rpst):
        with open(rpst) as f:
            rpst = f.read()
    private_key = os.environ['OCI_RESOURCE_PRINCIPAL_PRIVATE_PEM']
    if os.path.isabs(private_key):
        with open(private_key) as f:
            private_key = f.read()
    return get_claims(rpst), SignedRequestAuth('ST${}'.format(rpst),
        private_key)

def get_claims(rpst):
    """Parse an RPST as a JWT; return a dictionary of claims
    
The claims that are important are: sub, res_compartment, and res_tenant. These carry the resource OCID together with its location.
    """
    s = rpst.split('.')[1]
    s += "=" * ((4 - len(s) % 4) % 4)  # Pad to a multiple of 4 characters
    return json.loads(base64.b64decode(s).decode('utf-8'))

# Use RP credentials to make a request
region = os.environ['OCI_RESOURCE_PRINCIPAL_REGION']
claims, rp_auth = rp_auther()
response = requests.get("https://identity.{}.oraclecloud.com/20160918/
    tenancies/\{".format(region, claims['res_tenant']), auth=rp_auth)
print(response.json())
```

## Connecting to Oracle Autonomous Database Instances from Running Functions

You can deploy a function to Oracle Functions that connects to Oracle Autonomous Database instances.

Note that an Oracle Autonomous Database instance can be protected by an access control list (ACL). If the ACL is enabled, only those IP addresses and VCNs explicitly added to the ACL are allowed to connect to the database.

If you want a function running in a private subnet to connect to an Oracle Autonomous Database instance that has ACL enabled, edit the database's access control list and add the VCN.
If you want a function running in a public subnet to connect to an Oracle Autonomous Database instance that has ACL enabled:

1. Remove the default route rule that routes all outgoing internet traffic through the VCN's internet gateway.
2. Add a NAT gateway to the VCN.
3. Configure the subnet's route table with a rule that sends all outgoing internet traffic to the NAT gateway, and configure the subnet's security lists to allow internet traffic.
4. Review the NAT gateway's properties to obtain its public IP address.
5. Edit the database's access control list and add the NAT gateway's public IP address.

For more information about Oracle Autonomous Databases and ACLs, see Access Control Lists (ACLs) for Databases on Shared Exadata Infrastructure on page 1153.

Permissions Granted to Containers Running Functions

When a function you've deployed to Oracle Functions is invoked, it runs inside a container. The operations that a container can perform are determined by the user ID (UID) and group ID (GID) specified when the container is started. If a UID or GID is not specified, the container runs processes as the root user, with all the default capabilities enabled.

When starting a container to run a function, Oracle Functions always specifies a user named 'fn' with a UID of 1000, and a group name 'fn' with a GID of 1000. No privileges are granted to UID 1000 and GID 1000, so the container (and the function running inside it) does not acquire the default capabilities listed in the Docker documentation. In addition, the container is prevented from gaining privileges.

As a result, do not create and deploy functions that:

• depend on capabilities that are unavailable
• depend on privilege elevation (for example, su, sudo or setuid)

If you are using your own Dockerfile, include the following lines:

```bash
groupadd --gid 1000 fn && 
adduser --uid 1000 --gid fn fn
```

For example:

```bash
FROM oraclelinux:7-slim
RUN  yum -y install oracle-release-el7 oracle-nodejs-release-el7 & & \ 
    yum-config-manager --disable ol7_developer_EPEL & & \ 
    yum -y install oracle-instantclient19.3-basiclite nodejs & & \ 
    rm -rf /var/cache/yum & & \ 
    groupadd --gid 1000 fn & & \ 
    adduser --uid 1000 --gid fn fn
WORKDIR /function
ADD . /function/
RUN npm install
CMD exec node func.js
```

Note that if you do not include the `groupadd` and `adduser` lines in the above example Dockerfile, you will see the following error message:

```
(cx_Oracle.DatabaseError: ORA-12560: TNS:protocol adapter error
```

Oracle Functions Support for Private Network Access

Oracle Functions supports private communication between a function in a VCN and other Oracle Cloud Infrastructure resources and supported services in the Oracle Services Network without the traffic going over the internet. You can:
• enable a function in the VCN to access other resources and services
• enable other resources and services to invoke functions in the VCN

To provide such private access:

• create and deploy functions in private subnets
• add a service gateway to the VCN

For more information, see Access to Oracle Services: Service Gateway on page 3256.

Invoking Oracle Functions from Other Oracle Cloud Infrastructure Services

You can invoke functions in Oracle Functions from other Oracle Cloud Infrastructure services. Typically, you’ll want an event in another service to trigger a request to invoke a function defined in Oracle Functions.

This functionality is currently available in:

• The Events service. For more information, see Functions on page 1877 in Services that Produce Events on page 1817.
• The Notifications service. For more information, see Notifications Overview on page 3350. For a scenario, see Scenario A: Automatically Resize VMs on page 3366.
• The API Gateway service. For more information, see Adding a Function in Oracle Functions as an API Gateway Back End on page 410.
• The Oracle Integration service, using the OCI Signature Version 1 security policy. For more information, see Configure Oracle Integration to Call Oracle Cloud Infrastructure Functions with the REST Adapter in Using the REST Adapter with Oracle Integration.
• The Service Connector Hub service. For more information, see Service Connector Hub Overview on page 3750. For a scenario, see Scenario: Send Log Data to an Autonomous Database on page 3767.

Changing Oracle Functions Default Behavior

You can change several aspects of Oracle Functions default behavior using configuration parameters and environment variables.

Depending on the parameter, you can override a default value by specifying an alternative value in the following ways (note the order of precedence):

• by adding an entry to the func.yaml file (which overrides default values)
• by explicitly setting an environment variable (which overrides values set in the func.yaml file)
• by including a command option when you invoke the function using the Fn Project CLI (which overrides values set in environment variables or in the func.yaml file)

The following table indicates the parameters you can set, the default value, and where the default value can be overridden.

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Default Value</th>
<th>Units</th>
<th>func.yaml Parameter</th>
<th>Environment Variable</th>
<th>Fn CLI option</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Maximum time a function will be allowed to run | 30 | Seconds | timeout | n/a | n/a | Maximum value: 300
Best practice is to specify a timeout that is close to that likely to be required, rather than significantly more. |
<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Default Value</th>
<th>Units</th>
<th>func.yaml Parameter</th>
<th>Environment Variable</th>
<th>Fn CLI option</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum memory threshold for a function</td>
<td>128</td>
<td>MB</td>
<td>memory</td>
<td>FN_MEMORY</td>
<td>n/a</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 128</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 512</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 1024</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If this limit is exceeded during execution, the function is stopped and an error message is logged.</td>
</tr>
</tbody>
</table>

For more information about the above parameters, and other configuration parameters, see Func files in the Fn Project documentation.

**Differences between Oracle Functions and Fn Project**

In general, Oracle Functions and Fn Project are very similar. However there are some differences, as detailed below.

**Differences in Authentication When Making API Calls**

When you use the Oracle Cloud Infrastructure API with Oracle Functions, in the request header you have to provide:

- the OCID of the compartment to which the function belongs
- Oracle Cloud Infrastructure authentication details

**Differences When Invoking Functions**

To invoke a function deployed to Oracle Functions, you have to explicitly specify an Oracle Cloud Infrastructure endpoint (unless you're using the Fn Project CLI).

For example, when you use oci-curl to invoke a function, you have to send a request to the function's invoke endpoint (for example `https://fht7ns4mn2q.us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx.aaaa___uxoa/actions/invoke`).

You can obtain the appropriate endpoint by making a call to the API, either directly or by using the Fn Project CLI command:

```
fn inspect function <app-name> <function-name>
```

**Additional Context Configuration Parameters in Oracle Functions**

As well as supporting Fn Project context configuration parameters, Oracle Functions also has some additional parameters, as shown in the following table.
<table>
<thead>
<tr>
<th>Additional Parameter</th>
<th>Set in</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
</table>
| provider             | A context configuration .yaml file in ~/.fn/contexts | oracle          | Enables Oracle Functions rather than Fn Project functionality. When provider is set to oracle, the following parameters are valid:  
  - oracle.compartment-id  
  - oracle.profile  
  See 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053. |
| oracle.compartment-id| A context configuration .yaml file in ~/.fn/contexts | <compartment-ocid> | Specifies the OCID of the Oracle Cloud Infrastructure compartment that owns function-related resources.  
  See 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053. |
| oracle.profile       | A context configuration .yaml file in ~/.fn/contexts | <profile-name>   | Specifies which profile to use from the ~/.oci/config file. If not set, the profile named default is used.  
  See 7. Set the Context for the Fn Project CLI Using the oracle.profile Parameter on page 2055 |

**Use of Annotations**

When you're creating and viewing Oracle Functions resources using the Fn Project CLI, annotations enable you to identify and specify associated Oracle Cloud Infrastructure resources.

For example:

- When you're using the Fn Project CLI to create a new application, you use the --annotation parameter to specify the OCID of the subnet in which to run the function.
- When you're using the Fn Project CLI to view the properties of a function, the annotations element shows the OCID of the compartment that owns the function.

Note that unlike other configuration parameters and environment variables, annotation values cannot be passed as arguments to running Docker containers.

**Troubleshooting Oracle Functions**

This topic covers common issues related to Oracle Functions and how to address them.

Use the following techniques to find out more about an error or issue:
• **Use DEBUG=1 to see more details about an error:** If you encounter an unexpected error when using an Fn Project CLI command, you can find out more about the problem by starting the command with the string DEBUG=1 and running the command again. For example:

```
DEBUG=1 fn invoke helloworld-app helloworld-func
```

Note that DEBUG=1 must appear before the command, and that DEBUG must be in upper case.

• **Use --display-call-id when invoking functions to aid issue resolution:** If you encounter an issue when invoking a function, you can engage with Oracle Support. Oracle Support can investigate the issue more efficiently if you provide the call id of the function invocation. You can obtain the call id using the --display-call-id command option. For example:

```
fn invoke helloworld-app helloworld-func --display-call-id
```

Output:

```
Call ID: 01CS23SDG71BT2N9GZJ002DQM5
Hello World!
```

The issues in this topic are organized in the following broad categories:

• **Setting up and running Oracle Functions**

<table>
<thead>
<tr>
<th>Error number and message (if applicable)</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>401: Not authenticated</strong></td>
<td>Running Fn Project CLI commands returns a 401 error on page 2100</td>
</tr>
<tr>
<td><strong>404: Resource is not authorized or not found</strong></td>
<td>Running Fn Project CLI commands returns a 404 error on page 2100</td>
</tr>
<tr>
<td><strong>x509: decryption password incorrect</strong></td>
<td>Running Fn Project CLI commands returns an X509: decryption password incorrect error on page 2100</td>
</tr>
<tr>
<td><strong>Error response from daemon... unknown: Unauthorized</strong></td>
<td>Performing Docker-related operations with the Fn Project CLI displays an &quot;Error response from daemon... unknown: Unauthorized” message on page 2101</td>
</tr>
<tr>
<td><strong>asn1:structure error: tags don't match</strong></td>
<td>Running an Fn Project CLI command displays an &quot;Fn: asn1:structure error: tags don't match” message on page 2101</td>
</tr>
<tr>
<td><strong>Client version: n.n.nn is not latest: n.n.nn</strong></td>
<td>Running fn version shows that a more recent version of the Fn Project CLI is available on page 2101</td>
</tr>
</tbody>
</table>

• **Creating applications and functions**

<table>
<thead>
<tr>
<th>Error number and message (if applicable)</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unable to create your app, please try again.</strong></td>
<td>Creating a new application displays an error message in the New Application dialog on page 2101</td>
</tr>
</tbody>
</table>

• **Deploying applications and functions**

<table>
<thead>
<tr>
<th>Error number and message (if applicable)</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>unauthorized: incorrect username or password</strong></td>
<td>Deploying an application returns an &quot;unauthorized: incorrect username or password” message on page 2102</td>
</tr>
</tbody>
</table>
### Functions

<table>
<thead>
<tr>
<th>Error number and message (if applicable)</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>denied: requested access to the resource is denied</td>
<td>Deploying a function returns an &quot;error running docker push, are you logged into docker?&quot; message on page 2102</td>
</tr>
<tr>
<td>Fn: error running docker push, are you logged into docker?: exit status 1</td>
<td></td>
</tr>
<tr>
<td>500: Internal server error</td>
<td>Deploying a function returns a ListTriggers message and a 500 error on page 2102</td>
</tr>
<tr>
<td>Image &lt;image-name&gt; does not exist or you do not have access to use it.</td>
<td>Deploying a function returns an &quot;Image does not exist or you do not have access to use it&quot; message on page 2103</td>
</tr>
<tr>
<td>401: Missing subnets annotation</td>
<td>Deploying a function to Oracle Functions returns &quot;Fn: Missing subnets annotation&quot; message on page 2103</td>
</tr>
</tbody>
</table>

### Invoking functions

<table>
<thead>
<tr>
<th>Error number and message (if applicable)</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>502: Function failed</td>
<td>Invoking a function returns a Function failed message and a 502 error on page 2103</td>
</tr>
<tr>
<td>502: Syslog endpoint unavailable</td>
<td>Invoking a function returns a FunctionInvokeSyslogUnavailable message and a 502 error on page 2103</td>
</tr>
<tr>
<td>502: Failed to pull function image</td>
<td>Invoking a function returns a FunctionInvokeImageNotAvailable message and a 502 error on page 2103</td>
</tr>
<tr>
<td>502: subnet ocid1.subnet.... is out of IPs</td>
<td>Invoking a function returns a FunctionInvokeSubnetOutOfRange message and a 502 error on page 2104</td>
</tr>
<tr>
<td>502: subnet ocid1.subnet.... does not exist or Oracle Functions is not authorized to use it</td>
<td>Invoking a function returns a FunctionInvokeSubnetNotAvailable message and a 502 error (due to a subnet issue) on page 2105</td>
</tr>
<tr>
<td>502: dhcp options ocid1.dhcpoptions.... does not exist or Oracle Functions is not authorized to use it</td>
<td>Invoking a function returns a FunctionInvokeSubnetNotAvailable message and a 502 error (due to a DHCP Options issue) on page 2105</td>
</tr>
<tr>
<td>504: Container failed to initialize, please ensure you are using the latest fdk and check the logs 'ModuleNotFoundError: No module named 'contextvars'</td>
<td>Invoking a function returns a FunctionInvokeContainerInitFail error message, a 504 error, and a 'ModuleNotFoundError: No module named 'contextvars' log message on page 2105</td>
</tr>
<tr>
<td>504: Container failed to initialize, please ensure you are using the latest fdk and check the logs</td>
<td>Invoking a function returns FunctionInvokeContainerInitFail and 'Container initialization timed out' messages, and a 504 error on page 2106</td>
</tr>
<tr>
<td>504: Timed out</td>
<td>Invoking a function returns a FunctionInvokeTimeout message and a 504 error on page 2106</td>
</tr>
</tbody>
</table>
**Functions**

- **Miscellaneous**

<table>
<thead>
<tr>
<th>Error number and message (if applicable)</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>error getting credentials - err: exit status 1, out: Error spawning command line <code>dbus-launch --autolaunch...</code></td>
<td>When running Oracle Functions on Ubuntu, Docker login returns an &quot;error getting credentials - err: exit status 1...&quot; message on page 2107</td>
</tr>
</tbody>
</table>

**Issues setting up and running Oracle Functions**

You might encounter these issues when setting up and running Oracle Functions.

**Running Fn Project CLI commands returns a 401 error**

If you see a message similar to the following when running an Fn Project CLI command, double-check that the credentials specified for your current profile in the `~/.oci/config` file are authenticating you correctly:

```
$ fn list apps
Fn: [GET /apps][401] ListApps default &{Fields: Message:Not authenticated}
```

For example:

- Does `user` specify the OCID of your Oracle Cloud Infrastructure user account?
- Does `fingerprint` specify the fingerprint of the public API key value uploaded to the Console?
- Does `key_file` specify the full path to the private key file?

See 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049. Also see API Errors on page 4372.

**Running Fn Project CLI commands returns a 404 error**

If you see a message similar to the following when running an Fn Project CLI command, double-check that you are authorized to access function-related and network resources:

```
$ fn list apps
Fn: [GET /apps][404] ListApps default &{Fields: Message:Resource is not authorized or not found}
```

For example:

- Does `oracle.compartment-id` in your current context correctly specify the OCID of the compartment that owns deployed functions?
- Have policies been set up correctly to give group access to function-related and network resources?
- If you are using a local machine as your Oracle Functions development environment, has your user account been included correctly in the group to which access to function-related and network resources has been granted?
- If you are using an Oracle Cloud Infrastructure compute instance as your Oracle Functions development environment, has the compute instance's OCID been included correctly in the dynamic group that has been granted access to Oracle Cloud Infrastructure Registry?
- Has a policy been set up to give Oracle Functions access to network resources?

See Different Options for Function Development Environments on page 2045. 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053, and Create Policies to Control Access to Network and Function-Related Resources on page 2041. Also see API Errors on page 4372.

**Running Fn Project CLI commands returns an X509: decryption password incorrect error**

If you see a message similar to the following when running an Fn Project CLI command, double-check that the `pass_phrase` specified for your current profile in the `~/.oci/config` file is correct:

```
$ fn list apps
```
Functions

See [2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File](#) on page 2049.

**Performing Docker-related operations with the Fn Project CLI displays an "Error response from daemon... unknown: Unauthorized" message**

To enable the Fn Project CLI to access the Docker registry specified in the Fn Project CLI context, the local Docker client (the Docker daemon on Linux) in your development environment must be logged in to that Docker registry. If the Docker client is not logged in to the Docker registry, you see a message similar to the following:

```
Error response from daemon: Get https://phx.ocir.io/v2/: unknown: Unauthorized
```

Follow the instructions in [10. Log in to Oracle Cloud Infrastructure Registry](#) on page 2057 to log the Docker client in to the appropriate Oracle Cloud Infrastructure Registry, an Oracle-managed Docker registry available in a number of different regions.

**Running an Fn Project CLI command displays an "Fn: asn1:structure error: tags don't match" message**

When running an Fn Project CLI command, you might see a message similar to the following:

```
Fn: asn1: structure error: tags don't match (16 vs {class:1 tag:15 length:112 isCompound:true}) {optional:false explicit:false application:false private:false defaultValue:<nil> tag:<nil> stringType:0 timeType:0 set:false omitEmpty:false} pkcs1PrivateKey @2
```

This message indicates a problem with the format of the private key. Double-check the private key is PEM-encoded by opening the private key file in the ~/.oci directory and confirming that the private key starts with `BEGIN RSA PRIVATE KEY`. For more information about generating keys, see [1. Set up an Oracle Cloud Infrastructure API Signing Key for Use with Oracle Functions](#) on page 2047.

**Running fn version shows that a more recent version of the Fn Project CLI is available**

If you see a message similar to the following when you enter the `fn version` command, a more recent version of the Fn Project CLI is available:

```
$ fn version
Client version: 0.5.33 is not latest: 0.5.34
Server version: ?
```

To upgrade the Fn Project CLI to the most recent version, reinstall the Fn Project CLI by following the instructions in [5. Install the Fn Project CLI](#) on page 2053.

**Issues creating applications and functions**

You might encounter these issues when creating applications and functions with Oracle Functions.

**Creating a new application displays an error message in the New Application dialog**

If you've already reached the limit for the number of applications in your tenancy, you might see a message similar to the following in the New Application dialog when trying to create a new application:

```
Unable to create your app, please try again.
```

Double-check how many applications already exist in your tenancy. Compare that with the number of applications you're allowed to create. See [Oracle Functions Capabilities and Limits](#) on page 2033.

If you've exceeded the number of applications allowed in your tenancy, consider:
• Deleting unwanted applications (see Deleting Applications and Functions on page 2083).
• Requesting an increase to the application limit (see Service Limits on page 215 for instructions).

Issues deploying applications and functions

You might encounter these issues when deploying applications and functions with Oracle Functions.

Deploying an application returns an "unauthorized: incorrect username or password" message

When deploying an application, you might see a message similar to the following:

```sh
$ fn -v deploy --app acme-app
Deploying go-app to app: acme-app
Bumped to version 0.0.2
Building image phx.ocir.io/ansh81vru1zp/acme-repo/go-app:0.0.2
FN_REGISTRY: phx.ocir.io/ansh81vru1zp/acme-repo
Current Context: acme-functions-compartment
Sending build context to Docker daemon 5.12kB
Step 1/10 : FROM fnproject/go:dev as build-stage
Get https://registry-1.docker.io/v2/fnproject/go/manifests/dev:
  unauthorized: incorrect username or password
```

The message indicates an unnecessary and unsuccessful attempt to log in to Docker Hub. To resolve this situation, log out from Docker using the following command:

```sh
docker logout
```

Having logged out from Docker, re-run the command to deploy the application.

Deploying a function returns an "error running docker push, are you logged into docker?" message

If you see a message similar to the following when deploying a function, double-check that your development environment doesn't have the FN_REGISTRY environment variable set to your Docker username:

```sh
The push refers to repository [docker.io. ... .
  ...
  denied: requested access to the resource is denied
Fn: error running docker push, are you logged into docker?: exit status 1
See fn <command> --help' for more information.
```

If you have used the open source Fn Project platform, you might have followed instructions in the Fn Project documentation to set the FN_REGISTRY environment variable to your Docker username to enable interaction with the official Docker registry (docker.io).

The FN_REGISTRY environment variable overrides the value of the registry option in your Fn Project CLI context.

To use the Fn Project CLI with Oracle Functions, do one of the following:

• Unset the FN_REGISTRY environment variable.
• Override the FN_REGISTRY environment variable using the --registry global option whenever you enter an Fn Project CLI command that interacts with Oracle Cloud Infrastructure Registry.

Deploying a function returns a ListTriggers message and a 500 error

When deploying a function that you've previously created using an earlier version of the Fn Project CLI, you might see a message similar to the following:

```sh
Fn: [GET /triggers][500] ListTriggers default &{Fields: Message:Internal server error}
```
This message indicates that the function's `func.yaml` file contains one or more HTTP trigger definitions. Oracle Functions does not currently support HTTP triggers. To deploy the function, remove the `triggers:` section from the `func.yaml` file.

To avoid creating new `func.yaml` files containing trigger definitions, follow the instructions in 5. Install the Fn Project CLI on page 2053 to upgrade the Fn Project CLI to the most recent version.

**Deploying a function returns an "Image does not exist or you do not have access to use it" message**

When deploying a function using an Oracle Cloud Infrastructure compute instance as your Oracle Functions development environment, you might see a message similar to the following:

```
Fn: Image phx.ocir.io/ansh8lvrulzp/acme-repo/helloworld-func:0.0.2 does not exist or you do not have access to use it.
```

This message indicates that the compute instance does not have access to Oracle Cloud Infrastructure Registry. Double-check that a policy statement (similar to the one below) exists in the tenancy's root compartment to allow a dynamic group that includes the compute instance's OCID to access Oracle Cloud Infrastructure Registry:

```
Allow dynamic-group <dynamic-group-name> to read repos in tenancy
```

For more information about using an Oracle Cloud Infrastructure compute instance as your development environment, see Different Options for Function Development Environments on page 2045.

**Deploying a function to Oracle Functions returns "Fn: Missing subnets annotation" message**

When you deploy a function to Oracle Functions, you might see the following message:

```
$ fn deploy --app joes-helloworld-app
Deploying helloworld-func to app: joes-helloworld-app.
.
.
Fn: Missing subnets annotation
```

If you see the `Fn: Missing subnets annotation` message, confirm that you entered the correct application name. For example:

- the application might not be in the compartment currently specified by the Fn Project CLI context
- the application might have existed previously, but has subsequently been deleted

**Issues invoking functions**

You might encounter these issues when invoking functions deployed to Oracle Functions.

**Invoking a function returns a Function failed message and a 502 error**

If there is a problem with a function's code, you will see the following error when you invoke the function:

```
Fn: Error invoking function. status: 502 message: Function failed
```

To investigate the issue with the function's code, check the logs output by the function. The Oracle Cloud Infrastructure Logging service is the default and recommended option for accessing, searching, and storing function logs. Note that to store and view logs for a function, the function must include print statements. For more information, see Storing and Viewing Function Logs on page 2078.

**Invoking a function returns a FunctionInvokeSyslogUnavailable message and a 502 error**

Oracle Functions enables you to send a function's logs to an external logging destination (like Papertrail) by setting a syslog URL for the application. See Storing and Viewing Function Logs on page 2078.
Functions

If the syslog URL is invalid or unreachable, you will see the following error when you invoke the function:
{"code":"FunctionInvokeSyslogUnavailable","message":"Syslog endpoint
unavailable"}
Fn: Error invoking function. status: 502 message: Syslog endpoint
unavailable
To confirm that the external logging destination's URL is the cause of the error:
1. Update the application to unset the syslog URL using the Fn Project CLI. For example, by entering:
fn update app helloworld-app --syslog-url ''
2. Deploy the function you want to run. See Creating and Deploying Functions on page 2063.
3. Invoke the function. See Invoking Functions on page 2071.
If the function runs successfully, the external logging destination's URL is not reachable from the subnet in which the
function is running. Double-check that:
•
•
•

The external logging destination's URL is valid.
The external logging destination's URL is publicly accessible.
The subnet in which the function is running has outbound access to the public internet.

Invoking a function returns a FunctionInvokeImageNotAvailable message and a 502 error
When you invoke a function, Oracle Functions pulls the corresponding image from Oracle Cloud Infrastructure
Registry using the VCN and subnets specified for the application.
If Oracle Functions is unable to pull the image, the following message is returned when you invoke a function:
{"code":"FunctionInvokeImageNotAvailable","message":"Failed to pull function
image"}
Fn: Error invoking function. status: 502 message: Failed to pull function
image

Possible solutions:
•
•
•

Double-check that the image specified for the function still exists in the specified location in Oracle Cloud
Infrastructure Registry.
Double-check that Oracle Cloud Infrastructure is available (this message is returned if Oracle Cloud Infrastructure
is unexpectedly unavailable).
Double-check that the VCN includes an internet gateway or service gateway. For Oracle Functions to be able
to access Oracle Cloud Infrastructure Registry to pull an image, the VCN must include an internet gateway or a
service gateway, as follows:
•

•

If public subnets were specified for the application, the VCN must also include an internet gateway. A route
table must include a route rule that targets the internet gateway, with its Destination CIDR Block property set
to 0.0.0.0/0. A security list must include a stateful egress rule that allows access to Oracle Cloud Infrastructure
Registry (for example, with its Destination Type property set to Service, its Destination Service property
set to All <region> services In Oracle Services Network, and its IP Protocol property set
to All).
If private subnets were specified for the application, the VCN must also include a service gateway. The
service gateway must be set up to allow access to All <region> Services In Oracle Services
Network. A route table must include a route rule that targets the service gateway, with its Destination
Service property set to All <region> Services In Oracle Services Network. A security
list must include a stateful egress rule that allows access to Oracle Cloud Infrastructure Registry (for example,

Oracle Cloud Infrastructure User Guide

2104


Functions

with its Destination Type property set to Service, its Destination Service property set to All <region>
services In Oracle Services Network, and its IP Protocol property set to All).
If an internet gateway or service gateway has not been defined for the VCN already, define one now.
Invoking a function returns a FunctionInvokeSubnetOutOfIPs message and a 502 error
When you invoke a function that you've deployed to Oracle Functions, you might see the following error message:
{"code":"FunctionInvokeSubnetOutOfIPs","message":"subnet
ocid1.subnet.oc1.phx.aaaaaaaac... is out of IPs"}
Fn: Error invoking function. status: 502 message: subnet
ocid1.subnet.oc1.phx.aaaaaaaac... is out of IPs
If you see this error, double-check that each subnet in the VCN has at least the required minimum number of free IP
addresses specified in Create the VCN and Subnets to Use with Oracle Functions, if they don't exist already on page
2040.
Invoking a function returns a FunctionInvokeSubnetNotAvailable message and a 502 error (due to a
subnet issue)
When you invoke a function that you've deployed to Oracle Functions, you might see the following error message:
{"code":"FunctionInvokeSubnetNotAvailable","message":"subnet
ocid1.subnet.oc1.phx.aaaaaaaac... does not exist or Oracle Functions is not
authorized to use it"}
Fn: Error invoking function. status: 502 message: subnet
ocid1.subnet.oc1.phx.aaaaaaaac... does not exist or Oracle Functions is not
authorized to use it
If you see this error, double-check that the subnet specified for the application still exists.
Invoking a function returns a FunctionInvokeSubnetNotAvailable message and a 502 error (due to a
DHCP Options issue)
When you invoke a function that you've deployed to Oracle Functions, you might see the following error message:
{"code":"FunctionInvokeSubnetNotAvailable","message":"dhcp options
ocid1.dhcpoptions.oc1.phx.aaaaaaaac... does not exist or Oracle Functions
is not authorized to use it"}
Fn: Error invoking function. status: 502 message: dhcp options
ocid1.dhcpoptions.oc1.phx.aaaaaaaac... does not exist or Oracle Functions
is not authorized to use it
If you see this error, double-check that the set of DHCP Options in the VCN specified for the application still exists.
Invoking a function returns a FunctionInvokeContainerInitFail error message, a 504 error, and a
'ModuleNotFoundError: No module named 'contextvars'' log message
When you invoke a Python 3.6 function that you've deployed to Oracle Functions, you might see the following error
message:
{"code":"FunctionInvokeContainerInitFail","message":"Container failed to
initialize, please ensure you are using the latest fdk and check the logs"}
Fn: Error invoking function. status: 504 message: Container failed to
initialize, please ensure you are using the latest fdk and check the logs
If you see this error, check the function's logs. If you see a "ModuleNotFoundError: No module named
'contextvars' message in the function's logs:

Oracle Cloud Infrastructure User Guide

2105


1. Add the following line to the function's requirements.txt file:

   fdk>=0.1.21

2. Re-deploy the function to Oracle Functions.
3.Invoke the function again.

**Invoking a function returns FunctionInvokeContainerInitFail and 'Container initialization timed out' messages, and a 504 error**

When you invoke a function that you've deployed to Oracle Functions, the function execution is subject to a maximum memory threshold. If this limit is exceeded, function execution stops and the following error message is returned:

```
{
  "code":"FunctionInvokeContainerInitFail","message":"Container failed to initialize, please ensure you are using the latest fdk and check the logs"
}
```

Fn: Error invoking function. status: 504 message: Container failed to initialize, please ensure you are using the latest fdk and check the logs

If you see this error, increase the maximum memory threshold when you invoke the function. Valid values for the maximum memory threshold are 128MB, 256MB, 512MB, and 1024MB (see [Changing Oracle Functions Default Behavior](#) on page 2095).

For example, to set a function's maximum memory threshold to 256MB, do one of the following:

- Click **Edit Function** on the **Function Details** page in the Console, and select **256** from the **Memory (in MBs)** drop-down list.
- Add the following line to the function's func.yaml file. This will set the maximum memory threshold to 256MB whenever the function is invoked:

```
memory: 256
```

Note that if you edit the func.yaml file, you must re-deploy the function to Oracle Functions before invoking it again.

It's a good idea to use the latest version of the Fn Project CLI when creating a helloworld Python function. When you enter the `fn init --runtime python <function-name>` command to create the helloworld function, the line `memory: 256` is added to the func.yaml file automatically.

**Invoking a function returns a FunctionInvokeTimeout message and a 504 error**

When you invoke a function that you've deployed to Oracle Functions, the function is only allowed to run for a certain amount of time. If this time limit is exceeded, function execution stops and the following error message is returned:

```
{
  "code":"FunctionInvokeTimeout","message":"Timed out"
}
```

Fn: Error invoking function. status: 504 message: Timed out

If you see this error, increase the maximum time a function is allowed to run for. For example, to set the maximum time to 120 seconds, do one of the following:

- Click **Edit Function** on the **Function Details** page in the Console, and enter **120** in the **Timeout** field.
- Add the following line to the function's func.yaml file. This will set the maximum time limit to 120 seconds whenever the function is invoked:

```
timeout: 120
```

Note that if you edit the func.yaml file, you must re-deploy the function to Oracle Functions before invoking it again.
You might also see this error message when a function running in a public subnet is unable to connect to an Oracle Autonomous Database instance that has access control lists (ACLs) enabled. If this is the case, see Connecting to Oracle Autonomous Database Instances from Running Functions on page 2093 for more information about:

- Configuring the subnet to send all outgoing internet traffic to a NAT gateway, and to allow internet traffic.
- Adding the NAT gateway's public IP address to the database's access control list.

Miscellaneous issues when using Oracle Functions

You might encounter these miscellaneous issues when using Oracle Functions.

When running Oracle Functions on Ubuntu, Docker login returns an "error getting credentials - err: exit status 1..." message

When you configure your development environment for Oracle Functions, you have to install Docker (see 4. Install Docker for Use with Oracle Functions on page 2052). If your development environment is running Ubuntu, when you follow the subsequent instructions to log in to Oracle Cloud Infrastructure Registry using Docker (see 10. Log in to Oracle Cloud Infrastructure Registry on page 2057), you might see a message similar to the following:

```
error getting credentials - err: exit status 1, out: Error spawning command line 'dbus-launch --autolaunch=d7159335070ef1c0854c75de55c8f588 --binary-syntax --close-stderr': Child process exited with code 1
```

For more information about this Docker issue, including likely causes and possible resolutions, see https://github.com/docker/docker-credential-helpers/issues/60.

Function Metrics

You can monitor the health, capacity, and performance of functions you've deployed to Oracle Functions by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace `oci.faas` (the Oracle Functions service).

Resources: functions

Overview of the Oracle Functions Service Metrics

Oracle Functions monitors function execution, and collects and reports metrics such as:

- The number of times a function is invoked.
- The length of time a function runs for.
- The number of times a function failed.
- The number of requests to invoke a function that returned a '429 Too Many Requests' error in the response (known as 'throttled function invocations').

Prerequisites

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

For more information about the policy statement required to access metrics emitted by Oracle Functions, see Create a Policy to Give Oracle Functions Users Access to Function-Related Resources on page 2043.

Available Metrics: oci.faas

The metrics listed in the following tables are automatically available for any functions you create. You do not need to enable monitoring on the resource to get these metrics.
Oracle Functions metrics include the following dimensions:

**APPLICATIONID**

The *OCID* of the application containing functions.

**RESOURCEID**

The *OCID* of the function.

**RESPONSETYPE**

The response when a function is invoked (one of Success, Error, or Throttled).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>FunctionExecutionDuration</td>
<td>Function Duration</td>
<td>ms</td>
<td>Total function execution duration. Expressed in milliseconds.</td>
<td>applicationId, resourceId</td>
</tr>
<tr>
<td>FunctionInvocationCount</td>
<td>Function Invocations</td>
<td>count</td>
<td>Total number of function invocations.</td>
<td>applicationId, resourceId</td>
</tr>
<tr>
<td>FunctionResponseCount</td>
<td></td>
<td>count</td>
<td>Total number of function responses.</td>
<td>applicationId, resourceId</td>
</tr>
</tbody>
</table>

**Using the Console**

**To view default metric charts for a single function**

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Functions.
2. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that’s specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).
3. Select the compartment containing the application with functions for which you want to view metrics.
   The Applications page shows all the applications in the compartment you selected.
4. Click the name of the application containing the function for which you want to view metrics.
5. Click the name of the function for which you want to view metrics.

   The Metrics page displays a chart for each metric that is emitted by the metric namespace for Oracle Functions. For more information about the emitted metrics, see Available Metrics: oci_faaas on page 2107.

   For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**Not seeing the function metrics data you expect?**

If you don't see the metrics data for a function that you expect, see the following possible causes and resolutions.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing functions: A function I invoked is missing from the Invocations chart.</td>
<td>The chart range (time period or x-axis window) does not cover the time of invocation.</td>
<td>Adjust the chart range or time period as necessary.</td>
</tr>
<tr>
<td>Gaps in metrics data: The chart line is discontinuous. I want to see data in the charts as a continuous line over time, but the line has gaps in it.</td>
<td>No metrics data exist in the times indicated by the gaps.</td>
<td>Smooth out the display by increasing the chart interval to see if gaps are removed.</td>
</tr>
<tr>
<td>Empty charts: The Errors and Throttles charts never show data.</td>
<td>No metrics data exists for these charts in the specified chart range. No errors have occurred, and no requests have been throttled. Empty Errors and Throttles charts are expected.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Throttles data: The Throttles chart shows data. What should I do?</td>
<td>Data in the Throttles chart indicates at least one request to invoke a function returned a ‘429 Too Many Requests’ error in the response.</td>
<td>Resubmit the throttled invocation requests. Submit future invocation requests less frequently.</td>
</tr>
</tbody>
</table>

**To view default metric charts for all functions in an application**

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.
2. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see **6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure** on page 2053).
3. Select the compartment containing the application for which you want to view function metrics.
   
   The **Applications** page shows all the applications in the compartment you selected.
4. Click the name of the application for which you want to view function metrics.
5. Under **Resources**, click **Metrics**.
   
   The Metrics page displays a chart for each metric that is emitted by the metric namespace for Oracle Functions. For more information about the emitted metrics, see **Available Metrics: oci_faaas** on page 2107.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**To view default metric charts for all the functions in all the applications in a compartment**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

3. Select the compartment containing the applications for which you want to view function metrics.

4. For Metric Namespace, select `oci_faas`.

   The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace. For more information about the emitted metrics, see Available Metrics: `oci_faas` on page 2107.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)
Chapter 20

Health Checks

This chapter explains how to monitor the health of your endpoints.

Overview of the Health Checks Service

The Oracle Cloud Infrastructure Health Checks service provides users with high frequency external monitoring to determine the availability and performance of any publicly facing service, including hosted websites, API endpoints, or externally facing load balancers. By using Health Checks, users can ensure that they are immediately aware of any availability issue affecting their customers.

Health Checks Service Components

The following list describes the key components used in creating a health check.

**MONITORS**

Monitors allow you to continuously monitor the health of public-facing endpoints. You can configure monitors to use either HTTP and ping protocols. Monitors are classified as either Basic or Premium, based on the configured test interval. A monitor is considered Premium if the test interval is set to 10 seconds, and considered Basic if the test interval is greater than 10 seconds. Behavioral differences do not exist between a Basic and Premium monitor, other than the frequency that the monitor is run.

**ON-DEMAND PROBES**

On-demand probes allow you to run a one-time probe to assess the health of a public-facing endpoint. You can configure on-demand probes to use either or both HTTP and ping protocols. This feature is only available through the REST API. A limit exists on how many on-demand probes can be run in a 24-hour period. On-demand credits are consumed as the probes are run, and replenished gradually over time.

**VANTAGE POINTS**

Vantage points are geographic locations from which monitors and probes can be run to your specified target. Oracle Cloud Infrastructure maintains dozens of vantage points around the world.

**PROTOCOLS**

The Health Checks service allows you to configure both HTTP and ping type monitors. Each type has respective protocols.

Ways to Access the Health Checks Service

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide.

To access the Console, you must use a supported browser. You can use the Console link at the top of this page to go to the sign-in page. Enter your tenancy, user name, and your password.
Health Checks

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you're a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Health Checks Service Capabilities and Limits

The Oracle Cloud Infrastructure Health Checks service is limited to 1000 endpoint tests per account.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Required IAM Service Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies. For more details about policies for Health Checks, see Details for the Health Checks Service on page 2278.

Policy examples:

- To enable all operations on Health Checks for all users in a tenant:

  Allow any-user to manage health-check-family in tenancy

- To enable all operations on Health Checks for all users in a compartment:

  Allow any-user to manage health-check-family in compartment <Compartment Name>

- To enable all operations on Health Checks for a specific user group:

  Allow group <Your Group Name> to manage health-check-family in compartment <Compartment Name>

Moving Health Checks to a Different Compartment

You can move health checks from one compartment to another. When you move a health check to a new compartment, its associated monitor and test results moves with it. After the move, health checks are accessible through the SDK, CLI, and Console. For more information, see Managing Compartments on page 2431.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.
Getting Started With the Health Checks API

The Health Checks service allows you to configure and deploy monitors and on-demand probes using the Health Checks API. Use the following guide to learn how to set up monitors and probes then retrieve their results using the REST API.

**Note:**
Monitors, metrics, and probes created with the API, SDK and CLI are associated with the region where they were configured. While using the API, you must perform monitor updates (including compartment changes), metrics retrieval, and probe results retrieval in the region where they were configured. However, you can get a list of currently configured monitors and monitor details in every region, no matter where the monitors were configured.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Endpoints

The Health Checks API can be accessed via the following endpoints:

- https://healthchecks.ap-chuncheon-1.oraclecloud.com/20180501
- https://healthchecks.ap-hyderabad-1.oraclecloud.com/20180501
- https://healthchecks.ap-melbourne-1.oraclecloud.com/20180501
- https://healthchecks.ap-mumbai-1.oraclecloud.com/20180501
- https://healthchecks.ap-osaka-1.oraclecloud.com/20180501
- https://healthchecks.ap-seoul-1.oraclecloud.com/20180501
- https://healthchecks.ap-sydney-1.oraclecloud.com/20180501
- https://healthchecks.ap-tokyo-1.oraclecloud.com/20180501
- https://healthchecks.ca-montreal-1.oraclecloud.com/20180501
- https://healthchecks.ca-toronto-1.oraclecloud.com/20180501
- https://healthchecks.eu-amsterdam-1.oraclecloud.com/20180501
- https://healthchecks.eu-frankfurt-1.oraclecloud.com/20180501
- https://healthchecks.eu-zurich-1.oraclecloud.com/20180501
- https://healthchecks.me-dubai-1.oraclecloud.com/20180501
- https://healthchecks.me-jeddah-1.oraclecloud.com/20180501
- https://healthchecks.sa-santiago-1.oraclecloud.com/20180501
- https://healthchecks.sa-saopaulo-1.oraclecloud.com/20180501
- https://healthchecks.uk-cardiff-1.oraclecloud.com/20180501
- https://healthchecks.uk-london-1.oraclecloud.com/20180501
- https://healthchecks.us-ashburn-1.oraclecloud.com/20180501
- https://healthchecks.us-phoenix-1.oraclecloud.com/20180501
Health Checks

Available Protocols For Probes and Monitors

You can configure monitors and probes to use HTTP or ping requests. You will need to ensure that the endpoint being monitored is configured to accept the specified protocol.

**HTTP** - Configure a GET or HEAD request using HTTP/1.1 to test the target for availability. The probe results are returned in JSON and include the HTTP Status Code and DNS lookup, connection and response timings.

**HTTPS** - Configure an encrypted HTTPS GET or HEAD request to test the availability of any secure hosted target. Defaults to port 443. The probe results are returned in JSON and include the HTTP Status Code and DNS lookup, connection and response timings.

**ICMP** - Configure an ICMP echo request ping. The results include the round trip time (RTT) latency.

**TCP** - Configure a TCP handshake to the specified end point. You should be sure to own this endpoint as testing this connection can be costly to the recipient. The results include the round trip time (RTT) latency.

Create A Monitor

Monitors allow you to monitor the health of endpoints over time. The following example shows how to create an HTTPS monitor that checks the health of www.example.com at an interval of every 30 seconds using a GET request.

```json
POST /20180501/httpMonitors
{
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "protocol": "HTTPS",
    "port": 443,
    "targets": [
        "www.example.com"
    ],
    "timeoutInSeconds": 30,
    "method": "GET",
    "displayName": "Example HTTP monitor",
    "intervalInSeconds": 30
}
```

Targets can be either hostnames or IP addresses and the `path` field can be used to specify an optional path, such as `www.example.com/project/help.htm`. Optionally, you can specify which geographic locations you would like the monitor to launch from by using the `vantagePointNames` field. At least one vantage point must be listed when using this field. For a list of available vantage points, see Vantage Points on page 2117.

A 200 response will be returned with the successful creation of a probe and the results of the probe can be retrieved from the URL in the `resultsUrl` field of the response.

```json
{
    "id": "ocid1.httpmonitor.OC2..<unique_ID>",
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "resultsUrl": "https://healthchecks.us-ashburn-1.oraclecloud.com/20180501/httpProbeResults/ocid1.httpmonitor.OC2..<unique_ID>",
    "targets": [
        "www.example.com",
        "www.oracle.com"
    ],
    "vantagePointNames": [
        "ibm-sjc",
        "aws-dub",
        "dgo-nyc"
    ],
    "protocol": "HTTPS",
    "timeoutInSeconds": 30,
    "displayName": "Example Monitor",
```
Health Checks

For more information about creating an HTTP monitor, see CreateHttpMonitor.

**Note:**
You can configure a similar style monitors using TCP or ICMP protocols. For more information, see CreatePingMonitor.

Create An On-Demand Probe

Probes are one-off health assessments of an endpoint that can be deployed at anytime. The following example shows how to create an on-demand HTTP probe that checks the health of www.example.com with a GET request.

```
POST /20180501/httpProbeResults
{
   "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
   "protocol": "HTTP",
   "targets": [
      "www.example.com"
   ],
   "timeoutInSeconds": 30,
   "method": "GET"
}
```

Targets can be either hostnames or IP addresses and the path field can be used to specify an optional path, such as www.example.com/project/help.htm. Additionally, you can specify which geographic locations you would like the probe to launch from by using the vantagePointNames field. For a list of available vantage points, see Vantage Points on page 2117.

A 200 response will be returned with the successful creation of a probe and the results of the probe can be retrieved from the URL in the resultsUrl field of the response. It will take a few moments for results to display once the tests have been configured.

```
{
   "id":"ocid1.pingprobe.OC2..<unique_ID>",
   "compartmentId":"ocid1.compartment.oc1..<unique_ID>",
   "resultsUrl":"https://healthchecks.us-ashburn-1.oraclecloud.com/20180501/pingProbeResults/ocid1.pingprobe.OC2..<unique_ID>",
   "targets":[
      "www.example.com"
   ],
   "vantagePointNames": [
      "ibm-sjc",
      "aws-dub",
      "dgo-nyc"
   ],
   "protocol":"ICMP",
   "timeoutInSeconds":30
}
```

For more information about creating a probe, see CreateOnDemandHttpProbe.

**Note:**
You can configure similar style probes using TCP or ICMP protocols. For more information, see CreateOnDemandPingProbe.
Health Checks

Retrieving Probe And Monitor Results

Probe and monitor results can be retrieved from URL in the `resultsUrl` field of a monitor or probe creation response. It will take a few moments for results to display once the tests have been configured. Results can also be retrieved at anytime using the following methods:

- **ListPingProbeResults** - For monitors or on-demand probes using TCP or ICMP protocols.
- **ListHttpProbeResults** - For monitors or on-demand probes using HTTP protocols.

Retrieving results for an on-demand probe or monitor requires the probe or monitor's configuration ID as a parameter. On-demand probe and configuration IDs are assigned upon their creation and are returned in the id field of the POST response. You can also use the **ListHttpMonitor** method to retrieve a list of currently configured monitors and probes using HTTP protocols. Use the **ListPingMonitors** method to retrieve a list of currently configured monitors and probes using TCP and ICMP protocols.

The following is an example of results retrieved using `GET /httpProbeResults/ {probeConfigurationId}`.

```
{
    "key": "651b9f3a46041cace0530204060ae27e",
    "probeConfigurationId": "ocid1.httpmonitor.OC2..<unique_ID>",
    "startTime": 1517323711505,
    "target": "www.example.com",
    "vantagePointName": "dgo-nyc",
    "protocol": "HTTPS",
    "connection": {
        "connectDuration": 114,
        "secureConnectDuration": 99,
        "address": "93.184.216.34",
        "port": 443
    },
    "dns": {
        "domainLookupDuration": 29,
        "addresses": [
            "93.184.216.34",
        ]
    },
    "statusCode": 200,
    "fetchStart": 1517323711505,
    "domainLookupStart": 1517323711505,
    "domainLookupEnd": 1517323711534,
    "connectStart": 1517323711535,
    "secureConnectionStart": 1517323711550,
    "connectEnd": 1517323711649,
    "requestStart": 1517323711649,
    "responseStart": 1517323711673,
    "responseEnd": 1517323711676,
    "duration": 171,
    "encodedBodySize": 1270,
    "isTimedOut": false,
    "isHealthy": true
}
```

Vantage Points

Vantage points are geographic locations from which monitors and probes can be launched. Oracle Cloud Infrastructure maintains vantage points on the infrastructure of cloud providers around the world, including AWS, IBM, and Azure. The list below is a sampling of the vantage points available. The list of vantage points is dynamic and changes frequently. Use the **ListHealthChecksVantagePoints** method to return a list of available vantage points.
## Managing Health Checks

The Health Checks service allows you to monitor the health of IP addresses and hostnames, as measured from geographic vantage points of your choosing, using HTTP and ping probes. After configuring a health check, you can view the monitor's results. The results include the location from which the host was monitored, the availability of the endpoint, and the date and time the test was performed.

### Using the Console

To add a health check

<table>
<thead>
<tr>
<th>Provider</th>
<th>Location</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Singapore</td>
<td>aws-sin</td>
</tr>
<tr>
<td>Amazon</td>
<td>Sao Paolo</td>
<td>aws-sao</td>
</tr>
<tr>
<td>Amazon</td>
<td>Dublin</td>
<td>aws-dub</td>
</tr>
<tr>
<td>Amazon</td>
<td>San Francisco</td>
<td>aws-sfo</td>
</tr>
<tr>
<td>Azure</td>
<td>Dublin</td>
<td>azr-dub</td>
</tr>
<tr>
<td>Azure</td>
<td>Amsterdam</td>
<td>azr-ams</td>
</tr>
<tr>
<td>Azure</td>
<td>Singapore</td>
<td>azr-sin</td>
</tr>
<tr>
<td>Azure</td>
<td>Sydney</td>
<td>azr-syd</td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>Toronto</td>
<td>dgo-yyz</td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>Frankfurt</td>
<td>dgo-fra</td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>New York City</td>
<td>dgo-nyc</td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>Biratnagar, Nepal</td>
<td>dgo-blr</td>
</tr>
<tr>
<td>Google</td>
<td>Taiwan</td>
<td>goo-tpe</td>
</tr>
<tr>
<td>Google</td>
<td>Brussels</td>
<td>goo-bru</td>
</tr>
<tr>
<td>Google</td>
<td>Council Bluffs, IA</td>
<td>goo-cbf</td>
</tr>
<tr>
<td>Google</td>
<td>Charleston, SC</td>
<td>goo-chs</td>
</tr>
<tr>
<td>IBM</td>
<td>San Jose, CA</td>
<td>ibm-sjc</td>
</tr>
<tr>
<td>IBM</td>
<td>Tokyo</td>
<td>ibm-hnd</td>
</tr>
<tr>
<td>IBM</td>
<td>Dallas, TX</td>
<td>ibm-dfw</td>
</tr>
<tr>
<td>IBM</td>
<td>Hong Kong</td>
<td>ibm-hkg</td>
</tr>
<tr>
<td>Rack Space</td>
<td>Ashburn, VA</td>
<td>rck-iad</td>
</tr>
<tr>
<td>Rack Space</td>
<td>Dallas, TX</td>
<td>rck-dfw</td>
</tr>
<tr>
<td>Rack Space</td>
<td>London</td>
<td>rck-lhr</td>
</tr>
<tr>
<td>Rack Space</td>
<td>Sydney</td>
<td>rck-syd</td>
</tr>
</tbody>
</table>

**Important:**

If you have selected the HTTPS protocol for this monitor and have entered an IP address as a Target to be monitored, you must specify a Host header with the domain name associated with the TLS certificate for that target. If you do not add the Host header, the TLS connection phase will not complete.
Health Checks

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Click Create Health Check.
3. In the Create Health Check dialog box, enter the following:
   - **Health Check Name**: The name used for the health check. Avoid entering confidential information.
   - **Compartment**: Select the compartment the health check runs in.
   - **Target(s)**: The IP address or fully qualified domain name (FQDN) of the host being monitored. Additional targets can be added.
   - **Vantage Points**: Select the location from which the health of the target is monitored. No more than ten vantage points can be added.
   - **Request Type**: Select the type of request sent to monitor the target.
     - **HTTP** - Enter the following:
       - **Protocol**: The network protocol used to interact with your endpoint, such as HTTP protocol, which initializes an HTTP handshake with your endpoint.
       - **Port**: The port for the monitor to look for a connection. The default is port 80 for HTTP. For HTTPS, use port 443.
       - **Path**: The specific path on the target to be monitored.
       - **Header Name**: (Optional) The name displayed in the request header as part of the health check. Avoid entering confidential information.
       - **Header Value**: (Optional) Specifies the data requested by the header. Click + Add Header to add multiple headers in succession.
       - **Method**: Select the HTTP method used for the health check.
       - **Timeout**: Select the maximum time to wait for a reply before marking the health check as failed.
       - **Interval**: Select the period of time between health checks of the target.
     - **Ping** - Enter the following:
       - **Protocol**: The network protocol used to interact with your endpoint, such as HTTP protocol, which initializes an HTTP handshake with your endpoint.
       - **Port**: If you have selected the TCP protocol, enter the port for the monitor to look for a connection. The default port is 80.
       - **Timeout**: Select the maximum time to wait for a reply before marking the health check as failed.
       - **Interval**: Select the period of time between health checks of the target.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
4. Click Create Health Check.

The health check is added to the health check list. To view more details, click the health check name. It will take a few moments for results to display once the tests have been configured.

**To edit a health check**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Select the check box for the health check you want to edit.
3. Select Edit from the Actions drop-down menu.
4. In the Edit Health Check dialog box, make the needed changes, and then click Edit Health Check.
Health Checks

To disable a health check

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Select the check box for the health check you want to disable.

   Tip:
   To help find a health check, you can enter the name of the health check in the Search field.

3. Select Disable from the Actions drop-down menu.

   The status of the health check changes to Disabled in the health check list.

To duplicate a health check

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Select the check box for the health check you want to duplicate.
3. Select Duplicate from the Actions drop-down menu.
4. In the Create Health Check dialog box, make any updates to the duplicated health check, and then click Create Health Check.

To delete a health check

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Select the check box for the health check you want to delete.

   Tip:
   To help find a health check, you can enter the name of the health check in the Search field.

3. Select Delete from the Actions drop-down menu.
4. In the confirmation dialog box, click Delete.

To view the history of a health check

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Click the name of the health check you want to view.

   The Health Check history displays a list of results for the past 90 days.

   Tip:
   To help find a result, you can use the Start Date, Start Time, End Date, End Time, and Targets filter options.

3. Click the drop-down arrow beside the Timestamp to view the monitor result details. You can use the API to download the data.

To manage tags for a health check

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. Click the name of the health check you want to view.
3. Click the Tags tab to view or edit the existing tags. Or click Apply tag(s) to add new ones.

   For more information, see Resource Tags on page 211.

To move a health check to a different compartment

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Health Checks.
2. In the Scope section, select a compartment.
3. Find the health check in the list, click the Actions icon (three dots), and then click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.

   For more information, see Managing Compartments on page 2431.
Tip:
If your health checks are continually failing, please ensure that you have permission to monitor the host and that the ports on the host have been configured to receive traffic from Health Checks.

Using the API

For information about using the API and signing requests, see REST APIs and Security Credentials. For information about SDKs, see Software Development Kits and Command Line Interface.

• Use the CreateHTTPMonitor operation to create a Health Check monitor that uses the HTTP protocol.
• Use the CreatePingMonitor operation to create a Health Check monitor that uses the ping protocol.
• Use the ListHealthChecksVantagePoints to retrieve a list of available vantage points from which to execute monitors.
• Use the UpdateHttpMonitor operation to update the configuration of an HTTP health check monitor. You can also use this operation to disable an HTTP monitor by setting the isEnabled field to false.
• Use the UpdatePingMonitor operation to update the configuration of ping health check monitor. You can also use this operation to disable a ping monitor by setting the isEnabled field to false.
• Use the DeleteHttpMonitor operation to remove an HTTP health check monitor from your setup.
• Use the DeletePingMonitor operation to remove a ping health check monitor from your setup.
• Use the ListHttpProbeResults operation to retrieve the results of an HTTP health check monitor.
• Use the ListPingProbeResults operation to retrieve results of a ping health check monitor.

Health Checks Metrics

You can monitor the health, capacity, and performance of your health checks by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace oci_healthchecks (the Health Checks service).

Overview of the Health Checks Service Metrics

Oracle Cloud Infrastructure Health Checks provides users with high frequency external monitoring to determine the availability and performance of any publicly facing service, including hosted websites, API endpoints, or externally facing load balancers. The Health Checks service metrics help you monitor the performance of your endpoints over a 24 hour period.

Prerequisites

• IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_healthchecks

The metrics listed in the following table are automatically available for each health check that you create. You do not need to enable monitoring on the health check to get these metrics.

Each metric includes the following dimensions:

RESOURCEID

The OCID of the policy to which the metric applies.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PING.isHealthy</td>
<td>Ping Test Success Rate</td>
<td>percent</td>
<td>Displays availability of end point being monitored.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage icmpCode</td>
</tr>
<tr>
<td>HTTP.DNSLookupTime</td>
<td>HTTP(S) DNS Lookup Time</td>
<td>ms</td>
<td>The time taken for domain name lookup in milliseconds.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage icmpCode</td>
</tr>
<tr>
<td>HTTP.TCPConnectTime</td>
<td>HTTP(S) Connection Duration</td>
<td>ms</td>
<td>The total TCP connection duration for the test which applies to both HTTP and HTTPS protocols.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage</td>
</tr>
<tr>
<td>HTTP.RequestTime</td>
<td>HTTP(S) Request Duration</td>
<td>ms</td>
<td>The total duration of the request in milliseconds.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage</td>
</tr>
<tr>
<td>HTTP.ResponseTime</td>
<td>HTTP(S) Response Duration</td>
<td>ms</td>
<td>The total duration of response in milliseconds.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage</td>
</tr>
<tr>
<td>HTTP.TotalDuration</td>
<td>HTTP(S) Total Duration</td>
<td>ms</td>
<td>The total duration of the test run in milliseconds.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage</td>
</tr>
<tr>
<td>PING.Latency</td>
<td>Ping Latency Measurement</td>
<td>ms</td>
<td>Latency measurement for ping test in milliseconds.</td>
<td>target vantagePoint resourceId resourceDisplayName protocol errorMessage</td>
</tr>
</tbody>
</table>

**Using the Console**

To view metric charts for resources related to a health check monitor

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Health Checks**.
2. Click the name of the health check you want to view metrics for.
3. Click **Metrics**.

**To view health check metric charts using monitoring**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Metrics Explorer**.

   For **Metric Namespace**, select **oci_healthchecks**.

2. Select a metric to view from the **Metric Name** field.

3. Select a qualifier specified in the Dimension Name field. For example, the dimension **resourceId** is specified in the metric definition for **BasicCount**.

4. Select the value you want to use for the specified dimension in the **Dimension Value** field. For example, the resource identifier for your instance of interest.

5. Click **Update Chart**.

   The chart will be updated with the metrics that have been requested.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**Using the API**

Use the following APIs for monitoring:

- **Monitoring API** for metrics and alarms
- **Notifications API** for notifications (used with alarms)
Chapter 21

I AM

This chapter explains how to set up administrators, users, and groups and specify their permissions.

Overview of Oracle Cloud Infrastructure Identity and Access Management

Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who has access to your cloud resources. You can control what type of access a group of users have and to which specific resources. This section gives you an overview of IAM components and an example scenario to help you understand how they work together.

Note:

This document uses the term "you" broadly to mean any administrator in your company who has access to work with IAM.

Components of IAM

IAM uses the components described in this section. To better understand how the components fit together, see Example Scenario on page 2126.

RESOURCE

The cloud objects that your company's employees create and use when interacting with Oracle Cloud Infrastructure. For example: compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, route tables, etc.

USER

An individual employee or system that needs to manage or use your company's Oracle Cloud Infrastructure resources. Users might need to launch instances, manage remote disks, work with your virtual cloud network, etc. End users of your application are not typically IAM users. Users have one or more IAM credentials (see User Credentials on page 2360).

GROUP

A collection of users who all need the same type of access to a particular set of resources or compartment.

DYNAMIC GROUP

A special type of group that contains resources (such as compute instances) that match rules that you define (thus the membership can change dynamically as matching resources are created or deleted). These instances act as "principal" actors and can make API calls to services according to policies that you write for the dynamic group.

NETWORK SOURCE

A group of IP addresses that are allowed to access resources in your tenancy. The IP addresses can be public IP addresses or IP addresses from a VCN within your tenancy. After you create the network source, you use policy to restrict access to only requests that originate from the IPs in the network source.
COMPARTMENT

A collection of related resources. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources. You use them to clearly separate resources for the purposes of measuring usage and billing, access (through the use of policies), and isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of your organization. For more information, see “Setting Up Your Tenancy” in the Oracle Cloud Infrastructure Getting Started Guide.

TENANCY

The root compartment that contains all of your organization's Oracle Cloud Infrastructure resources. Oracle automatically creates your company's tenancy for you. Directly within the tenancy are your IAM entities (users, groups, compartments, and some policies; you can also put policies into compartments inside the tenancy). You place the other types of cloud resources (e.g., instances, virtual networks, block storage volumes, etc.) inside the compartments that you create.

POLICY

A document that specifies who can access which resources, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. For more information, see Example Scenario on page 2126 and How Policies Work on page 2136. The word "policy" is used by people in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named “policy” document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources.

HOME REGION

The region where your IAM resources reside. All IAM resources are global and available across all regions, but the master set of definitions reside in a single region, the home region. You must make changes to your IAM resources in your home region. The changes will be automatically propagated to all regions. For more information, see Managing Regions on page 2445.

FEDERATION

A relationship that an administrator configures between an identity provider and a service provider. When you federate Oracle Cloud Infrastructure with an identity provider, you manage users and groups in the identity provider. You manage authorization in Oracle Cloud Infrastructure's IAM service. Oracle Cloud Infrastructure tenancies are federated with Oracle Identity Cloud Service by default.

Services You Can Control Access To

You can write policies to control access to all of the services within Oracle Cloud Infrastructure.

The Administrators Group and Policy

When your company signs up for an Oracle account and Identity Domain, Oracle sets up a default administrator for the account. This person will be the first IAM user for your company and will be responsible for initially setting up additional administrators. Your tenancy comes with a group called Administrators, and the default administrator automatically belongs in this group. You can't delete this group, and there must always be at least one user in it.

Your tenancy also automatically has a policy that gives the Administrators group access to all of the Oracle Cloud Infrastructure API operations and all of the cloud resources in your tenancy. You can neither change nor delete this policy. Any other users you put into the Administrators group will have full access to all of the services. This means they can create and manage IAM resources such as, groups, policies, and compartments. And they can create and manage the cloud resources such as virtual cloud networks (VCNs), instances, block storage volumes, and any other new types of Oracle Cloud Infrastructure resources that become available in the future.
Example Scenario

The goal of this scenario is to show how the different IAM components work together, and basic features of policies.

In this scenario, Acme Company has two teams that will be using Oracle Cloud Infrastructure resources for infrastructure: Project A and Project B. In reality, your company may have many more.

Acme Company plans to use a single virtual cloud network (VCN) for both teams, and wants a network administrator to manage the VCN.

Acme Company also wants the Project A team and Project B team to each have their own set of instances and block storage volumes. The Project A team and Project B teams shouldn't be able to use each other's instances. These two teams also shouldn't be allowed to change anything about the VCN set up by the network administrator. Acme Company wants each team to have administrators for that team's resources. The administrators for the Project A team can decide who can use the Project A cloud resources, and how. Same for the Project B team.

Acme Company Gets Started with Oracle Cloud Infrastructure

Acme Company signs up to use Oracle Cloud Infrastructure and tells Oracle that an employee named Wenpei will be the default administrator. In response, Oracle:

- Creates a tenancy for Acme Company (see the following diagram).
- Creates an IAM user account for Wenpei in the tenancy.
- Creates the Administrators group in the tenancy and places Wenpei in that group.
- Creates a policy in Acme Company's tenancy that gives the Administrators group access to manage all of the resources in the tenancy. Here's that policy:

  Allow group Administrators to manage all-resources in tenancy

The default setup for a new tenancy:

<table>
<thead>
<tr>
<th>CompanyA Tenancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies attached to the tenancy:</td>
</tr>
<tr>
<td>Allow group Administrators to manage all-resources in tenancy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wenpei</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
</tr>
<tr>
<td>Wenpei</td>
</tr>
</tbody>
</table>

The Default Administrator Creates Some Groups and Another Administrator

Wenpei next creates several groups and users (see the following diagram). She:

- Creates groups called NetworkAdmins, A-Admins, and B-Admins (these last two are for Project A and Project B within the company)
- Creates a user called Alex and puts him in the Administrators group.
- Leaves the new groups empty.

To learn how to create groups, see Working with Groups on page 2420. To learn how to create users and put them in groups, see Working with Users on page 2415.
The Default Administrator Creates Some Compartments and Policies

Wenpei next creates compartments to group resources together (see the following diagram). She:

- Creates a compartment called Networks to control access to the Acme Company’s VCN, subnets, IPSec VPN, and other components from Networking.
- Creates a compartment called Project-A to organize Project A team’s cloud resources and control access to them.
- Creates a compartment called Project-B to organize Project B team’s cloud resources and control access to them.

To learn how to manage compartments, see Working with Compartments on page 2432.

Wenpei then creates a policy to give the administrators for each compartment their required level of access. She attaches the policy to the tenancy, which means that only users with access to manage policies in the tenancy can later update or delete the policy. In this scenario, that is only the Administrators group. The policy includes multiple statements that:

- Give the NetworkAdmins group access to manage networks and instances (for the purposes of easily testing the network) in the Networks compartment
- Give both the A-Admins and B-Admins groups access to use the networks in the Networks compartment (so they can create instances into the network).
- Give the A-Admins group access to manage all resources in the Project-A compartment.
- Give the B-Admins group access to manage all resources in the Project-B compartment.

Here’s what that policy looks like (notice it has multiple statements in it):

```
Allow group NetworkAdmins to manage virtual-network-family in compartment Networks
Allow group NetworkAdmins to manage instance-family in compartment Networks
Allow group A-Admins,B-Admins to use virtual-network-family in compartment Networks
Allow group A-Admins to manage all-resources in compartment Project-A
Allow group B-Admins to manage all-resources in compartment Project-B
```

Notice the difference in the verbs (manage, use), as well as the resources (virtual-network-family, instance-family, all-resources). For more information about them, see Verbs on page 2138 and Resource-Types on page 2139. To learn how to create policies, see To create a policy on page 2454.
Important:

A-Admins and B-Admins can use the virtual-network-family in the compartment Networks. However, they can't create instances in that compartment. They can only create instances in the Project-A or Project-B compartment. Remember, a compartment is a logical grouping, not a physical one, so resources that make up or reside on the same VCN can belong to different compartments.

Acme Company wants to let the administrators of the Project-A and Project-B compartments decide which users can use the resources in those compartments. So Wenpei creates two more groups: A-Users and B-Users. She then adds six more statements that give the compartment admins the required access they need in order to add and remove users from those groups:

- Allow group A-Admins to use users in tenancy where target.group.name='A-Users'
- Allow group A-Admins to use groups in tenancy where target.group.name='A-Users'
- Allow group B-Admins to use users in tenancy where target.group.name='B-Users'
- Allow group B-Admins to use groups in tenancy where target.group.name='B-Users'
- Allow group A-Admins,B-Admins to inspect users in tenancy
- Allow group A-Admins,B-Admins to inspect groups in tenancy

Notice that this policy doesn't let the project admins create new users or manage credentials for the users. It lets them decide which existing users can be in the A-Users and B-Users groups. The last two statements are necessary for A-Admins and B-Admins to list all the users and groups, and confirm which users are in which groups.
An Administrator Creates New Users

At this point, Alex is in the Administrators group and now has access to create new users. So he provisions users named Leslie, Jorge, and Cheri and places them in the NetworkAdmins, A-Admins, and B-Admins groups,
respectively. Alex also creates other users who will eventually be put in the A-Users and B-Users groups by the admins for Project A and Project B.

### CompanyA Tenancy

**Policies attached to the tenancy:**

- Allow group `Administrators` to manage all-resources in tenancy
- Allow group `NetworkAdmins` to manage virtual-network-family in compartment Networks
- Allow group `NetworkAdmins` to manage instance-family in compartment Networks
- Allow group `A-Admins,B-Admins` to use virtual-network-family in compartment Networks
- Allow group `A-Admins` to manage all-resources in compartment Project-A
- Allow group `B-Admins` to manage all-resources in compartment Project-B
- Allow group `A-Admins` to use users in tenancy where target.group.name='A-Users'
- Allow group `A-Admins` to use groups in tenancy where target.group.name='A-Users'
- Allow group `B-Admins` to use users in tenancy where target.group.name='B-Users'
- Allow group `B-Admins` to use groups in tenancy where target.group.name='B-Users'
- Allow group `A-Admins,B-Admins` to inspect users in tenancy
- Allow group `A-Admins,B-Admins` to inspect groups in tenancy

<table>
<thead>
<tr>
<th>Users</th>
<th>Alex</th>
<th>Cheri</th>
<th>Dylan</th>
<th>Fred</th>
<th>Helali</th>
<th>Jorge</th>
<th>Laura</th>
<th>Leslie</th>
<th>Tarik</th>
<th>Wenpei</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Groups</th>
<th>Administrators</th>
<th>NetworkAdmins</th>
<th>A-Admins</th>
<th>B-Admins</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Wenpei</td>
<td>Leslie</td>
<td>Jorge</td>
<td>Cheri</td>
</tr>
<tr>
<td></td>
<td>Alex</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compartments</th>
<th>Networks</th>
<th>Project-A</th>
<th>Project-B</th>
</tr>
</thead>
</table>
The Network Admin Sets Up the Network

Leslie (in the NetworkAdmins group) has access to manage virtual-network-family and instance-family in the Networks compartment. She creates a virtual cloud network (VCN) with a single subnet in that compartment. She also sets up an Internet gateway for the VCN, and updates the VCN's route table to allow traffic via that gateway. To test the VCN's connectivity to the on-premises network, she launches an instance in the subnet in the VCN. As part of the launch request, she must specify which compartment the instance should reside in. She specifies the Networks compartment, which is the only one she has access to. She then confirms connectivity from the on-premises network to the VCN by logging in to the instance via SSH from the on-premises network.

Leslie terminates her test instance and lets Jorge and Cheri know that the VCN is up and running and ready to try out. She lets them know that their compartments are named Project-A and Project-B respectively. For more information about setting up a cloud network, see Networking on page 2746. For information about launching instances into the network, see Overview of the Compute Service on page 590.

Compartment Admins Set Up Their Compartments

Jorge and Cheri now need to set up their respective compartments. Each admin needs to do the following:

- Launch instances in their own compartment
- Put users in their "users" group (e.g., A-Users)
- Decide the type of access to give those users, and accordingly attach a policy to their compartment

Jorge and Cheri both launch instances into the subnet in the VCN, into their respective team's compartments. They create and attach block volumes to the instances. Only the compartment admins can launch/terminate instances or attach/detach block volumes in their respective team's compartments.

### Important:

Network Topology and Compartment Access Are Different Concepts

It's important to understand the difference between the network topology of the VCN and the access control that the compartments provide. The instances Jorge launched reside in the VCN from a network topology standpoint. But from an access standpoint, they're in the Project-A compartment, not the Networks compartment where the VCN is. Leslie (the Networks admin) can't terminate or reboot Jorge's instances, or launch new ones into the Project-A compartment. But Leslie controls the instances' network, so she controls what traffic will be routed to them. If Jorge had specified the Networks compartment instead of the Project-A compartment when launching his instances, his request would have been denied. The story is similar for Cheri and the Project-B compartment.

But it's also important to note that Wenpei and Alex in the Administrators group do have access to the resources inside the compartments, because they have access to manage all kinds of resources in the tenancy. Compartments inherit any policies attached to their parent compartment (the tenancy), so the Administrators access also applies to all compartments within the tenancy.

Next, Jorge puts several of the users that Alex created into the A-Users group. Cheri does the same for B-Users.

Then Jorge writes a policy that gives users the level of access they need in the Project-A compartment.

```java
Allow group A-Users to use instance-family in compartment Project-A
Allow group A-Users to use volume-family in compartment Project-A
Allow group A-Users to inspect virtual-network-family in compartment Networks
```

This lets them use existing instances (with attached block volumes) that the compartment admins already launched in the compartment, and stop/start/reboot them. It does not let A-Users create/delete or attach/detach any volumes. To give that ability, the policy would need to include manage volume-family.
Jorge attaches this policy to the Project-A compartment. Anyone with the ability to manage policies in the compartment can now modify or delete this policy. Right now, that is only the A-Admins group (and the Administrators group, which can do anything throughout the tenancy).

Cheri creates and attaches her own policy to the Project-B compartment, similar to Jorge's policy:

```
Allow group B-Users to use instance-family in compartment Project-B
Allow group B-Users to use volume-family in compartment Project-B
Allow group B-Users to inspect virtual-network-family in compartment Networks
```

Now the A-Users and B-Users can work with the existing instances and attached volumes in the Project-A and Project-B compartments, respectively. Here's what the layout looks like:
# CompanyA Tenancy

**Policies attached to the tenancy:**

- Allow group **Administrators** to manage all-resources in tenancy
- Allow group **NetworkAdmins** to manage virtual-network-family in compartment **Networks**
- Allow group **NetworkAdmins** to manage instance-family in compartment **Networks**
- Allow group **A-Admins,B-Admins** to use virtual-network-family in compartment **Networks**
- Allow group **A-Admins** to manage all-resources in compartment **Project-A**
- Allow group **B-Admins** to manage all-resources in compartment **Project-B**
- Allow group **A-Admins** to use users in tenancy where target.group.name='A-Users'
- Allow group **A-Admins** to use groups in tenancy where target.group.name='A-Users'
- Allow group **B-Admins** to use users in tenancy where target.group.name='B-Users'
- Allow group **B-Admins** to use groups in tenancy where target.group.name='B-Users'
- Allow group **A-Admins,B-Admins** to inspect users in tenancy
- Allow group **A-Admins,B-Admins** to inspect groups in tenancy

<table>
<thead>
<tr>
<th>Users</th>
<th>Alex</th>
<th>Cheri</th>
<th>Fred</th>
<th>Jorge</th>
<th>Leslie</th>
<th>Wenpei</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dylan</td>
<td>Helali</td>
<td>Jenna</td>
<td>Laura</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Groups**

- **Administrators**
  - Wenpei
  - Alex
- **NetworkAdmins**
  - Leslie
  - Jorge
- **A-Admins**
  - Jorge
- **B-Admins**
  - Cheri
- **A-Users**
  - Laura
  - Helali
  - Dylan
- **B-Users**
  - Fred
  - Jenna
  - Tarik

**Compartments**

- **Networks**
- **Project-A**
  - Policy attached and managed by Jorge
  - Allow group **A-Users** to use instance-family in compartment **Project-A**
  - Allow group **A-Users** to use volume-family in compartment **Project-A**
- **Project-B**
  - Policy attached and managed by Cheri
  - Allow group **B-Users** to use instance-family in compartment **Project-B**
  - Allow group **B-Users** to use volume-family in compartment **Project-B**
  - Allow group **B-Users** to inspect virtual-network-family in compartment **Networks**
  - Allow group **B-Users** to inspect virtual-network-family in compartment **Networks**
For more information about basic and advanced features of policies, see How Policies Work on page 2136. For examples of other typical policies your organization might use, see Common Policies on page 2142.

**Viewing Resources by Compartment in the Console**

In the Console, you view your cloud resources by compartment. This means that after you sign in to the Console, you'll choose which compartment to work in (there's a list of the compartments you have access to on the left side of the page). Notice that compartments can be nested inside other compartments. The page will update to show that compartment's resources that are within the current region. If there are none, or if you don't have access to the resource in that compartment, you'll see a message.

This experience is different when you're viewing the lists of users, groups, dynamic groups, and federation providers. Those reside in the tenancy itself (the root compartment), not in an individual compartment.

As for policies, they can reside in either the tenancy or a compartment, depending on where the policy is attached. Where it's attached controls who has access to modify or delete it. For more information, see Policy Attachment on page 2141.

**The Scope of IAM Resources**

Oracle Cloud Infrastructure uses the concepts of regions and availability domains (see Regions and Availability Domains). Some resources are available regionally, whereas others are available only within a certain availability domain. IAM resources (users, groups, dynamic groups, compartments, tag namespaces, federation providers, and policies) are global and available across all regions. See Managing Regions on page 2445.

**Creating Automation with Events**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

The following IAM resources emit events:

- Authentication policies
- Credentials
- Dynamic groups
- Groups
- Identity Providers
- Multi-factor Authentication TOTP Devices
- Policies
- Users

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later
For general information about using the API, see REST APIs on page 4368.

Limits on IAM Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Getting Started with Policies

If you're new to Oracle Cloud Infrastructure Identity and Access Management (IAM) policies, this topic gives guidance on how to proceed.

If You’re Doing a Proof-of-Concept

If you're just trying out Oracle Cloud Infrastructure or doing a proof-of-concept project with infrastructure resources, you may not need more than a few administrators with full access to everything. In that case, you can simply create any new users you need and add them to the Administrators group. The users will be able to do anything with any kind of resource. And you can create all your resources directly in the tenancy (the root compartment). You don't need to create any compartments yet, or any other policies beyond the Tenant Admin Policy, which automatically comes with your tenancy and can't be changed.

Note:
Don't forget to add your new users to the Administrators group; it's easy to forget to do that after creating them.

If You’re Past the Proof-of-Concept Phase

If you're past the proof-of-concept phase and want to restrict access to your resources, first:

• Make sure you're familiar with the basic IAM components, and read through the example scenario: Overview of Oracle Cloud Infrastructure Identity and Access Management on page 2124
• Think about how to organize your resources into compartments: See "Setting Up Your Tenancy" in the Oracle Cloud Infrastructure Getting Started Guide
• Learn the basics of how policies work: How Policies Work on page 2136
• Check out some typical policies: Common Policies on page 2142
• Read the FAQs below

Policy FAQs

Which of the services within Oracle Cloud Infrastructure can I control access to through policies?

All of them, including IAM itself. You can find specific details for writing policies for each service in the Policy Reference on page 2167.

Can users do anything without an administrator writing a policy for them?

Yes. All users can automatically do these things without an explicit policy:

• Change or reset their own Console password.
• Manage their own API signing keys and other credentials.

Why should I separate resources by compartment? Couldn't I just put all the resources into one compartment and then use policies to control who has access to what?

You could put all your resources into a single compartment and use policies to control access, but then you would lose the benefits of measuring usage and billing by compartment, simple policy administration at the compartment level, and clear separation of resources between projects or business units.

Can I control or deny access to an individual user?

Yes. However, there are a couple things to know first:
• Enterprise companies typically have multiple users that need similar permissions, so policies are designed to give access to groups of users, not individual users. A user gains access by being in a group.
• Policies are designed to allow access; there’s no explicit “deny” when you write a policy.

If you need to grant access to a particular user, you can add a condition to the policy that specifies the user’s OCID in a variable. This construction restricts the access granted in the policy to only the user specified in the condition. For example:

```
allow any-user to read object-family in compartment ObjectStorage where request.user.id = 'ocid1.user.oc1..<user_OCID>'
```

For information about using conditions and variables in policies, see Conditions on page 2160.

If you need to restrict a particular user’s access, you can:
• Remove the user from the particular group of interest
• Delete the user entirely from IAM (you have to remove the user from all groups first)

**How do I delete a user?**

First ensure the user isn’t in any groups. Only then can you delete the user.

**How do I delete a compartment?**

See To delete a compartment on page 2444.

**How can I tell which policies apply to a particular group or user?**

You need to look at the individual statements in all your policies to see which statements apply to which group. There’s not currently an easy way to get this information.

**How can I tell which policies apply to a particular compartment?**

You need to look at the individual statements in all the policies in the tenancy to see if any apply to the particular compartment. You also need to look at any policies in the compartment itself. Policies in any of the sibling compartments cannot refer to the compartment of interest, so you don't need to check those policies.

**How Policies Work**

This topic describes how policies work and the basic features.

**Overview of Policies**

A policy is a document that specifies who can access which Oracle Cloud Infrastructure resources that your company has, and how. A policy simply allows a group to work in certain ways with specific types of resources in a particular compartment. If you’re not familiar with users, groups, or compartments, see Overview of Oracle Cloud Infrastructure Identity and Access Management on page 2124.

In general, here’s the process an IAM administrator in your organization needs to follow:

1. Define users, groups, and one or more compartments to hold the cloud resources for your organization.
2. Create one or more policies, each written in the policy language. See Common Policies on page 2142.
3. Place users into the appropriate groups depending on the compartments and resources they need to work with.
4. Provide the users with the one-time passwords that they need in order to access the Console and work with the compartments. For more information, see User Credentials on page 2360.

After the administrator completes these steps, the users can access the Console, change their one-time passwords, and work with specific cloud resources as stated in the policies.
Policy Basics

To govern control of your resources, your company will have at least one policy. Each policy consists of one or more policy statements that follow this basic syntax:

```
Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>
```

Notice that the statements always begin with the word Allow. Policies only allow access; they cannot deny it. Instead there's an implicit deny, which means by default, users can do nothing and have to be granted access through policies. (There's one exception to this rule; see Can users do anything without an administrator writing a policy for them? on page 2135)

An administrator in your organization defines the groups and compartments in your tenancy. Oracle defines the possible verbs and resource-types you can use in policies (see Verbs on page 2138 and Resource-Types on page 2139).

In some cases you'll want the policy to apply to the tenancy and not a compartment inside the tenancy. In that case, change the end of the policy statement like so:

```
Allow group <group_name> to <verb> <resource-type> in tenancy
```

For more details about the syntax, see Policy Syntax on page 2164.

For information about how many policies you can have, see Service Limits on page 215.

A Few Examples

Let's say your administrator creates a group called HelpDesk whose job is to manage users and their credentials. Here is a policy that enables that:

```
Allow group HelpDesk to manage users in tenancy
```

Notice that because users reside in the tenancy (the root compartment), the policy simply states the word tenancy, without the word compartment in front of it.

Next, let's say you have a compartment called Project-A, and a group called A-Admins whose job is to manage all of the Oracle Cloud Infrastructure resources in the compartment. Here's an example policy that enables that:

```
Allow group A-Admins to manage all-resources in compartment Project-A
```

Be aware that the policy directly above includes the ability to write policies for that compartment, which means A-Admins can control access to the compartment's resources. For more information, see Policy Attachment on page 2141.

If you wanted to limit A-Admins' access to only launching and managing compute instances and block storage volumes (both the volumes and their backups) in the Project-A compartment, but the network itself lives in the Networks compartment, then the policy could instead be:

```
Allow group A-Admins to manage instance-family in compartment Project-A
Allow group A-Admins to manage volume-family in compartment Project-A
Allow group A-Admins to use virtual-network-family in compartment Networks
```

The third statement with the virtual-network-family resource-type enables the instance launch process, because the cloud network is involved. Specifically, the launch process creates a new VNIC and attaches it to the subnet where the instance resides.

For additional examples, see Common Policies on page 2142.
Details about Specifying Groups and Compartments

Typically you'll specify a group or compartment by name in the policy. However, you can use the OCID instead. Just make sure to add "id" before the OCID. For example:

```
Allow group
  id ocid1.group.oc1..aaaaaaaqjihfhvmumrl3isyrfw3n6c4rzwckawuc7i5xwe6s7qmsb6a
  to manage instance-family in compartment Project-A
```

You can specify multiple groups separated by commas:

```
Allow group A-Admins, B-Admins to manage instance-family in compartment Projects-A-and-B
```

Verbs

Oracle defines the possible verbs you can use in your policies. Here's a summary of the verbs, from least amount of access to the most:

<table>
<thead>
<tr>
<th>Verb</th>
<th>Types of Access Covered</th>
<th>Target User</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>Ability to list resources, without access to any confidential information or user-specified metadata that may be part of that resource. <strong>Important:</strong> The operation to list policies includes the contents of the policies themselves, and the list operations for the Networking resource-types return all the information (e.g., the contents of security lists and route tables).</td>
<td>Third-party auditors</td>
</tr>
<tr>
<td>read</td>
<td>Includes inspect plus the ability to get user-specified metadata and the actual resource itself.</td>
<td>Internal auditors</td>
</tr>
<tr>
<td>use</td>
<td>Includes read plus the ability to work with existing resources (the actions vary by resource type). Includes the ability to update the resource, except for resource-types where the &quot;update&quot; operation has the same effective impact as the &quot;create&quot; operation (e.g., UpdatePolicy, UpdateSecurityList, etc.), in which case the &quot;update&quot; ability is available only with the manage verb. In general, this verb does not include the ability to create or delete that type of resource.</td>
<td>Day-to-day end users of resources</td>
</tr>
<tr>
<td>manage</td>
<td>Includes all permissions for the resource.</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

The verb gives a certain general type of access (e.g., inspect lets you list and get resources). When you then join that type of access with a particular resource-type in a policy (e.g., Allow group XYZ to inspect compartments in the tenancy), then you give that group access to a specific set of permissions and API operations (e.g., ListCompartments, GetCompartment). For more examples, see Details for Verbs + Resource-Type Combinations on page 2281. The Policy Reference on page 2167 includes a similar table for each service, giving you a list of exactly which API operations are covered for each combination of verb and resource-type.

There are some special exceptions or nuances for certain resource-types.

**Users:** Access to both manage users and manage groups lets you do anything with users and groups, including creating and deleting users and groups, and adding/removing users from groups. To add/remove users from groups without access to creating and deleting users and groups, only both use users and use groups are required. See Common Policies on page 2142.
**Policies:** The ability to update a policy is available only with manage policies, not use policies, because updating a policy is similar in effect to creating a new policy (you can overwrite the existing policy statements). In addition, inspect policies lets you get the full contents of the policies.

**Object Storage objects:** inspect objects lets you list all the objects in a bucket and do a HEAD operation for a particular object. In comparison, read objects lets you download the object itself.

**Load Balancing resources:** Be aware that inspect load-balancers lets you get all information about your load balancers and related components (backend sets, etc.).

**Networking resources:**

Be aware that the inspect verb not only returns general information about the cloud network's components (for example, the name and OCID of a security list, or of a route table). It also includes the contents of the component (for example, the actual rules in the security list, the routes in the route table, and so on).

Also, the following types of abilities are available only with the manage verb, not the use verb:

- Update (enable/disable) internet-gateways
- Update security-lists
- Update route-tables
- Update dhcp-options
- Attach a dynamic routing gateway (DRG) to a virtual cloud network (VCN)
- Create an IPSec connection between a DRG and customer-premises equipment (CPE)
- Peer VCNs

**Important:**

Each VCN has various components that directly affect the behavior of the network (route tables, security lists, DHCP options, Internet Gateway, and so on). When you create one of these components, you establish a relationship between that component and the VCN, which means you must be allowed in a policy to both create the component and manage the VCN itself. However, the ability to update that component (to change the route rules, security list rules, and so on) does NOT require permission to manage the VCN itself, even though changing that component can directly affect the behavior of the network. This discrepancy is designed to give you flexibility in granting least privilege to users, and not require you to grant excessive access to the VCN just so the user can manage other components of the network. Be aware that by giving someone the ability to update a particular type of component, you're implicitly trusting them with controlling the network's behavior.

**Resource-Types**

Oracle also defines the resource-types you can use in your policies. First, there are individual types. Each individual type represents a specific type of resource. For example, the vcn resource-type is specifically for virtual cloud networks (VCNs).

To make policy writing easier, there are family types that include multiple individual resource-types that are often managed together. For example, the virtual-network-family type brings together a variety of types related to the management of VCNs (e.g., vcn, subnets, route-tables, security-lists, etc.). If you need to write a more granular policy that gives access to only an individual resource-type, you can. But you can also easily write a policy to give access to a broader range of resources.

In another example: Block Volume has volumes, volume-attachments, and volume-backups. If you need to give access to only making backups of volumes, you can specify the volume-backups resource-type in your policy. But if you need to give broad access to all of the Block Volume resources, you can specify the family type called volume-family. For a full list of the family resource-types, see Resource-Types on page 2169.
Important: If a service introduces new individual resource-types, they will typically be included in the family type for that service. For example, if Networking introduces a new individual resource-type, it will be automatically included in the definition of the virtual-network-family resource type. For more information about future changes to the definitions of resource-types, see Policies and Service Updates on page 2142.

Note that there are other ways to make policies more granular, such as the ability to specify conditions under which the access is granted. For more information, see Advanced Policy Features on page 2160.

Access that Requires Multiple Resource-Types

Some API operations require access to multiple resource-types. For example, LaunchInstance requires the ability to create instances and work with a cloud network. The CreateVolumeBackup operation requires access to both the volume and the volume backup. That means you’ll have separate statements to give access to each resource-type (for an example, see Let volume backup admins manage only backups on page 2146). These individual statements do not have to be in the same policy. And a user can gain the required access from being in different groups. For example, George could be in one group that gives the required level of access to the volumes resource-type, and in another group that gives the required access to the volume-backups resource-type. The sum of the individual statements, regardless of their location in the overall set of policies, gives George access to CreateVolumeBackup.

Policy Inheritance

A basic feature of policies is the concept of inheritance: Compartments inherit any policies from their parent compartment. The simplest example is the Administrators group, which automatically comes with your tenancy (see The Administrators Group and Policy on page 2125). There’s a built-in policy that enables the Administrators group to do anything in the tenancy:

Allow group Administrators to manage all-resources in tenancy

Because of policy inheritance, the Administrators group can also do anything in any of the compartments in the tenancy.

To illustrate further, consider a tenancy with three levels of compartments: CompartmentA, CompartmentB, and CompartmentC, shown here:

![Compartment Hierarchy Diagram]

Policies that apply to resources in CompartmentA also apply to resources in CompartmentB and CompartmentC. So this policy:

Allow group NetworkAdmins to manage virtual-network-family in compartment CompartmentA

allows the group NetworkAdmins to manage VCNs in CompartmentA, CompartmentB, and CompartmentC.
**Policy Attachment**

Another basic feature of policies is the concept of attachment. When you create a policy you must attach it to a compartment (or the tenancy, which is the root compartment). **Where you attach it controls who can then modify it or delete it.** If you attach it to the tenancy (in other words, if the policy is in the root compartment), then anyone with access to manage policies in the tenancy can then change or delete it. Typically that's the Administrators group or any similar group you create and give broad access to. Anyone with access only to a child compartment cannot modify or delete that policy.

If you instead attach the policy to a child compartment, then anyone with access to manage the policies in that compartment can change or delete it. In practical terms, this means it's easy to give compartment administrators (i.e., a group with access to manage all-resources in the compartment) access to manage their own compartment's policies, without giving them broader access to manage policies that reside in the tenancy. For an example that uses this kind of compartment administrator design, see Example Scenario on page 2126. (Recall that because of policy inheritance, users with access to manage policies in the tenancy automatically have the ability to manage policies in compartments inside the tenancy.)

The process of attaching the policy is easy (whether attaching to a compartment or the tenancy): If you're using the Console, when you add the policy to IAM, simply make sure you're in the desired compartment when you create the policy. If you're using the API, you specify the OCID of the desired compartment (either the tenancy or other compartment) as part of the request to create the policy.

When you attach a policy to a compartment, you must be in that compartment and you must indicate directly in the statement which compartment it applies to. If you are not in the compartment, you'll get an error if you try to attach the policy to a different compartment. Notice that attachment occurs during policy creation, which means a policy can be attached to only one compartment. To learn how to attach a policy to a compartment, see To create a policy on page 2454.

**Policies and Compartment Hierarchies**

As described in the previous section, a policy statement must specify the compartment for which access is being granted (or the tenancy). Where you create the policy determines who can update the policy. If you attach the policy to the compartment or its parent, you can simply specify the compartment name. If you attach the policy further up the hierarchy, you must specify the path. The format of the path is each compartment name (or OCID) in the path, separated by a colon:

<compartment_level_1>:<compartment_level_2>:...<compartment_level_n>

For example, assume you have a three-level compartment hierarchy, shown here:

![Compartment Hierarchy Diagram]

You want to create a policy to allow NetworkAdmins to manage VCNs in CompartmentC. If you want to attach this policy to CompartmentC or to its parent, CompartmentB, write this policy statement:

Allow group NetworkAdmins to manage virtual-network-family in compartment CompartmentC
However, if you want to attach this policy to CompartmentA (so that only administrators of CompartmentA can modify it), write this policy statement that specifies the path:

```
Allow group NewtworkAdmins to manage virtual-network-family in compartment CompartmentB:CompartmentC
```

To attach this policy to the tenancy, write this policy statement that specifies the path from CompartmentA to CompartmentC:

```
Allow group NewtworkAdmins to manage virtual-network-family in compartment CompartmentA:CompartmentB:CompartmentC
```

**Policies and Service Updates**

It's possible that the definition of a verb or resource-type could change in the future. For example, let's say that the `virtual-network-family` resource-type changes to include a new kind of resource that's been added to Networking. By default, your policies automatically stay current with any changes in service definition, so any policy you have that gives access to `virtual-network-family` would automatically include access to the newly added resource.

**Writing Policies for Each Service**

The Policy Reference on page 2167 includes details of the specific resource-types for each service, and which verb + resource-type combination gives access to which API operations.

**Common Policies**

This section includes some common policies you might want to use in your organization.

**Note:**

These policies use example group and compartment names. Make sure to replace them with your own names.

**Let the Help Desk manage users**

*Type of access:* Ability to create, update, and delete users and their credentials. It does not include the ability to put users in groups.

*Where to create the policy:* In the tenancy, because users reside in the tenancy.

```
Allow group HelpDesk to manage users in tenancy
```

**Let auditors inspect your resources**

*Type of access:* Ability to list the resources in all compartments. Be aware that:

- The operation to list IAM policies includes the contents of the policies themselves
- The list operations for Networking resource-types return all the information (for example, the contents of security lists and route tables)
- The operation to list instances requires the `read` verb instead of `inspect`, and the contents include the user-provided metadata.
- The operation to view Audit service events requires the `read` verb instead of `inspect`.

*Where to create the policy:* In the tenancy. Because of the concept of `policy inheritance`, auditors can then inspect both the tenancy and all compartments beneath it. Or you could choose to give auditors access to only specific compartments if they don't need access to the entire tenancy.

```
Allow group Auditors to inspect all-resources in tenancy

Allow group Auditors to read instances in tenancy
```
Allow group Auditors to read audit-events in tenancy

Let network admins manage a cloud network

**Type of access:** Ability to manage all components in Networking. This includes cloud networks, subnets, gateways, virtual circuits, security lists, route tables, and so on. If the network admins need to launch instances to test network connectivity, see Let users launch compute instances on page 2143.

**Where to create the policy:** In the tenancy. Because of the concept of policy inheritance, NetworkAdmins can then manage a cloud network in any compartment. To reduce the scope of access to a particular compartment, specify that compartment instead of the tenancy.

Allow group NetworkAdmins to manage virtual-network-family in tenancy

Let network admins manage load balancers

**Type of access:** Ability to manage all components in Load Balancing. If the group needs to launch instances, see Let users launch compute instances on page 2143.

**Where to create the policy:** In the tenancy. Because of the concept of policy inheritance, NetworkAdmins can then manage load balancers in any compartment. To reduce the scope of access to a particular compartment, specify that compartment instead of the tenancy.

Allow group NetworkAdmins to manage load-balancers in tenancy

If the group uses the Console to manage load balancers, an additional policy to use the associated networking resources is required:

Allow group NetworkAdmins to manage load-balancers in tenancy
Allow group NetworkAdmins to use virtual-network-family in tenancy

If a particular group needs to update existing load balancers (for example, modify the backend set) but not create or delete them, use this statement:

Allow group LBUsers to use load-balancers in tenancy

Let users launch compute instances

**Type of access:** Ability to do everything with instances launched into the cloud network and subnets in compartment XYZ, and attach/detach any existing volumes that already exist in compartment ABC. The first statement also lets the group create and manage instance images in compartment ABC. If the group doesn't need to attach/detach volumes, you can delete the volume-family statement.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartments (ABC and XYZ) to have control over the individual policy statements for their compartments, see Policy Attachment on page 2141.

Allow group InstanceLaunchers to manage instance-family in compartment ABC
Allow group InstanceLaunchers to read app-catalog-listing in tenancy
Allow group InstanceLaunchers to use volume-family in compartment ABC
Allow group InstanceLaunchers to use virtual-network-family in compartment XYZ

To allow users to create new cloud networks and subnets, see Let network admins manage a cloud network on page 2143.
Let users launch compute instances from a specific custom image

**Type of access:** Ability to launch instances into the cloud network and subnets in compartment XYZ using only the specified custom image. The policy also includes the ability to attach/detach any existing volumes that already exist in compartment ABC. If the group doesn't need to attach/detach volumes, you can delete the `volume-family` statement.

To specify multiple custom images, you can use conditions.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartments (ABC and XYZ) to have control over the individual policy statements for their compartments, see Policy Attachment on page 2141.

```
Allow group ImageUsers to inspect instance-images in compartment ABC
Allow group ImageUsers to {INSTANCE_IMAGE_READ} in compartment ABC where target.image.id='<image_OCID>'
Allow group ImageUsers to manage instances in compartment ABC
Allow group ImageUsers to read app-catalog-listing in tenancy
Allow group ImageUsers to use volume-family in compartment ABC
Allow group ImageUsers to use virtual-network-family in compartment XYZ
```

Let image admins manage custom images

**Type of access:** Ability to do everything with custom images and compute instances. Also includes the ability to do everything with Object Storage buckets, objects, and namespaces in compartment Y (for creating images from objects and creating pre-authenticated requests to images); to attach/detach any existing volumes in compartment X; and to launch instances into the cloud network and subnets in compartment Z (for creating new instances to base an image on). If the group doesn't need to attach/detach volumes, you can delete the `volume-family` statement.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartments (X, Y, and Z) to have control over the individual policy statements for their compartments, see Policy Attachment on page 2141.

```
Allow group ImageAdmins to manage instances in compartment X
Allow group ImageAdmins to manage instance-images in compartment X
Allow group ImageAdmins to read app-catalog-listing in tenancy
Allow group ImageAdmins to manage object-family in compartment Y
Allow group ImageAdmins to use volume-family in compartment X
Allow group ImageAdmins to use virtual-network-family in compartment Z
```

Let users manage Compute instance configurations, instance pools, and cluster networks

**Type of access:** Ability to do all things with instance configurations, instance pools, and cluster networks in all compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the instance configurations, instance pools, and cluster networks in a particular compartment, specify that compartment instead of the tenancy.

```
Allow group InstancePoolAdmins to manage compute-management-family in tenancy
```

If a group needs to create instance configurations using existing instances as a template, and uses the API, SDKs, or command line interface (CLI) to do this, add the following statements to the policy:

```
Allow group InstancePoolAdmins to read instance-family in tenancy
Allow group InstancePoolAdmins to inspect volumes in tenancy
```
If a particular group needs to start, stop, or reset the instances in existing instance pools, but not create or delete instance pools, use this statement:

```
Allow group InstancePoolUsers to use instance-pools in tenancy
```

If resources used by the instance pool contain default tags, add the following statement to the policy to give the group permission to the tag namespace `Oracle-Tags`:

```
Allow group InstancePoolUsers to use tag-namespaces in tenancy where target.tag-namespace.name = 'oracle-tags'
```

### Let users manage Compute autoscaling configurations

**Type of access:** Ability to create, update, and delete autoscaling configurations.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the autoscaling configurations in a particular compartment, specify that compartment instead of the tenancy.

```
Allow group AutoscalingAdmins to manage auto-scaling-configurations in tenancy
Allow group AutoscalingAdmins to manage instance-pools in tenancy
```

### Let users list and subscribe to images from the Partner Image catalog

**Type of access:** Ability to list and create subscriptions to images in the Partner Image catalog. It does not include the ability to create instances using images from the Partner Image catalog (see Let users launch compute instances on page 2143).

**Where to create the policy:** In the tenancy. To reduce the scope of access to just creating subscriptions in a particular compartment, specify that compartment instead of the tenancy in the third statement.

```
Allow group CatalogSubscribers to inspect app-catalog-listing in tenancy
Allow group CatalogSubscribers to read app-catalog-listing in tenancy
Allow group CatalogSubscribers to manage app-catalog-listing in tenancy
```

### Let users create Compute instance console connections

**Type of access:** Ability to create instance console connections.

**Where to create the policy:** In the tenancy.

```
Allow group <group_name> to manage instance-console-connection in tenancy
Allow group <group_name> to read instance in tenancy
```

### Let users manage Compute dedicated virtual machine hosts

**Type of access:** Ability to create, update, and delete dedicated virtual machine hosts as well as launch instances on dedicated virtual machine hosts.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the dedicated virtual machine hosts and instances in a particular compartment, specify that compartment instead of the tenancy.

```
Allow group DedicatedVMHostAdmins to manage dedicated-vm-hosts in tenancy
Allow group DedicatedVMHostAdmins to manage instances in tenancy
```
Let users launch Compute instances on dedicated virtual machine hosts

Type of access: Ability to launch instances on dedicated virtual machine hosts.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the dedicated virtual machine hosts and instances in a particular compartment, specify that compartment instead of the tenancy.

| Allow group DedicatedVMHostAdmins to use dedicated-vm-hosts in tenancy |
| Allow group DedicatedVMHostAdmins to manage instances in tenancy |

Let volume admins manage block volumes, backups, and volume groups

Type of access: Ability to do all things with block storage volumes, volume backups, and volume groups in all compartments with the exception of copying volume backups across regions. This makes sense if you want to have a single set of volume admins manage all the volumes, volume backups, and volume groups in all the compartments. The second statement is required in order to attach/detach the volumes from instances.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes/backups and instances in a particular compartment, specify that compartment instead of the tenancy.

| Allow group VolumeAdmins to manage volume-family in tenancy |
| Allow group VolumeAdmins to use instance-family in tenancy |

If the group needs to also copy volume backups and boot volume backups across regions, add the following statements to the policy:

| Allow group VolumeAdmins to use volume-backups in tenancy where request.permission='VOLUME_BACKUP_COPY' |
| Allow group VolumeAdmins to use boot-volume-backups in tenancy where request.permission='BOOT_VOLUME_BACKUP_COPY' |

Let volume backup admins manage only backups

Type of access: Ability to do all things with volume backups, but not create and manage volumes themselves. This makes sense if you want to have a single set of volume backup admins manage all the volume backups in all the compartments. The first statement gives the required access to the volume that is being backed up; the second statement enables creation of the backup (and the ability to delete backups). The third statement enables the creation and management of user defined backup policies; the fourth statement enables assignment and removal of assignment of backup policies.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes and backups in a particular compartment, specify that compartment instead of the tenancy.

| Allow group VolumeBackupAdmins to use volumes in tenancy |
| Allow group VolumeBackupAdmins to manage volume-backups in tenancy |
| Allow group VolumeBackupAdmins to manage backup-policies in tenancy |
| Allow group VolumeBackupAdmins to manage backup-policy-assignments in tenancy |

If the group will be using the Console, the following policy gives a better user experience:

| Allow group VolumeBackupAdmins to use volumes in tenancy |
Allow group VolumeBackupAdmins to manage volume-backups in tenancy
Allow group VolumeBackupAdmins to inspect volume-attachments in tenancy
Allow group VolumeBackupAdmins to inspect instances in tenancy
Allow group VolumeBackupAdmins to manage backup-policies in tenancy
Allow group VolumeBackupAdmins to manage backup-policy-assignments in tenancy

The last two statements are not necessary in order to manage volume backups. However, they enable the Console to display all the information about a particular volume and the available backup policies.

Let boot volume backup admins manage only backups

**Type of access:** Ability to do all things with boot volume backups, but not create and manage boot volumes themselves. This makes sense if you want to have a single set of boot volume backup admins manage all the boot volume backups in all the compartments. The first statement gives the required access to the boot volume that is being backed up; the second statement enables creation of the backup (and the ability to delete backups). The third statement enables the creation and management of user defined backup policies; the fourth statement enables assignment and removal of assignment of backup policies.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the boot volumes and backups in a particular compartment, specify that compartment instead of the tenancy.

Allow group BootVolumeBackupAdmins to use volumes in tenancy
Allow group BootVolumeBackupAdmins to manage boot-volume-backups in tenancy
Allow group BootVolumeBackupAdmins to manage backup-policies in tenancy
Allow group BootVolumeBackupAdmins to manage backup-policy-assignments in tenancy

If the group will be using the Console, the following policy gives a better user experience:

Allow group BootVolumeBackupAdmins to use volumes in tenancy
Allow group BootVolumeBackupAdmins to manage boot-volume-backups in tenancy
Allow group BootVolumeBackupAdmins to inspect instances in tenancy
Allow group BootVolumeBackupAdmins to manage backup-policies in tenancy
Allow group BootVolumeBackupAdmins to manage backup-policy-assignments in tenancy

The last two statements are not necessary in order to manage volume backups. However, they enable the Console to display all the information about a particular boot volume and the available backup policies.

Let users create a volume group

**Type of access:** Ability to create a volume group from a set of volumes.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes and volume groups in a particular compartment, specify that compartment instead of the tenancy.

Allow group VolumeGroupCreators to inspect volumes in tenancy
Allow group VolumeGroupCreators to manage volume-groups in tenancy

Let users clone a volume group

Type of access: Ability to clone a volume group from an existing volume group.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes and volume groups in a particular compartment, specify that compartment instead of the tenancy.

Allow group VolumeGroupCloners to inspect volumes in tenancy
Allow group VolumeGroupCloners to manage volume-groups in tenancy
Allow group VolumeGroupCloners to manage volumes in tenancy

Let users create a volume group backup

Type of access: Ability to create a volume group backup.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes/backups and volume groups/volume group backups in a particular compartment, specify that compartment instead of the tenancy.

Allow group VolumeGroupBackupAdmins to inspect volume-groups in tenancy
Allow group VolumeGroupBackupAdmins to manage volumes in tenancy
Allow group VolumeGroupBackupAdmins to manage volume-group-backups in tenancy
Allow group VolumeGroupBackupAdmins to manage volume-backups in tenancy

Let users restore a volume group backup

Type of access: Ability to create a volume group by restoring a volume group backup.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the volumes/backups and volume groups/volume group backups in a particular compartment, specify that compartment instead of the tenancy.

Allow group VolumeGroupBackupAdmins to inspect volume-group-backups in tenancy
Allow group VolumeGroupBackupAdmins to read volume-backups in tenancy
Allow group VolumeGroupBackupAdmins to manage volume-groups in tenancy
Allow group VolumeGroupBackupAdmins to manage volumes in tenancy

Let users create, manage, and delete file systems

Type of access: Ability to create, manage, or delete a file system or file system clone. Administrative functions for a file system include the ability to rename or delete it or disconnect from it.

Where to create the policy: In the tenancy, so that the ability to create, manage, or delete a file system is easily granted to all compartments by way of policy inheritance. To reduce the scope of these administrative functions to file systems in a particular compartment, specify that compartment instead of the tenancy.

Allow group StorageAdmins to manage file-family in tenancy

Let users create file systems

Type of access: Ability to create a file system or file system clone.
**Where to create the policy:** In the tenancy, so that the ability to create a file system is easily granted to all compartments by way of policy inheritance. To reduce the scope of these administrative functions to file systems in a particular compartment, specify that compartment instead of the tenancy.

- Allow group Managers to manage file-systems in tenancy
- Allow group Managers to read mount-targets in tenancy

The second statement is required when users create a file system using the Console. It enables the Console to display a list of mount targets that the new file system can be associated with.

**Let Object Storage admins manage buckets and objects**

**Type of access:** Ability to do all things with Object Storage buckets and objects in all compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the buckets and objects in a particular compartment, specify that compartment instead of the tenancy.

- Allow group ObjectAdmins to manage buckets in tenancy
- Allow group ObjectAdmins to manage objects in tenancy

**Let users write objects to Object Storage buckets**

**Type of access:** Ability to write objects to any Object Storage bucket in compartment ABC (imagine a situation where a client needs to regularly write log files to a bucket). This consists of the ability to list the buckets in the compartment, list the objects in a bucket, and create a new object in a bucket. Although the second statement gives broad access with the manage verb, that access is then scoped down to only the OBJECT_INSPECT and OBJECT_CREATE permissions with the condition at the end of the statement.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of compartment ABC to have control over the policy, see Policy Attachment on page 2141.

- Allow group ObjectWriters to read buckets in compartment ABC
- Allow group ObjectWriters to manage objects in compartment ABC where any 
  
  `{request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT'}`

**Access limited to a specific bucket:** To limit access to a specific bucket in a particular compartment, add the condition where target.bucket.name='<bucket_name>'. The following policy allows the user to list all the buckets in a particular compartment, but they can only list the objects in and upload objects to BucketA:

- Allow group ObjectWriters to read buckets in compartment ABC
- Allow group ObjectWriters to manage objects in compartment ABC where all 
  
  `{target.bucket.name='BucketA', any {request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT'}}`

For more information about using conditions, see Advanced Policy Features on page 2160.

**Let users download objects from Object Storage buckets**

**Type of access:** Ability to download objects from any Object Storage bucket in compartment ABC. This consists of the ability to list the buckets in the compartment, list the objects in a bucket, and read existing objects in a bucket.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of compartment ABC to have control over the policy, see Policy Attachment on page 2141.

- Allow group ObjectReaders to read buckets in compartment ABC

Oracle Cloud Infrastructure User Guide
IAM

**Allow group ObjectReaders to read objects in compartment ABC**

**Access limited to a specific bucket:** To limit access to a specific bucket in a particular compartment, add the condition `where target.bucket.name='<bucket_name>'`. The following policy allows the user to list all buckets in a particular compartment, but they can only read the objects in and download from BucketA:

```
Allow group ObjectReaders to read buckets in compartment ABC
Allow group ObjectReaders to read objects in compartment ABC where target.bucket.name='BucketA'
```

For more information about using conditions, see Advanced Policy Features on page 2160.

**Let database admins manage Oracle Cloud database systems**

**Type of access:** Ability to do all things with the following system types and their associated resources in all compartments:

- Exadata Cloud Service instances
- bare metal DB systems
- virtual machine DB systems

This makes sense if you want to have a single set of database admins manage all the bare metal, virtual machine, and Exadata systems in all the compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the database systems in a particular compartment, specify that compartment instead of the tenancy.

```
Allow group DatabaseAdmins to manage database-family in tenancy
```

**Let database admins manage Exadata Cloud@Customer instances**

**Type of access:** Ability to do all things with the Exadata Cloud@Customer resources in all compartments. This makes sense if you want to have a single set of database admins manage all the Exadata Cloud@Customer systems in all the compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the Exadata Cloud@Customer systems in a particular compartment, specify that compartment instead of the tenancy.

```
Allow group ExaCCAdmins to manage database-family in tenancy
```

**Let database admins manage Oracle Cloud external database resources**

**Type of access:** Ability to do all things with the following OCI external database resources in all compartments:

- OCI external container database resources
- OCI external pluggable database resources
- OCI external non-container database resources
- OCI external database connectors

This makes sense if you want to have a single set of database admins manage all the OCI external database resources in all the compartments.
Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the OCI external database resources in a particular compartment, specify that compartment instead of the tenancy.

Allow group OnPremDatabaseAdmins to manage external-database-family in tenancy

Let database and fleet admins manage Autonomous Databases

Type of access: Ability to do all things with Autonomous Database instances in all compartments. Applicable if you want to have a single set of database administrators manage all the Autonomous Database databases in all the compartments.

Where to create the policy: In the tenancy, so that the access is granted to all compartments by way of policy inheritance. To reduce the scope of access to just the Autonomous Databases in a particular compartment, specify that compartment instead of the tenancy.

Example 1: For fleet administrators. Enables Autonomous Database fleet administrator access to the various workload types (Autonomous Data Warehouse, Autonomous JSON Database, and Autonomous Transaction Processing), and to dedicated Exadata infrastructure resources (container databases and Autonomous Exadata Infrastructure instances).

Allow group DatabaseAdmins to manage autonomous-database-family in tenancy

If you must restrict access to the Autonomous Exadata Infrastructure and Autonomous Container Database resource types (applicable only to dedicated Exadata infrastructure systems), then you can do so by creating separate policy statements for database administrators that allow access to only Autonomous Databases and their backups. Because a policy statement can only specify one resource type, you must create separate statements for the database and backup resources.

Example 2: For database administrators. Enables Autonomous Database database administrators access to databases and backups of the various workload types, but denies access to Autonomous Container Databases and Autonomous Exadata Infrastructure instances.

Allow group ADB-Admins to manage autonomous-database in tenancy

Allow group ADB-Admins to manage autonomous-backup in tenancy

To reduce the scope of access to either the Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing workload types, use a where clause, as shown in the next example.

Example 3: For database administrators. Limits Autonomous Database access to Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing databases and backups.

Allow group ADB-Admins to manage autonomous-database in tenancy where target.workloadType = 'workload_type'

Allow group ADB-Admins to manage autonomous-backup in tenancy where target.workloadType = 'workload_type'

In the preceding code examples, workload_type can be DW, AJD, or OLTP for Autonomous Data Warehouse, Autonomous JSON Database, or Autonomous Transaction Processing, respectively.

Let security admins manage vaults, keys, and secrets

Type of access: Ability to do all things with the Vault service in all compartments. This makes sense if you want to have a single set of security admins manage all the vaults, keys, and secret components (including secrets, secret versions, and secret bundles) in all compartments.
**Where to create the policy:** In the tenancy, so that access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the vaults, keys, and secret components in a particular compartment, specify that compartment instead of the tenancy. To reduce the scope of access to just vaults, keys, or secret components, include only the policy statement that pertains to the respective individual or aggregate resource-type, as appropriate.

| Allow group SecurityAdmins to manage vaults in tenancy |
| Allow group SecurityAdmins to manage keys in tenancy |
| Allow group SecurityAdmins to manage secret-family in tenancy |

**Let security admins manage all keys in a specific vault in a compartment**

**Type of access:** Ability to do all things with keys in a specific vault in compartment ABC.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartment (ABC) to have control over the individual policy statements for their compartment, see Policy Attachment on page 2141.

| Allow group SecurityAdmins to manage keys in compartment ABC where target.vault.id='<vault_OCID>' |

**Let security admins use a specific key in a compartment**

**Type of access:** Ability to list, view, and perform cryptographic operations with a specific key in a compartment.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartment (ABC) to have control over the individual policy statements for their compartment, see Policy Attachment on page 2141.

| Allow group SecurityAdmins to use keys in compartment ABC where target.key.id='<key_OCID>' |

**Let a user group delegate key usage in a compartment**

**Type of access:** Ability to associate an Object Storage bucket, Block Volume volume, File Storage file system, Kubernetes cluster, or Streaming stream pool with a specific key authorized for use in a specific compartment. With this policy, a user in the specified group does not have permission to use the key itself. Rather, by association, the key can be used by Object Storage, Block Volume, File Storage, Container Engine for Kubernetes, or Streaming on behalf of the user to:

- Create or update an encrypted bucket, volume, or file system and to encrypt or decrypt data in the bucket, volume, or file system.
- Create Kubernetes clusters with encrypted Kubernetes secrets at rest in the etcd key-value store.
- Create a stream pool to encrypt data in the streams in the stream pool.

This policy requires that you also have a companion policy that lets Object Storage, Block Volume, File Storage, Container Engine for Kubernetes, or Streaming use the key to perform cryptographic operations.

**Where to create the policy:** The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartment (ABC) to have control over the individual policy statements for their compartment, see Policy Attachment on page 2141.

| Allow group ObjectWriters, VolumeWriters, FileWriters, ClusterWriters, StreamWriters to use key-delegate in compartment ABC where target.key.id = '<key_OCID>' |
Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools

Type of access: Ability to list, view, and perform cryptographic operations with all keys in compartment ABC. Because Object Storage is a regional service, it has regional endpoints. As such, you must specify the regional service name for each region where you’re using Object Storage with Vault encryption. This policy also requires that you have a companion policy that allows a user group to use the delegated key that Object Storage, Block Volume, File Storage, Container Engine for Kubernetes, or Streaming will use.

Where to create the policy: The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartment (ABC) to have control over the individual policy statements for their compartment, see Policy Attachment on page 2141.

Allow service blockstorage, objectstorage-<region_name>, FssOc1Prod, oke, streaming to use keys in compartment ABC where target.key.id = '<key_OCID>'

For Object Storage, replace <region_name> with the appropriate region identifier, for example:

- objectstorage-us-phoenix-1
- objectstorage-us-ashburn-1
- objectstorage-eu-frankfurt-1
- objectstorage-uk-london-1
- objectstorage-ap-tokyo-1

To determine the region name value of an Oracle Cloud Infrastructure region, see Regions and Availability Domains on page 180.

For File Storage, the service name used in the policy is FssOc1Prod.

For Container Engine for Kubernetes, the service name used in the policy is oke.

For Streaming, the service name used in the policy is streaming.

Let security admins manage all secrets in a specific vault in a compartment

Type of access: Ability to do all things with secrets in a specific vault in compartment ABC.

Where to create the policy: The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartment (ABC) to have control over the individual policy statements for their compartment, see Policy Attachment on page 2141.

Allow group SecurityAdmins to manage secret-family in compartment ABC where target.vault.id='<vault_OCID>'

Let users read, update, and rotate all secrets

Type of access: Ability to read, update, and rotate all secrets in any vault in the tenancy.

Where to create the policy: In the tenancy, so that access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the vaults, keys, and secrets in a particular compartment, specify that compartment instead of the tenancy.

Allow group SecretsUsers to use secret-family in tenancy

Let users manage their own passwords and credentials

No policy is required to let users manage their own credentials. All users have the ability to change and reset their own passwords, manage their own API keys, and manage their own auth tokens. For more information, see User Credentials on page 2360.
Let a compartment admin manage the compartment

**Type of access:** Ability to manage all aspects of a particular compartment. For example, a group called A-Admins could manage all aspects of a compartment called Project-A, including writing additional policies that affect the compartment. For more information, see Policy Attachment on page 2141. For an example of this kind of setup and additional policies that are useful, see Example Scenario on page 2126.

**Where to create the policy:** In the tenancy.

```
Allow group A-Admins to manage all-resources in compartment Project-A
```

Restrict admin access to a specific region

**Type of access:** Ability to manage resources in a specific region. Remember that IAM resources must be managed in the home region. If the specified region is not the home region, then the Admin will not be able to manage IAM resources. For more information about the home region, see Managing Regions on page 2445.

**Where to create the policy:** In the tenancy.

```
Allow group PHX-Admins to manage all-resources in tenancy where request.region='phx'
```

The preceding policy allows PHX-Admins to manage all aspects of all resources in US West (Phoenix).

Members of the PHX-Admins group can only manage IAM resources if the tenancy’s home region is US West (Phoenix).

Restrict user access to view only summary announcements

**Type of access:** Ability to view the summary versions of announcements about the operational status of Oracle Cloud Infrastructure services.

**Where to create the policy:** In the tenancy.

```
Allow group AnnouncementListers to inspect announcements in tenancy
```

The preceding policy allows AnnouncementListers to view a list of summary announcements.

Let users view details of announcements

**Type of access:** Ability to view the details of announcements about the operational status of Oracle Cloud Infrastructure services.

**Where to create the policy:** In the tenancy.

```
Allow group AnnouncementReaders to read announcements in tenancy
```

The preceding policy allows AnnouncementReaders to view a list of summary announcements and the details of specific announcements.

Let streaming users manage streams

**Type of access:** Ability to do all things with the Streaming service in all compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the streams in a particular compartment, specify that compartment instead of the tenancy.

```
Allow group StreamAdmins to manage streams in tenancy
```
Let streaming users publish messages to streams

**Type of access:** Ability to produce messages to streams with the Streaming service in all compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the streams in a particular compartment, specify that compartment instead of the tenancy.

.Allow group StreamUsers to use stream-push in tenancy

Let streaming users publish messages to a specific stream

**Type of access:** Ability to produce messages to a stream with the Streaming service.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the streams in a particular compartment, specify that compartment instead of the tenancy.

.Allow group StreamUsers to use stream-push in tenancy where target.stream.id = '<stream_ocid>'

Let streaming users publish messages to a stream in a specific stream pool

**Type of access:** Ability to produce messages to a stream with the Streaming service.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the streams in a particular compartment, specify that compartment instead of the tenancy.

.Allow group StreamUsers to use stream-push in tenancy where target.streampool.id = '<stream_ocid>'

Let streaming users consume messages from streams

**Type of access:** Ability to consume messages from streams with the Streaming service in all compartments.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the streams in a particular compartment, specify that compartment instead of the tenancy.

.Allow group StreamUsers to use stream-pull in tenancy

Let users view metric definitions in a compartment

**Type of access:** Ability to view metric definitions in a specific compartment. For more information about metrics, see Metrics Feature Overview on page 2663.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the metric definitions in a particular compartment, specify that compartment instead of the tenancy.

.Allow group MetricReaders to inspect metrics in compartment ABC

Let users access monitoring metrics in a compartment

**Type of access:** Ability to view and retrieve monitoring metrics for supported resources in a specific compartment. For more information about metrics, see Metrics Feature Overview on page 2663.
Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the metrics in a particular compartment, specify that compartment instead of the tenancy.

Allow group MetricReaders to read metrics in compartment ABC

Restrict user access to a specific metric namespace

Type of access: Ability to view and retrieve monitoring metrics for resources under a specific metric namespace. For more information about metrics, see Metrics Feature Overview on page 2663.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just metrics in a particular compartment, specify that compartment instead of the tenancy.

Allow group MetricReaders to read metrics in compartment ABC where target.metrics.namespace='oci_computeagent'

The preceding policy allows MetricReaders to view and retrieve metric data points from all monitoring-enabled Compute instances in the ABC compartment.

Let users publish custom metrics

Type of access: Ability to publish custom metrics under a specific metric namespace to the Monitoring service. For instructions, see Publishing Custom Metrics on page 2717.

Where to create the policy: In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just metrics in a particular compartment, specify that compartment instead of the tenancy.

Allow group MetricPublishers to use metrics in tenancy where target.metrics.namespace='mycustomnamespace'

The preceding policy allows MetricPublishers to publish data points for the custom metric namespace mycustomnamespace in the tenancy.

Let instances make API calls to access monitoring metrics in the tenancy

Type of access: Ability to call the Monitoring API for access to monitoring metrics. The instances on which API requests originate must be members of the dynamic group indicated in the policy. For more information, see Calling Services from an Instance on page 2410 and Metrics Feature Overview on page 2663.

Where to create the policy: In the tenancy.

Allow dynamic-group MetricInstances to read metrics in tenancy

The preceding policy allows applications that are running on Compute instances in the dynamic group MetricInstances to send API requests to the Monitoring service in the tenancy.

Let users view alarms

Type of access: Ability to view alarms for supported resources in tenancy. Does not include the ability to create alarms or to create or delete topics. For more information about alarms, see Alarms Feature Overview on page 2664.

Where to create the policy: In the tenancy. Because of the concept of policy inheritance, AlarmUsers can then view alarms in any compartment. To reduce the scope of access to a particular compartment, specify that compartment instead of the tenancy.

Allow group AlarmUsers to read alarms in tenancy
IAM

Allow group AlarmUsers to read metrics in tenancy

Let users manage alarms

**Type of access:** Ability to view and create *alarms* with existing notification topics for supported resources in the tenancy. Does not include the ability to create or delete topics. For more information about alarms, see *Alarms Feature Overview* on page 2664.

All statements are required to let AlarmUsers create alarms.

**Where to create the policy:** In the tenancy. Because of the concept of *policy inheritance*, AlarmUsers can then view and create alarms in any compartment. To reduce the scope of access to a particular compartment, specify that compartment instead of the tenancy.

<table>
<thead>
<tr>
<th>Allow group AlarmUsers to manage alarms in tenancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow group AlarmUsers to read metrics in tenancy</td>
</tr>
<tr>
<td>Allow group AlarmUsers to use ons-topics in tenancy</td>
</tr>
</tbody>
</table>

Let users manage alarms and create topics

**Type of access:** Ability to view and create *alarms* (with new or existing *topics*) for supported resources in tenancy. Also includes the ability to create *subscriptions* in the tenancy, to publish *messages* (broadcast notification messages) to all subscriptions in the tenancy, and to move alarms to different compartments in the tenancy. For more information about alarms, see *Alarms Feature Overview* on page 2664.

**Where to create the policy:** In the tenancy. Because of the concept of *policy inheritance*, AlarmUsers can then view and create alarms in any compartment. To reduce the scope of access to a particular compartment, specify that compartment instead of the tenancy.

<table>
<thead>
<tr>
<th>Allow group AlarmUsers to manage alarms in tenancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow group AlarmUsers to read metrics in tenancy</td>
</tr>
<tr>
<td>Allow group AlarmUsers to manage ons-topics in tenancy</td>
</tr>
</tbody>
</table>

Let users access usage reports

**Type of access:** Ability to view usage reports for your tenancy. For more information about usage reports, see *Cost and Usage Reports Overview* on page 278.

**Where to create the policy:** This is a special cross-tenancy policy and must be created in the tenancy. For more information, see *Cost and Usage Reports Overview* on page 278.

<table>
<thead>
<tr>
<th>define tenancy usage-report as</th>
</tr>
</thead>
<tbody>
<tr>
<td>ocid1.tenancy.oc1..aaaaaaaaned4fkpkisbwjlr56u7cj631f3wffb1vqknstgtvzub7vhqkggq</td>
</tr>
<tr>
<td>endorse group Administrators to read objects in tenancy usage-report</td>
</tr>
</tbody>
</table>

Let users analyze costs

**Type of access:** Ability to see costs for the tenancy. See *Checking Your Expenses and Usage* on page 55.

**Where to create the policy:** In the tenancy so that users in the *<Example_Group>* can see costs for the entire account.

| Allow group *<Example_Group>* to read usage-reports in tenancy |
### Allow a group to manage topics

**Type of access:** Ability to get, create, update, and delete *topics* in the tenancy, as well as move topics to different compartments in the tenancy. Also includes the ability to create *subscriptions* in the tenancy and to publish *messages* (broadcast notification messages) to all subscriptions in the tenancy.

**Where to create the policy:** In the tenancy.

| Allow group A-Admins to manage ons-topics in tenancy |

### Allow a group to manage topic subscriptions

**Type of access:** Ability to list, create, update, and delete *subscriptions* for topics in the tenancy. Ability to move subscriptions to different compartments in the tenancy.

**Where to create the policy:** In the tenancy.

| Allow group A-Admins to manage ons-subscriptions in tenancy |

### Allow a group to publish messages to topics

**Type of access:** Ability to broadcast notification *messages* to all *subscriptions* in the tenancy, as well as list, create, update, and delete subscriptions in the tenancy.

**Where to create the policy:** In the tenancy.

| Allow group A-Admins to use ons-topics in tenancy |

### Let users create, deploy, and manage functions and applications using Cloud Shell

**Type of access:** Ability to create, deploy, and manage Functions applications and functions using Cloud Shell. These policy statements give the group access to Cloud Shell, repositories in Oracle Cloud Infrastructure Registry, logs, metrics, functions, and networks.

**Where to create the policy:** In the tenancy, so that the access is easily granted to all compartments by way of policy inheritance. To reduce the scope of access to just the resources in a particular compartment, you can specify the compartment instead of the tenancy in the to manage logging-family, to read metrics, to manage functions-family, and to use virtual-network-family policy statements. However, the remaining policy statements (to use cloud-shell, to manage repos, to read objectstorage-namespaces, and to read logging-family) must always be scoped to the tenancy.

| Allow group functions-developers to use cloud-shell in tenancy |
| Allow group functions-developers to manage repos in tenancy |
| Allow group functions-developers to read objectstorage-namespaces in tenancy |
| Allow group functions-developers to manage logging-family in tenancy |
| Allow group functions-developers to read metrics in tenancy |
| Allow group functions-developers to manage functions-family in tenancy |
| Allow group functions-developers to use virtual-network-family in tenancy |

### Let users list Events rules in a compartment

**Type of access:** Ability to list Events rules.

**Where to create the policy:** In the tenancy.

| Allow group RuleReaders to read cloudevents-rules in tenancy |
The preceding policy allows RuleReaders to list rules in the tenancy.

**Let admins manage Events rules in a compartment**

**Type of access:** Ability to manage Events rules, including creating, deleting and updating rules.

**Where to create the policy:** In the tenancy.

This line gives the user inspect access to resources in compartments to select actions.

```
allow group <RuleAdmins> to inspect compartments in tenancy
```

This line gives the user access to defined tags to apply filter tags to rules.

```
allow group <RuleAdmins> to use tag-namespaces in tenancy
```

These lines give the user access to Streaming resources for actions.

```
allow group <RuleAdmins> to inspect streams in tenancy
allow group <RuleAdmins> to use stream-push in tenancy
allow group <RuleAdmins> to use stream-pull in tenancy
```

These lines give the user access to Functions resources for actions.

```
allow group <RuleAdmins> to use virtual-network-family in tenancy
allow group <RuleAdmins> to manage function-family in tenancy
```

This line give the user access to Notifications topics for actions.

```
allow group <RuleAdmins> to use ons-topic in tenancy
```

This line gives the user manage access to rules for Events.

```
allow group <RuleAdmins> to manage cloudevents-rules in tenancy
```

**Allow a group to access all of Cloud Guard**

**Type of access:** Read-only access to all of Cloud Guard. In the example policy, the group is "CloudGuard_ReadOnly."

```
allow group CloudGuard_ReadOnly to read cloud-guard-family in tenancy
allow group CloudGuard_ReadOnly to read compartments in tenancy
allow group CloudGuard_ReadOnly to read announcements in tenancy
```

**Allow a group to access Cloud Guard problems**

**Type of access:** Read-only access to Cloud Guard problems. In the example policy, the group is "CloudGuard_ReadOnlyProblems."

```
allow group CloudGuard_ReadOnlyProblems to read cloud-guard-family in tenancy
allow group CloudGuard_ReadOnlyProblems to inspect cloud-guard-detectors in tenancy
allow group CloudGuard_ReadOnlyProblems to inspect cloud-guard-targets in tenancy
allow group CloudGuard_ReadOnlyProblems to inspect cloud-guard-resource-types in tenancy
allow group CloudGuard_ReadOnlyProblems to read announcements in tenancy
allow group CloudGuard_ReadOnlyProblems to read compartments in tenancy
```
allow group CloudGuard_ReadOnlyProblems to read cloud-guard-config in tenancy

**Allow a group to access Cloud Guard detector recipes**

**Type of access:** Read-only access to Cloud Guard detector recipes. In the example policy, the group is "CloudGuard_ReadOnlyDetectors."

allow group CloudGuard_ReadOnlyDetectors to read cloud-guard-detector-recipes in tenancy
allow group CloudGuard_ReadOnlyDetectors to read announcements in tenancy
allow group CloudGuard_ReadOnlyDetectors to read compartments in tenancy
allow group CloudGuard_ReadOnlyDetectors to read cloud-guard-config in tenancy

**Allow a group to access Cloud Guard in a single compartment**

**Type of access:** Read-only access to Cloud Guard in a single compartment. In the example policy, the group is "CloudGuard_ReadOnly_SingleCompartment" and the compartment name is "cgDemo_RestrictedAccess."

allow group CloudGuard_ReadOnly_SingleCompartment to read compartments in tenancy where target.compartment.name = 'cgDemo_RestrictedAccess'
allow group CloudGuard_ReadOnly_SingleCompartment to read cloud-guard-family in compartment cgDemo_RestrictedAccess
allow group CloudGuard_ReadOnly_SingleCompartment to read announcements in compartment cgDemo_RestrictedAccess
allow group CloudGuard_ReadOnly_SingleCompartment to read cloud-guard-config in tenancy

**Allow a group to manage service connectors**

**Type of access:** Ability to list, create, update, and delete service connectors in the tenancy. Ability to move service connectors to different compartments in the tenancy.

**Where to create the policy:** In the tenancy.

Allow group A-Admins to manage serviceconnectors in tenancy

**Allow a group to call Operations Insights ingest operations at tenancy**

**Type of access:** Ability to call ingest operations at the tenancy level only.

**Where to create the policy:** In the tenancy.

allow group opsi-users to use opsi-database-insights in tenancy where any
{request.operation='IngestSqlBucket',
request.operation='IngestSqlText',
request.operation='IngestSqlPlanLines'}

**Advanced Policy Features**

This section describes policy language features that let you grant more granular access.

**Conditions**

As part of a policy statement, you can specify one or more conditions that must be met in order for access to be granted.
Each condition consists of one or more predefined variables that you specify values for in the policy statement. Later, when someone requests access to the resource in question, if the condition in the policy is met, it evaluates to true and the request is allowed. If the condition is not met, it evaluates to false and the request is not allowed.

There are two types of variables: those that are relevant to the request itself, and those relevant to the resource being acted upon in the request, also known as the target. The name of the variable is prefixed accordingly with either request or target followed by a period. For example, there's a request variable called request.operation to represent the API operation being requested. This variable lets you write a broad policy statement, but add a condition based on the specific API operation. For an example, see Let users write objects to Object Storage buckets on page 2149.

**Important:**
Condition matching is case insensitive. This is important to remember when writing conditions for resource types that allow case-sensitive naming. For example, the Object Storage service allows you to create both a bucket named "BucketA" and a bucket named "bucketA" in the same compartment. If you write a condition that specifies "BucketA", it will apply also to "bucketA", because the condition matching is case insensitive.

Variables that Aren't Applicable to a Request Result in a Declined Request

If the variable is not applicable to the incoming request, the condition evaluates to false and the request is declined. For example, here are the basic policy statements that together let someone add or remove users from any group except Administrators:

```
Allow group GroupAdmins to use users in tenancy
   where target.group.name != 'Administrators'
```

```
Allow group GroupAdmins to use groups in tenancy
   where target.group.name != 'Administrators'
```

Given the above policy, if GroupAdmins tried to call a general API operation for users such as `ListUsers` or `UpdateUser` (which lets you change the user's description), the request would be declined, even though those API operations are covered by `use users`. This is because the above policy statement for `use users` also includes the `target.group.name` variable, but the `ListUsers` or `UpdateUser` request doesn't involve specifying a group. There is no `target.group.name` for those requests, so the request is declined.

If you want to also grant access to general user API operations that don't involve a particular group, you would need an additional statement that gives the level of access you want to grant, but without the condition. For example, if you want to grant access to `ListUsers`, you need this additional statement:

```
Allow group GroupAdmins to inspect users in tenancy
```

Or if you want to grant access to `UpdateUser`, you need this additional statement (which also covers `ListUsers` because the `use` verb includes the capabilities of the `inspect` verb):

```
Allow group GroupAdmins to use users in tenancy
```

This general concept also applies to groups (e.g., `ListGroups` and `UpdateGroup`), and any other resource type with target variables.

For more information about the syntax of conditions, see Conditions on page 2166. For a list of all the variables you can use in policies, see the tables in the Policy Reference on page 2167.

**Tag-Based Access Control**

Using conditions and a set of tag variables, you can write policy to scope access based on the tags that have been applied to a resource. Access can be controlled based on a tag that exists on the requesting resource (the group or dynamic group in the policy) or on the target of the request (resource or compartment). Tag-based access control provides additional flexibility to your policies by allowing you to define access that spans compartments, groups, and
resources. For details about how to write policies to scope access by tags, see Using Tags to Manage Access on page 3932.

**Permissions**

Permissions are the atomic units of authorization that control a user's ability to perform operations on resources. Oracle defines all the permissions in the policy language. When you write a policy giving a group access to a particular verb and resource-type, you're actually giving that group access to one or more predefined permissions. The purposes of verbs is to simplify the process of granting multiple related permissions that cover a broad set of access or a particular operational scenario. The next sections give more details and examples.

**Relation to Verbs**

To understand the relationship between permissions and verbs, let's look at an example. A policy statement that allows a group to inspect volumes actually gives the group access to a permission called VOLUME_INSPECT (permissions are always written with all capital letters and underscores). In general, that permission enables the user to get information about block volumes.

As you go from inspect > read > use > manage, the level of access generally increases, and the permissions granted are cumulative. The following table shows the permissions included with each verb for the volumes resource-type. Notice that no additional permissions are granted going from inspect to read.

<table>
<thead>
<tr>
<th>Inspect Volumes</th>
<th>Read Volumes</th>
<th>Use Volumes</th>
<th>Manage Volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOLUME_INSPECT</td>
<td>VOLUME_INSPECT</td>
<td>VOLUME_INSPECT</td>
<td>VOLUME_INSPECT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VOLUME_UPDATE</td>
<td>VOLUME_UPDATE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VOLUME_WRITE</td>
<td>VOLUME_WRITE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VOLUME_CREATE</td>
<td>VOLUME_CREATE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VOLUME_DELETE</td>
<td>VOLUME_DELETE</td>
</tr>
</tbody>
</table>

The policy reference lists the permissions covered by each verb for each given resource-type. For example, for block volumes and other resources covered by the Core Services, see the tables in Details for Verb + Resource-Type Combinations on page 2183. The left column of each of those tables lists the permissions covered by each verb. The other sections of the policy reference include the same kind of information for the other services.

**Relation to API Operations**

Each API operation requires the caller to have access to one or more permissions. For example, to use either ListVolumes or GetVolume, you must have access to a single permission: VOLUME_INSPECT. To attach a volume to an instance, you must have access to multiple permissions, some of which are related to the volumes resource-type, some to the volume-attachments resource-type, and some related to the instances resource-type:

- VOLUME_WRITE
- VOLUME_ATTACHMENT_CREATE
- INSTANCE_ATTACH_VOLUME

The policy reference lists which permissions are required for each API operation. For example, for the Core Services API operations, see the table in Permissions Required for Each API Operation on page 2225.

**Understanding a User's Access**

The policy language is designed to let you write simple statements involving only verbs and resource-types, without having to state the desired permissions in the statement. However, there may be situations where a security team member or auditor wants to understand the specific permissions a particular user has. The tables in the policy reference show each verb and the associated permissions. You can look at the groups the user is in and the policies applicable to those groups, and from there compile a list of the permissions granted. However, having a list of the permissions isn't the complete picture. Conditions in a policy statement can scope a user's access beyond individual
permissions (see the next section). Also, each policy statement specifies a particular compartment and can have conditions that further scope the access to only certain resources in that compartment.

**Scoping Access with Permissions or API Operations**

In a policy statement, you can use conditions combined with permissions or API operations to reduce the scope of access granted by a particular verb.

For example, let's say you want group XYZ to be able to list, get, create, or update groups (i.e., change their description), but not delete them. To list, get, create, and update groups, you need a policy with manage groups as the verb and resource-type. According to the table in Details for Verbs + Resource-Type Combinations on page 2281, the permissions covered are:

- GROUP_INSPECT
- GROUP_UPDATE
- GROUP_CREATE
- GROUP_DELETE

To restrict access to only the desired permissions, you could add a condition that explicitly states the permissions you want to allow:

Allow group XYZ to manage groups in tenancy where any 
{request.permission='GROUP_INSPECT',
request.permission='GROUP_CREATE',
request.permission='GROUP_UPDATE'}

An alternative would be a policy that allows all permissions except GROUP_DELETE:

Allow group XYZ to manage groups in tenancy where request.permission != 'GROUP_DELETE'

However, with this approach, be aware that any new permissions the service might add in the future would automatically be granted to group XYZ. Only GROUP_DELETE would be omitted.

Another alternative would be to write a condition based on the specific API operations. Notice that according to the table in Permissions Required for Each API Operation on page 2288, both ListGroups and GetGroup require only the GROUP_INSPECT permission. Here's the policy:

Allow group XYZ to manage groups in tenancy where any 
{request.operation='ListGroups',
request.operation='GetGroup',
request.operation='CreateGroup',
request.operation='UpdateGroup'}

It can be beneficial to use permissions instead of API operations in conditions. In the future, if a new API operation is added that requires one of the permissions listed in the permissions-based policy above, that policy will already control XYZ group's access to that new API operation.

But notice that you can further scope a user's access to a permission by also specifying a condition based on API operation. For example, you could give a user access to GROUP_INSPECT, but then only to ListGroups.

Allow group XYZ to manage groups in tenancy

where all 
{request.permission='GROUP_INSPECT',
request.operation='ListGroups'}
Scoping Policy by the IP Address of the Requestor

You can scope access to only a set of allowed IP addresses. For example, you can write policy to allow only requests from a given public IP range to access a specific Object Storage bucket; or, you can allow only specific subnets of a specific VCN to make requests over a service gateway.

To restrict access to a set of IP addresses, do the following:

1. Create a network source object that specifies the allowed IP addresses. See Managing Network Sources on page 2427 for details.
2. Write a policy that uses the network source object in a condition.

Use the following variable in your policy:

```
request.networkSource.name='<network_source_name>'
```

For example:

```
allow group GroupA to manage object-family in tenancy where request.networkSource.name='corpnet'
```

Policy Syntax

The overall syntax of a policy statement is as follows:

```
Allow <subject> to <verb> <resource-type> in <location> where <conditions>
```

Spare spaces or line breaks in the statement have no effect.

For limits on the number of policies and statements, see Service Limits on page 215.

Subject

Specify one or more comma-separated groups by name or OCID. Or specify any-user to cover all users in the tenancy.

**Syntax:**

```
group <group_name> | group id <group_ocid> | dynamic-group <dynamic-group_name> | dynamic-group id<dynamic-group_ocid> | any-user
```

**Examples:**

- To specify a single group by name:

```
Allow

group A-Admins

to manage all-resources in compartment Project-A
```

- To specify multiple groups by name (a space after the comma is optional):

```
Allow

group A-Admins, B-Admins

to manage all-resources in compartment Projects-A-and-B
```

- To specify a single group by OCID (the OCID is shortened for brevity):

```
Allow group

id ocid1.group.oc1..aaaaaaaqjihfhvxmlm...awuc7i5xwe6s7qmnsbc6a
```
to manage all-resources in compartment Project-A

- To specify multiple groups by OCID (the OCIDs are shortened for brevity):

  Allow group

  id ocid1.group.oc1..aaaaaaaaqjihfhvxmlr1...wuc7i5xwe6s7qmnsbc6a,
  id ocid1.group.oc1..aaaaaaavhea5mellwzb...66yfxv1462tdgx20eczyq

to manage all-resources in compartment Projects-A-and-B

- To specify any user in the tenancy:

  Allow any-user to inspect users in tenancy

**Verb**

Specify a single verb. For a list of verbs, see Verbs on page 2169. Example:

Allow group A-Admins to manage all-resources in compartment Project-A

**Resource-Type**

Specify a single resource-type, which can be one of the following:

- An individual resource-type (e.g., vcns, subnets, instances, volumes, etc.)
- A family resource-type (e.g., virtual-network-family, instance-family, volume-family, etc.)
- **all-resources**: Covers all resources in the compartment (or tenancy).

A family resource-type covers a variety of components that are typically used together. This makes it easier to write a policy that gives someone access to work with various aspects of your cloud network.

For a list of the available resource-types, see Resource-Types on page 2169.

**Syntax:** `<resource_type> | all-resources`

**Examples:**

- To specify a single resource-type:

  Allow group HelpDesk to manage users in tenancy

- To specify multiple resource-types, use separate statements:

  Allow group A-Users to manage instance-family in compartment Project-A

  Allow group A-Users to manage volume-family in compartment Project-A

- To specify all resources in the compartment (or tenancy):

  Allow group A-Admins to manage all-resources in compartment Project-A

**Location**

Specify a single compartment or compartment path by name or OCID. Or simply specify tenancy to cover the entire tenancy. Remember that users, groups, and compartments reside in the tenancy. Policies can reside in (i.e., be attached to) either the tenancy or a child compartment.

**Note:**

Granting Access to Specific Regions or availability domains
To create a policy that gives access to a specific region or availability domain, use the `request.region` or `request.ad` variable with a condition. See Conditions on page 2166.

The location is required in the statement. If you want to attach a policy to a compartment, you must be in that compartment when you create the policy. For more information, see Policy Attachment on page 2141.

To specify a compartment that is not a direct child of the compartment you are attaching the policy to, specify the path to the compartment, using the colon (:) as a separator. For more information, see Policies and Compartment Hierarchies on page 2141.

**Syntax:**
```plaintext
[ tenancy | compartment <compartment_name> | compartment id <compartment_ocid> ]
```

**Examples:**

- To specify a compartment by name:
  ```plaintext
  Allow group A-Admins to manage all-resources in compartment Project-A
  ```

- To specify a compartment by OCID:
  ```plaintext
  Allow group id ocid1.group.oc1..aaaaaaaaexampleocid to manage all-resources in compartment id ocid1.compartment.oc1..aaaaaaaaexampleocid
  ```

- To specify multiple compartments, use separate statements:
  ```plaintext
  Allow group InstanceAdmins to manage instance-family in compartment Project-A
  Allow group InstanceAdmins to manage instance-family in compartment Project-B
  ```

- To specify multiple compartments by OCID, use separate statements:
  ```plaintext
  Allow group id ocid1.group.oc1..aaaaaaaavheexampleocid to manage all-resources in compartment id ocid1.compartment.oc1..aaaaaaaayzexampleocid
  Allow group id ocid1.group.oc1..aaaaaaaaexampleocid to manage all-resources in compartment id ocid1.compartment.oc1..aaaaaexampledocid
  ```

- To specify a compartment that is not a direct child of the compartment where you are attaching the policy, specify the path:
  ```plaintext
  Allow group InstanceAdmins to manage instance-family in compartment Project-A:Project-A2
  ```

**Conditions**

Specify one or more conditions. Use any or all with multiple conditions for a logical OR or AND, respectively.

**Syntax for a single condition:**
```plaintext
variable =|!= value
```

**Syntax for multiple conditions:**
```plaintext
any|all {<condition>,<condition>,...}
```

**Important:**
Condition matching is case insensitive. This is important to remember when writing conditions for resource types that allow case-sensitive naming. For example, the Object Storage service allows you to create both a bucket named "BucketA" and a bucket named "bucketA" in the same compartment.
If you write a condition that specifies "BucketA", it will apply also to "bucketA", because the condition matching is case insensitive.

For a list of variables supported by all the services, see General Variables for All Requests on page 2169. Also see the details for each service in the Policy Reference on page 2167. Here are the types of values you can use in conditions:

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>'<a href="mailto:johnsmith@example.com">johnsmith@example.com</a>'</td>
</tr>
<tr>
<td></td>
<td>'ocid1.compartment.oc1..aaaaaaaph...ctehnqg756a'</td>
</tr>
<tr>
<td></td>
<td>(single quotation marks are required around the value)</td>
</tr>
<tr>
<td>Pattern</td>
<td>/HR*/ (matches strings that start with &quot;HR&quot;)</td>
</tr>
<tr>
<td></td>
<td>/*HR/ (matches strings that end with &quot;HR&quot;)</td>
</tr>
<tr>
<td></td>
<td>/<em>HR</em>/ (matches strings that contain &quot;HR&quot;)</td>
</tr>
</tbody>
</table>

Examples:

Note:

In the following examples, the statements that specify the condition do not let GroupAdmins actually list all the users and groups, therefore statements including the inspect verb are added for completeness. To understand why this is required, see Variables that Aren't Applicable to a Request Result in a Declined Request on page 2161.

- A single condition.

The following policy enables the GroupAdmins group to create, update, or delete any groups with names that start with "A-Users-":

Allow group GroupAdmins to manage groups in tenancy where target.group.name = /A-Users-*/
Allow group GroupAdmins to inspect groups in tenancy

The following policy enables the NetworkAdmins group to manage cloud networks in any compartment except the one specified:

Allow group NetworkAdmins to manage virtual-network-family in tenancy where target.compartment.id != 'ocid1.compartment.oc1..aaaaaaexampleocid'

- Multiple conditions.

The following policy lets GroupAdmins create, update, or delete any groups whose names start with "A-", except for the A-Admins group itself:

Allow group GroupAdmins to manage groups in tenancy where all {target.group.name=/A-*/,target.group.name!=A-Admins}'
Allow group GroupAdmins to inspect groups in tenancy

Policy Reference

This reference includes:

- Verbs on page 2169: A list of the available actions to pair with a resource-type
• Resource-Types on page 2169: A list of the main resource-types
• General Variables for All Requests on page 2169: Variables you can use when writing policies for any resource-type
• Analytics Cloud: See Give Users Permissions to Manage Analytics Cloud Instances
• Details for the Announcements Service on page 2172
• Details for API Gateway on page 2173
• Application Migration: See Manage Service Access and Security
• Details for the Audit Service on page 2177
• Big Data: See Understand Big Data Service Resources and Permissions in IAM Policies
• Blockchain Platform: See About Permissions and Policies to Manage Oracle Blockchain Platform
• Cloud Guard: See Cloud Guard Policies
• Details for Container Engine for Kubernetes on page 2177
• Details for the Core Services on page 2181 (this includes Networking, Compute, and Block Volume)
• Content and Experience: See Service Policies
• Data Catalog: See Data Catalog Policies
• Data Flow: See Data Flow Policies
• Data Integration: See Data Integration Policies
• Data Safe: See IAM Policies
• Data Science: See Data Science Policies
• Details for the Database Service on page 2240
• Details for Database Management on page 2258
• Digital Assistant: See Digital Assistant Policies
• Details for the DNS Service on page 2262
• Details for the Email Service on page 2270
• Details for the Events Service on page 2272
• Details for the File Storage Service
• Details for Functions on page 2276
• Details for the Health Checks Service on page 2278
• Details for IAM on page 2280
• Integration: See IAM Policy Details for Oracle Integration
• Details for Load Balancing on page 2292
• Details for Logging Analytics on page 2297
• Details for Management Agent on page 2314
• Details for Management Dashboard on page 2316
• Details for the Marketplace Service on page 2319
• Details for Monitoring on page 2320
• MySQL Database: See Policy Details for MySQL Database Service
• NoSQL Database Cloud: See Details for NoSQL Database Cloud
• Details for the Notifications Service on page 2322
• Details for Object Storage, Archive Storage, and Data Transfer on page 2324
• Details for Operations Insights on page 2330
• OS Management: See OS Management Policy Reference
• Details for Registry on page 2335
• Details for Resource Manager on page 2336
• Details for the Search Service
• Security Zones: See Security Zone IAM Policies
• Details for the Streaming Service on page 2343
• Details for the Vault Service on page 2347
• Details for the WAF Service on page 2353
For instructions on how to create and manage policies using the Console or API, see Managing Policies on page 2450.

**Verbs**

The verbs are listed in order of least amount of ability to most. The exact meaning of a each verb depends on which resource-type it's paired with. The tables later in this section show the API operations covered by each combination of verb and resource-type.

<table>
<thead>
<tr>
<th>Verb</th>
<th>Types of Access Covered</th>
<th>Target User</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>Ability to list resources, without access to any confidential information or user-specified metadata that may be part of that resource. <strong>Important:</strong> The operation to list policies includes the contents of the policies themselves, and the list operations for the Networking resource-types return all the information (e.g., the contents of security lists and route tables).</td>
<td>Third-party auditors</td>
</tr>
<tr>
<td>read</td>
<td>Includes inspect plus the ability to get user-specified metadata and the actual resource itself.</td>
<td>Internal auditors</td>
</tr>
<tr>
<td>use</td>
<td>Includes read plus the ability to work with existing resources (the actions vary by resource type). Includes the ability to update the resource, except for resource-types where the &quot;update&quot; operation has the same effective impact as the &quot;create&quot; operation (e.g., UpdatePolicy, UpdateSecurityList, etc.), in which case the &quot;update&quot; ability is available only with the manage verb. In general, this verb does not include the ability to create or delete that type of resource.</td>
<td>Day-to-day end users of resources</td>
</tr>
<tr>
<td>manage</td>
<td>Includes all permissions for the resource.</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

**Resource-Types**

The family resource-types are listed below. For the individual resource-types that make up each family, follow the links.

- all-resources: All Oracle Cloud Infrastructure resource-types
- cluster-family: See Details for Container Engine for Kubernetes on page 2177
- compute-management-family: See Details for the Core Services on page 2181
- data-catalog-family: See Data Catalog Policies
- database-family: See Details for the Database Service on page 2240
- dns: See Details for the DNS Service on page 2262
- file-family: See Details for the File Storage Service on page 2273
- instance-family: See Details for the Core Services on page 2181
- object-family: See Details for Object Storage, Archive Storage, and Data Transfer on page 2324
- virtual-network-family: See Details for the Core Services on page 2181
- volume-family: See Details for the Core Services on page 2181

IAM has no family resource-type, only individual ones. See Details for IAM on page 2280.

**General Variables for All Requests**

You use variables when adding conditions to a policy. For more information, see Conditions on page 2160. Here are the general variables applicable to all requests.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request.user.id</td>
<td>Entity (OCID)</td>
<td>The OCID of the requesting user.</td>
</tr>
<tr>
<td>request.user.mfaTotpVerified</td>
<td>Boolean</td>
<td>Whether the user has been verified by multi-factor authentication (MFA). To restrict access to only MFA-verified users, add the condition where request.user.mfaTotpVerified = 'true' See Managing Multi-Factor Authentication on page 2470 for information on setting up MFA.</td>
</tr>
<tr>
<td>request.groups.id</td>
<td>List of entities (OCIDs)</td>
<td>The OCIDs of the groups the requesting user is in.</td>
</tr>
<tr>
<td>request.permission</td>
<td>String</td>
<td>The underlying permission being requested (see Permissions on page 2162).</td>
</tr>
<tr>
<td>request.operation</td>
<td>String</td>
<td>The API operation name being requested (for example, ListUsers).</td>
</tr>
<tr>
<td>request.networkSource.name</td>
<td>String</td>
<td>The name of the network source group that specifies allowed IP addresses the request may come from. See Managing Network Sources on page 2427 for information.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>request.region</td>
<td>String</td>
<td>The 3-letter key for the region the request is made in. Allowed values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AMS - use for Netherlands Northwest (Amsterdam)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BOM - use for India West (Mumbai)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CWL - use for UK West (Newport)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DXB - use for UAE East (Dubai)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FRA - use for Germany Central (Frankfurt)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GRU - use for Brazil East (Sao Paulo)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HYD - use for India South (Hyderabad)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IAD - use for US East (Ashburn)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ICN - use for South Korea Central (Seoul)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• JED - use for Saudi Arabia West (Jeddah)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• KIX - use for Japan Central (Osaka)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• LHR - use for UK South (London)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MEL - use for Australia Southeast (Melbourne)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NRT - use for Japan East (Tokyo)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PHX - use for US West (Phoenix)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SCL - use for Chile (Santiago)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SJC - use for US West (San Jose)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SYD - use for Australia East (Sydney)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• YNY - use for South Korea North (Chuncheon)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• YUL - use for Canada Southeast (Montreal)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• YYZ - use for Canada Southeast (Toronto)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ZRH - use for Switzerland North (Zurich)</td>
</tr>
<tr>
<td>request.ad</td>
<td>String</td>
<td>The name of the availability domain the request is made in. To get a list of availability domain names, use the ListAvailabilityDomains operation.</td>
</tr>
<tr>
<td>request.principal.compartment.tag</td>
<td>String</td>
<td>The tags applied to the compartment that the requesting resource belongs to are evaluated for a match. For usage instructions, see Using Tags to Manage Access on page 3932.</td>
</tr>
<tr>
<td>request.principal.group.tag</td>
<td>String</td>
<td>The tags applied to the groups that the user belongs to are evaluated for a match. For usage instructions, see Using Tags to Manage Access on page 3932.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>target.compartment.name</td>
<td>String</td>
<td>The name of the compartment specified in target.compartment.id.</td>
</tr>
<tr>
<td>target.compartment.id</td>
<td>Entity (OCID)</td>
<td>The OCID of the compartment containing the primary resource. Note: target.compartment.id and target.compartment.name cannot be used with a &quot;List&quot; API operation to filter the list based on the requesting user's access to the compartment.</td>
</tr>
<tr>
<td>target.resource.compartment.tag</td>
<td></td>
<td>The tag applied to the target compartment of the request is evaluated. For usage instructions, see Using Tags to Manage Access on page 3932.</td>
</tr>
<tr>
<td>target.resource.tag</td>
<td></td>
<td>The tag applied to the target resource of the request is evaluated. For usage instructions, see Using Tags to Manage Access on page 3932.</td>
</tr>
</tbody>
</table>

**Details for the Announcements Service**

This topic covers details for writing policies to control access to the Announcements service.

**Resource-Types**

- announcements

**Supported Variables**

Only the general variables are supported (see General Variables for All Requests on page 2169).

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the announcements resource-type includes the same permissions and API operations as the inspect verb, plus the ANNOUNCEMENT_READ permission and an additional API operation, GetAnnouncement. However, the use verb and manage verbs cover no extra permissions or API operations compared to read.

**announcements**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ANNOUNCEMENT_LIST</td>
<td>ListAnnouncements</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ANNOUNCEMENT_READ</td>
<td>GetAnnouncement</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
Permissions Required for Each API Operation
The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListAnnouncements</td>
<td>ANNOUNCEMENT_LIST</td>
</tr>
<tr>
<td>GetAnnouncement</td>
<td>ANNOUNCEMENT_READ</td>
</tr>
</tbody>
</table>

Details for API Gateway
This topic covers details for writing policies to control access to API Gateway.

Resource-Types

Aggregate Resource-Type
api-gateway-family

Individual Resource-Types
- api-gateways
- api-deployments
- api-definitions
- api-workrequests
- api-certificates

Comments
A policy that uses <verb> api-gateway-family is equivalent to writing one with a separate <verb> <individual resource-type> statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2173 for details of the API operations covered by each verb, for each individual resource-type included in api-gateway-family.

Supported Variables
API Gateway supports all the general variables (see General Variables for All Requests on page 2169).

Details for Verb + Resource-Type Combinations
The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the api-gateways resource-type includes the same permissions and API operations as the inspect verb, plus the API_GATEWAY_READ permission and a number of API operations (e.g., GetGateway, etc.). The use verb covers additional permissions and API operations compared to read. Lastly, manage covers more permissions and operations compared to use.

<table>
<thead>
<tr>
<th>api-gateways</th>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>inspect</td>
<td>API_GATEWAY_LIST</td>
<td>ListGateways</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>GetDeployment (also needs read api-deployments)</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 2173
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>CreateDeployment and</td>
</tr>
<tr>
<td></td>
<td>API_GATEWAY_ADD_DEPLOYMENT</td>
<td></td>
<td>DeleteDeployment (both also need manage api-deployments)</td>
</tr>
<tr>
<td></td>
<td>API_GATEWAY_REMOVE_DEPLOYMENT</td>
<td></td>
<td>UpdateDeployment (also needs use api-deployments)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>Use +</td>
<td>CreateGateway</td>
</tr>
<tr>
<td></td>
<td>API_GATEWAY_CREATE DeleteGateway</td>
<td></td>
<td>(also needs use api-certificates)</td>
</tr>
<tr>
<td></td>
<td>API_GATEWAY_DELETE UpdateGateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_GATEWAY_UPDATE ChangeGatewayCompartment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_GATEWAY_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**api-deployments**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>API_DEPLOYMENT_LIST ListDeployments</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>no extra</td>
<td>GetDeployment (also needs read api-gateways)</td>
</tr>
<tr>
<td></td>
<td>API_DEPLOYMENT_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>UpdateDeployment (also needs use api-gateways)</td>
</tr>
<tr>
<td></td>
<td>API_DEPLOYMENT_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeDeploymentCompartment</td>
<td>CreateDeployment and DeleteDeployment (both also need use api-gateways)</td>
</tr>
<tr>
<td></td>
<td>API_DEPLOYMENT_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_DEPLOYMENT_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_DEPLOYMENT_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**apiDefinitions**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>API_DEFINITION_LIST ListApis</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetApi</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_DEFINITION_READ GetApiContent</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_DEFINITION_READ GetApiDeploymentSpecification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_DEFINITION_READ GetApiValidations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateApi</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_DEFINITION_UPDATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### APIs Fully Covered

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE + CreateApi</td>
<td>CreateApi</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_DEFINITION_CREATEDeleteApi</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_DEFINITION_DELETEChangeApiCompartment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_DEPLOYMENT_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### api-workrequests

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>API_WORK_REQUEST_LIST</td>
<td>ListWorkRequests</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_WORK_REQUEST_READ</td>
<td>ReadWorkRequest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListWorkRequestErrors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListWorkRequestLogs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_WORK_REQUEST_CANCEL</td>
<td>CancelWorkRequest</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

### api-certificates

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>API_CERTIFICATE_LIST</td>
<td>ListCertificates</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_CERTIFICATE_READ</td>
<td>GetCertificate</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>CreateGateway (also needs manage api-gateways)</td>
</tr>
<tr>
<td></td>
<td>API_CERTIFICATE_APPLY_TO_GATEWAY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateCertificate</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>API_CERTIFICATE_CREATEDeleteCertificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_CERTIFICATE_DELETEUpdateCertificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_CERTIFICATE_UPDATEChangeCertificateCompartment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API_CERTIFICATE_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type. For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListGateways</td>
<td>API_GATEWAY_LIST</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CreateGateway</td>
<td>API_GATEWAY_CREATE and API_CERTIFICATE_APPLY_TO_GATEWAY</td>
</tr>
<tr>
<td>GetGateway</td>
<td>API_GATEWAY_READ</td>
</tr>
<tr>
<td>UpdateGateway</td>
<td>API_GATEWAY_UPDATE</td>
</tr>
<tr>
<td>DeleteGateway</td>
<td>API_GATEWAY_DELETE</td>
</tr>
<tr>
<td>ChangeGatewayCompartment</td>
<td>API_GATEWAY_READ and API_GATEWAY_UPDATE and API_GATEWAY_MOVE</td>
</tr>
<tr>
<td>ListDeployments</td>
<td>API_DEPLOYMENT_LIST</td>
</tr>
<tr>
<td>CreateDeployment</td>
<td>API_DEPLOYMENT_CREATE and API_GATEWAY_READ and API_GATEWAY_ADD_DEPLOYMENT</td>
</tr>
<tr>
<td>GetDeployment</td>
<td>API_DEPLOYMENT_READ and API_GATEWAY_READ</td>
</tr>
<tr>
<td>UpdateDeployment</td>
<td>API_DEPLOYMENT_UPDATE and API_GATEWAY_READ and API_GATEWAY_ADD_DEPLOYMENT</td>
</tr>
<tr>
<td>DeleteDeployment</td>
<td>API_DEPLOYMENT_DELETE and API_GATEWAY_READ and API_GATEWAY_REMOVE_DEPLOYMENT</td>
</tr>
<tr>
<td>ChangeDeploymentCompartment</td>
<td>API_DEPLOYMENT_READ and API_DEPLOYMENT_UPDATE and API_DEPLOYMENT_MOVE</td>
</tr>
<tr>
<td>ListApis</td>
<td>API_DEFINITION_LIST</td>
</tr>
<tr>
<td>CreateApi</td>
<td>API_DEFINITION_CREATE</td>
</tr>
<tr>
<td>GetApi</td>
<td>API_DEFINITION_READ</td>
</tr>
<tr>
<td>GetApiContent</td>
<td>API_DEFINITION_READ</td>
</tr>
<tr>
<td>GetApiDeploymentSpecification</td>
<td>API_DEFINITION_READ</td>
</tr>
<tr>
<td>GetApiValidations</td>
<td>API_DEFINITION_READ</td>
</tr>
<tr>
<td>UpdateApi</td>
<td>API_DEFINITION_UPDATE</td>
</tr>
<tr>
<td>DeleteApi</td>
<td>API_DEFINITION_DELETE</td>
</tr>
<tr>
<td>ChangeApiCompartment</td>
<td>API_DEFINITION_MOVE</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>API_WORK_REQUEST_LIST</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>API_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>CancelWorkRequest</td>
<td>API_WORK_REQUEST_CANCEL</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>API_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>API_WORK_REQUEST_READ</td>
</tr>
</tbody>
</table>
IAM

API Operation | Permissions Required to Use the Operation
---|---
ListCertificates | API_CERTIFICATE_LIST
CreateCertificate | API_CERTIFICATE_CREATE
GetCertificate | API_CERTIFICATE_READ
UpdateCertificate | API_CERTIFICATE_UPDATE
DeleteCertificate | API_CERTIFICATE_DELETE
ChangeCertificateCompartment | API_CERTIFICATE_MOVE

Details for the Audit Service

This topic covers details for writing policies to control access to the Audit service.

**Resource-Types**

audit-events

**Supported Variables**

Only the general variables are supported (see General Variables for All Requests on page 2169).

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the use and manage verbs for the audit-events resource-type cover no extra permissions or API operations compared to the read verb.

**audit-events**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>AUDIT_EVENT_READ</td>
<td>ListEvents</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListEvents</td>
<td>AUDIT_EVENT_READ</td>
</tr>
</tbody>
</table>

**Details for Container Engine for Kubernetes**

This topic covers details for writing policies to control access to Container Engine for Kubernetes.
Resource-Types

Aggregate Resource-Type

• cluster-family

Individual Resource-Types

• clusters
• cluster-node-pools
• cluster-work-requests

Comments

A policy that uses `<verb> cluster-family` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2178 for details of the API operations covered by each verb, for each individual resource-type included in `cluster-family`.

Supported Variables

Container Engine for Kubernetes supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

The `clusters` resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>target.cluster.id</code></td>
<td>Entity (OCID)</td>
<td></td>
</tr>
</tbody>
</table>

The `cluster-node-pools` resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>target.nodepool.id</code></td>
<td>Entity (OCID)</td>
<td></td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the `read` verb for the `clusters` resource-type includes the same permissions and API operations as the `inspect` verb, plus the CLUSTER_READ permission and a number of API operations (e.g., `GetCluster`, etc.). The `use` verb covers still another permission and API operation compared to `read`. Lastly, `manage` covers more permissions and operations compared to `use`.

<table>
<thead>
<tr>
<th><code>clusters</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verbs</strong></td>
</tr>
<tr>
<td>inspect</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Verbs</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>read</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>use</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>manage</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**cluster-node-pools**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>CLUSTER_NODE_POOL_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ListWorkRequests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>CLUSTER_NODE_POOL_READ</td>
<td>GetNodePool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestErrors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestLogs</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>CreateNodePool,</td>
</tr>
<tr>
<td></td>
<td>CLUSTER_NODE_POOL_CREATE</td>
<td></td>
<td>DeleteNodePool,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and UpdateNodePool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>instance-family,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>use subnets, use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vnics, and inspect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>compartments)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type. For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListClusters</td>
<td>CLUSTER_INSPECT</td>
</tr>
<tr>
<td>CreateCluster</td>
<td>CLUSTER_CREATE</td>
</tr>
<tr>
<td>GetClusterKubeconfig</td>
<td>CLUSTER_USE</td>
</tr>
<tr>
<td>GetCluster</td>
<td>CLUSTER_READ</td>
</tr>
<tr>
<td>UpdateCluster</td>
<td>CLUSTER_UPDATE</td>
</tr>
<tr>
<td>DeleteCluster</td>
<td>CLUSTER_DELETE, CLUSTER_NODE_POOL_DELETE</td>
</tr>
<tr>
<td>AdministerK8s</td>
<td>CLUSTER_MANAGE</td>
</tr>
<tr>
<td>ListNodePools</td>
<td>CLUSTER_NODE_POOL_INSPECT</td>
</tr>
<tr>
<td>CreateNodePool</td>
<td>CLUSTER_NODE_POOL_CREATE</td>
</tr>
<tr>
<td>GetNodePool</td>
<td>CLUSTER_NODE_POOL_READ</td>
</tr>
<tr>
<td>GetNodePoolOptions</td>
<td>CLUSTER_READ</td>
</tr>
<tr>
<td>UpdateNodePool</td>
<td>CLUSTER_NODE_POOL_UPDATE</td>
</tr>
<tr>
<td>DeleteNodePool</td>
<td>CLUSTER_NODE_POOL_DELETE</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>CLUSTER_WORK_REQUEST_INSPECT, CLUSTER_NODE_POOL_INSPECT, CLUSTER_INSPECT</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>CLUSTER_WORK_REQUEST_READ, CLUSTER_NODE_POOL_READ, CLUSTER_READ</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>CLUSTER_WORK_REQUEST_READ, CLUSTER_NODE_POOL_READ, CLUSTER_READ</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>CLUSTER_WORK_REQUEST_READ, CLUSTER_NODE_POOL_READ, CLUSTER_READ</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>DeleteWorkRequest</td>
<td>CLUSTER_WORK_REQUEST_DELETE</td>
</tr>
</tbody>
</table>

Details for the Core Services

This topic covers details for writing policies to control access to the Core Services (Networking, Compute, and Block Volume).

Resource-Types

Networking

Aggregate Resource-Type

virtual-network-family

Individual Resource-Types

vcns
subnets
route-tables
network-security-groups
security-lists
dhcp-options
private-ips
public-ips
ipv6s
internet-gateways
nat-gateways
service-gateways
local-peering-gateways (which includes local-peering-from, and local-peering-to)
remote-peering-connections (which includes remote-peering-from, and remote-peering-to)
drgs
drg-attachments
cpes
ipsec-connections
cross-connects
cross-connect-groups
virtual-circuits
vnics
vnic-attachments
vlans
byoirrange
publicippool
Comments

A policy that uses `<verb> virtual-network-family` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2183 for details of the API operations covered by each verb, for each individual resource-type included in `virtual-network-family`.

Compute

**instance-family Aggregate Resource-Type**

The `instance-family` aggregate resource-type covers these individual resource-types:

- app-catalog-listing
- console-histories
- instances
- instance-console-connection
- instance-images
- volume-attachments (includes only the permissions required for attaching volumes to instances)

**compute-management-family Aggregate Resource-Type**

The `compute-management-family` aggregate resource-type covers these individual resource-types:

- instance-configurations
- instance-pools
- cluster-networks

**instance-agent-family Aggregate Resource-Type**

The `instance-agent-family` aggregate resource-type covers this individual resource-type:

- instance-agent-plugins

**instance-agent-command-family Aggregate Resource-Type**

The `instance-agent-command-family` aggregate resource-type covers this individual resource-type:

- instance-agent-commands

**Additional Individual Resource-Types**

- auto-scaling-configurations
- dedicated-vm-hosts
- instance-agent-commands
- work-requests

Comments

A policy that uses `<verb> instance-family` or `<verb> compute-management-family` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types in the family.

See the table in Details for Verb + Resource-Type Combinations on page 2183 for details of the API operations covered by each verb, for each individual resource-type.
Block Volume

Aggregate Resource-Type
volume-family

Individual Resource-Types
volumes
volume-attachments
volume-backups
boot-volume-backups
backup-policies
backup-policy-assignments
volume-groups
volume-group-backups

Comments
A policy that uses <verb> volume-family is equivalent to writing one with a separate <verb> <individual resource-type> statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2183 for details of the API operations covered by each verb, for each individual resource-type included in volume-family.

Supported Variables
The Core Services support all the general variables, plus the ones listed here. For more information about general variables supported by Oracle Cloud Infrastructure services, see General Variables for All Requests on page 2169.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.boot-volume.kms-key.id</td>
<td>String</td>
<td>Use this variable to control whether Compute instances can be launched with boot volumes that were created without a Vault service master encryption key.</td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations
The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read and use verbs for the vcns resource-type cover no extra permissions or API operations compared to the inspect verb. However, the manage verb includes several extra permissions and API operations.

For virtual-network-family Resource Types
The following tables list the permissions and API operations covered by each of the individual resource-types included in virtual-network-family.
vcns

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VCN_READ</td>
<td>ListVcns</td>
<td>CreateNatGateway,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteNatGateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>nat-gateways and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage vcns)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetVcn</td>
<td>Note: The above</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>operations in this cell</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>are totally covered</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>with just manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>virtual-network-family</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td>VCN_ATTACH</td>
<td>CreateVcn</td>
<td>CreateSubnet,</td>
<td>DeleteSubnet (both also need manage route-tables and manage-security-lists and manage-dhcp-options)</td>
</tr>
<tr>
<td>VCN_DETACH</td>
<td>UpdateVcn</td>
<td>DeleteSubnet (both also need manage route-tables and manage-security-lists and manage-dhcp-options)</td>
<td></td>
</tr>
<tr>
<td>VCN_UPDATE</td>
<td>DeleteVcn,</td>
<td>DeleteSubnet (both also need manage route-tables and manage-security-lists and manage-dhcp-options)</td>
<td></td>
</tr>
<tr>
<td>VCN_CREATE</td>
<td>AddVcnCidr,</td>
<td>DeleteSubnet (both also need manage route-tables and manage-security-lists and manage-dhcp-options)</td>
<td></td>
</tr>
<tr>
<td>VCN_DELETE</td>
<td>ModifyVcnCidr, RemoveVcnCidr</td>
<td>DeleteSubnet (both also need manage route-tables and manage-security-lists and manage-dhcp-options)</td>
<td></td>
</tr>
<tr>
<td>VCN_MOVE</td>
<td>ChangeVcnCompartment, CreateInternetGateway, DeleteInternetGateway (also need manage internet-gateways)</td>
<td>DeleteSubnet (both also need manage route-tables and manage-security-lists and manage-dhcp-options)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateLocalPeeringGateway (also need manage local-peering-gateways, and need manage route-tables if you associate a route table during creation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteLocalPeeringGateway (also need manage local-peering-gateways)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateNatGateway, DeleteNatGateway (also need manage nat-gateways)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateNetworkSecurityGroup, DeleteNetworkSecurityGroup (also need manage network-security-groups)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateRouteTable, DeleteRouteTable (also need manage route-tables, manage internet-gateways, manage drgs, manage private-ips, manage local-peering-gateways, use nat-gateways, use service-gateways)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateServiceGateway, DeleteServiceGateway (also need manage service-gateways)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateSecurityList, DeleteSecurityList (also need manage security-lists)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateDhcpOptions,</td>
<td></td>
</tr>
</tbody>
</table>
## subnets

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SUBNET_READ</td>
<td>ListSubnets, GetSubnet</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
| use | READ + | no extra | LaunchInstance (also need use vnics, use network-security-groups, and manage instance-family)  
TerminateInstance (also need manage instance-family, and use volumes if a volume is attached)  
AttachVnic (also need manage instances, use network-security-groups, and either use vnics or use instance-family)  
DetachVnic (also need manage instances and either use vnics or use instance-family)  
CreatePrivateIp, DeletePrivateIp (both also need use private-ips and use vnics) |
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>SUBNET_CREATE</td>
<td>ChangeSubnetCompartment, DeleteSubnet (both also need manage vcns, manage route-tables, manage security-lists, manage dhcp-options)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SUBNET_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SUBNET_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SUBNET_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateSubnet (also need manage route-tables if changing which route table is associated with the subnet, manage security-lists if changing which security lists are associated with the subnet, and manage dhcp-options if changing which set of DHCP options is associated with the subnet)</td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td>The above operations in this cell are covered with just manage virtual-network-family.</td>
<td></td>
</tr>
</tbody>
</table>

### route-tables

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ROUTE_TABLE_READ</td>
<td>ListRouteTables</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetRouteTable</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE + no extra</td>
<td></td>
<td>CreateRouteTable,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteRouteTable</td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_ATTACH</td>
<td></td>
<td>ChangeRouteTable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Compartment</td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_DETACH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: All of the above operations in this cell are totally covered with just manage virtual-network-family.

network-security-groups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>NETWORK_SECURITY_GROUP_INSPECT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>NETWORK_SECURITY_GROUP_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListNetworkSecurityGroups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>READ +</td>
</tr>
<tr>
<td></td>
<td>NETWORK_SECURITY_GROUP_LIST_SECURITY_RULES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NETWORK_SECURITY_GROUP_LIST_MEMBERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NETWORK_SECURITY_GROUP_UPDATE_MEMBERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListNetworkSecurityGroupSecurityRules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListNetworkSecurityGroupVnics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LaunchInstance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AttachVnic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UpdateVnic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>NETWORK_SECURITY_GROUP_UPDATE_SECURITY_RULES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UpdateNetworkSecurityGroupSecurityRules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RemoveNetworkSecurityGroupSecurityRules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CreateNetworkSecurityGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DeleteNetworkSecurityGroup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Both of the above operations in this cell are totally covered with just manage virtual-network-family.

---

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SECURITY_LIST_READ</td>
<td>ListSecurityLists</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetSecurityList</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

security-lists
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE + UpdateSecurityList,</td>
<td>CreateSecurityList,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SECURITY_LIST_ATTACH</td>
<td>DeleteSecurityList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SECURITY_LIST_DETACH</td>
<td>(both also need manage vcns)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SECURITY_LIST_UPDATE</td>
<td>CreateSubnet,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SECURITY_LIST_CREATE</td>
<td>DeleteSubnet (both also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SECURITY_LIST_DELETE</td>
<td>subnets, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SECURITY_LIST_MOVE</td>
<td>ChangeSecurityListCompartment,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateSubnet,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteSubnet (both also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnets, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage route-tables,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage dhcp-options)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UpdateSubnet (if changing which security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lists are associated with the subnet, also</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>need manage subnets)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: All of the above operations in this</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cell are totally covered with just manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>virtual-network-family.</td>
</tr>
</tbody>
</table>

### dhcp-options

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DHCP_READ</td>
<td>ListDhcpOptions</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDhcpOptions</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE + UpdateDhcpOptions</td>
<td>CreateDhcpOptions, DeleteDhcpOptions (both also need manage vcns)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Ability to update a set of DHCP options is available only with the manage verb, not the use verb.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP_ATTACH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP_DETACH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### private-ips

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>PRIVATE_IP_READ</td>
<td>ListPrivateIps</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetPrivateIp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: For ephemeral public IPs only:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListPublicIps, GetPublicIpByPrivateIpId, GetPublicIpByIpAddress</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

Note: All of the above operations in this cell are totally covered with just manage virtual-network-family.
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>CreatePrivateIp,</td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_UPDATE</td>
<td>For ephemeral public IPs: UpdatePublicIp, CreatePublicIp, DeletePublicIp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_ASSIGN</td>
<td>UpdatePublicIp, CreatePublicIp, DeletePublicIp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_UNASSIGN</td>
<td>UpdatePrivateIp (also needs use vnics)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_CREATE</td>
<td>For reserved public IPs: UpdatePublicIp, CreatePublicIp, DeletePublicIp (all also need manage public-ips)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_DELETE</td>
<td>UpdatePrivateIp (also needs use vnics)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_ASSIGN_PUBLIC_IP</td>
<td>CreatePrivateIp, DeletePrivateIp (both also need use subnets and use vnics)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_UNASSIGN_PUBLIC_IP</td>
<td>UpdatePrivateIp (also needs use vnics)</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>CreateRouteTable, DeleteRouteTable (both also need manage vcns, manage internet-gateways, manage drgs, and manage route-tables, manage local-peering-gateways, use nat-gateways, use service-gateways)</td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_ROUTE_TABLE_ATTACH</td>
<td>UpdateRouteTable (also need manage internet-gateways, manage drgs, manage route-tables, manage local-peering-gateways, use nat-gateways, use service-gateways)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_ROUTE_TABLE_DETACH</td>
<td>Note: The above operations in this cell are totally covered with just manage virtual-network-family.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The above operations in this cell are totally covered with just use virtual-network-family.
### public-ips

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>PUBLIC_IP_READ</td>
<td>For reserved public IPs only: ListPublicIps, GetPublicIpByPrivateIpId, GetPublicIpByIpAddress</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Permissions for listing/getting ephemeral public IPs are part of the private-ip permissions.</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_ASSIGN_PRIVATE_IP</td>
<td>For reserved public IPs: UpdatePublicIp, CreatePublicIp, DeletePublicIp (all of these also need use private-ips and manage public-ips).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_UNASSIGN_PRIVATE_IP</td>
<td>Note: The above operations in this cell are totally covered with just manage virtual-network-family.</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_UPDATE</td>
<td>For reserved public IPs: UpdatePublicIp, CreatePublicIp, DeletePublicIp (all of these also need use private-ips).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_CREATE</td>
<td>Note: The above operations in this cell are totally covered with just manage virtual-network-family.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### byoip

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>BYOIP_RANGE_INSPECT</td>
<td>ListByoipRanges</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT+</td>
<td>GetByoipRange</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_READ</td>
<td>ListByoipAllocatedRanges</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>AddPublicIpPoolCapacity</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_ADD_CAPACITY_FROM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateByoipRange</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_CREATE</td>
<td>DeleteByoipRange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_DELETE</td>
<td>UpdateByoipRange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_UPDATE</td>
<td>ValidateByoipRange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_VALIDATE</td>
<td>AdvertiseByoipRange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_ADVERTISE</td>
<td>WithdrawByoipRange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_WITHDRAW</td>
<td>ChangeByoipRangeCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYOIP_RANGE_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### publicippool

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>PUBLIC_IP_POOL_INSPECT</td>
<td>ListPublicIpPool</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>ReadPublicIpPool</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>PUBLIC_IP_POOL_READ</td>
<td>CreatePublicIpPool</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>PUBLIC_IP_POOL_CREATE_PUBLIC_IP_FROM</td>
<td>UpdatePublicIpPool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USE +</td>
<td>CreatePublicIp</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_POOL_CREATE</td>
<td>DeletePublicIpPool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_POOL_DELETE</td>
<td>UpdatePublicIpPool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_POOL_UPDATE</td>
<td>AddPublicIpPoolCapacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_POOL_ADD_CAPACITY</td>
<td>RemovePublicIpPoolCapacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_POOL_REMOVE_CAPACITY</td>
<td>ChangePublicIpPoolCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC_IP_POOL_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### ipv6s

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>IPV6_READ</td>
<td>GetIpv6</td>
<td></td>
</tr>
</tbody>
</table>

*Note: The above operation in this cell is totally covered with just use virtual-network-family.*

---

Oracle Cloud Infrastructure User Guide 2194
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>IPV6_UPDATE</td>
<td></td>
<td>UpdateIpv6 (also need use vnics)</td>
</tr>
<tr>
<td></td>
<td>IPV6_CREATE</td>
<td></td>
<td>CreateIpv6, DeleteIpv6 (both also need use vnics and use subnets)</td>
</tr>
<tr>
<td></td>
<td>IPV6_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: The above operations in this cell are totally covered with just manage virtual-network-family.

---

**internet-gateways**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INTERNET_GATEWAY_READ</td>
<td>InternetGateways</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetInternetGateway</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>INTERNET_GATEWAY_ATTACH</td>
<td>CreateInternetGateway, DeleteInternetGateway (both also need manage vcns)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INTERNET_GATEWAY_DETACH</td>
<td>CreateRouteTable, DeleteRouteTable (both also need manage route-tables, manage drgs, manage private-ips, manage local-peering-gateways, use nat-gateways)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INTERNET_GATEWAY_UPDATE</td>
<td>UpdateRouteTable (also need manage route-tables, manage drgs, manage private-ips, manage local-peering-gateways, use nat-gateways, use service-gateways)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INTERNET_GATEWAY_CREATE</td>
<td>ChangeInternetGatewayCompartment, CreateInternetGateway, DeleteInternetGateway (both also need manage vcns)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INTERNET_GATEWAY_DELETE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>INTERNET_GATEWAY_MOVE</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Ability to update an internet gateway is available only with the `manage` verb, not the `use` verb.

---

**nat-gateways**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>NAT_GATEWAY_READ</td>
<td>ListNatGateways, GetNatGateway</td>
<td>none</td>
</tr>
</tbody>
</table>

**Note:** All of the above operations in this cell are totally covered with just manage virtual-network-family.
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>READ +</td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_ATTACH</td>
<td></td>
<td>CreateRouteTable, DeleteRouteTable (both also need manage route-tables, manage vcns, manage drgs, manage private-ips, manage internet-gateways, manage local-peering-gateways, use service-gateways)</td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_DETACH</td>
<td></td>
<td>UpdateRouteTable (also need manage route-tables, manage drgs, manage private-ips, manage internet-gateways, manage local-peering-gateways, use service-gateways)</td>
</tr>
</tbody>
</table>

**Note:** All of the above operations in this cell are totally covered with just manage virtual-network-family.

<table>
<thead>
<tr>
<th>manage</th>
<th>USE +</th>
<th>USE +</th>
<th>CREATENatGateway, DeleteNatGateway (both also need manage vcn)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NAT_GATEWAY_UPDATE</td>
<td>UpdateNatGateway</td>
<td>ChangeNatGatewayCompartment</td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_CREATE</td>
<td>ChangeNatGatewayCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_DELETE</td>
<td>Note: Ability to update a NAT gateway is available only with the manage verb, not the use verb.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_MOVE</td>
<td></td>
<td>Note: All of the above operations in this cell are totally covered with just manage virtual-network-family.</td>
</tr>
</tbody>
</table>

### service-gateways

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SERVICE_GATEWAY_READ</td>
<td>ListServiceGateways none</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetServiceGateway</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
</tbody>
</table>
### IAM

**Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
--- | --- | --- | ---
**use** | READ + | no extra | READ +
 | SERVICE_GATEWAY_ATTACH | | CreateRouteTable, DeleteRouteTable (both also need manage route-tables, manage vcns, manage internet-gateways, manage drgs, manage private-ips, manage local-peering-gateways)
 | SERVICE_GATEWAY_DETACH | UpdateRouteTable (also need manage route-tables, manage drgs, manage internet-gateways, manage private-ips, manage local-peering-gateways)
**manage** | USE + | USE + | CreateServiceGateway (also need manage vcns, and need manage route-tables if you associate a route table during creation)
 | SERVICE_GATEWAY_UPDATE | | UpdateServiceGateway (also need manage route-tables if you associate a route table during the update)
 | SERVICE_GATEWAY_CREATE | | DeleteServiceGateway (also need manage vcns)
 | SERVICE_GATEWAY_DELETE | | 
 | SERVICE_GATEWAY_ADD_SERVICE | | 
 | SERVICE_GATEWAY_DELETE_SERVICE | | 
 | SERVICE_GATEWAY_MOVE | | 
**local-peering-gateways** | **Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
--- | --- | --- | --- | ---
**inspect** | LOCAL_PEERING_GATEWAY_READ | LOCAL_PEERING_GATEWAY_READ, GetLocalPeeringGateway | none
**read** | no extra | no extra | none

Oracle Cloud Infrastructure User Guide 2198
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>CreateLocalPeeringGateway (also need manage vcns, and need manage route-tables if you associate a route table during creation)</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_UPDATE</td>
<td></td>
<td>UpdateLocalPeeringGateway (also need manage route-tables if you associate a route table during the update)</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_ATTACH</td>
<td></td>
<td>DeleteLocalPeeringGateway (also need manage vcns)</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_DETACH</td>
<td></td>
<td>CreateRouteTable, DeleteRouteTable (both also need manage route-tables, manage vcns, manage internet-gateways, manage drgs, manage private-ips, use nat-gateways, use service-gateways)</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_CREATE</td>
<td></td>
<td>UpdateRouteTable (also need manage route-tables, manage internet-gateways, manage drgs, manage private-ips, use nat-gateways, use service-gateways)</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_DELETE</td>
<td></td>
<td>ChangeLocalPeeringGatewayCompartment</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_MOVE</td>
<td></td>
<td>Note: The above operations in this cell are totally covered with just manage virtual-network-family.</td>
</tr>
</tbody>
</table>

### local-peering-from

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOCAL_PEERING_GATEWAY_READ</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>
### IAM

**Verbs**

<table>
<thead>
<tr>
<th>Verb</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE + no extra</td>
<td>ConnectLocalPeeringGateways (acceptor in the peering relationship must also grant the requestor manage local-peering-to in the compartment where the acceptor's LPG resides. See Local VCN Peering (Within Region) on page 3267.) Note: The above operation in this cell is totally covered with just manage virtual-network-family.</td>
<td></td>
</tr>
</tbody>
</table>

### local-peering-to

**Verbs**

<table>
<thead>
<tr>
<th>Verb</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOCAL_PEERING_GATEWAY_READ</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE + no extra</td>
<td>ConnectLocalPeeringGateways (requestor in the peering relationship must also have manage local-peering-from in the compartment where the requestor's LPG resides. See Local VCN Peering (Within Region) on page 3267.) Note: The above operation in this cell is totally covered with just manage virtual-network-family.</td>
<td></td>
</tr>
</tbody>
</table>

### remote-peering-connections

**Verbs**

<table>
<thead>
<tr>
<th>Verb</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>REMOTE_PEERING_CONNECTION_READ</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>GetRemotePeeringConnection</td>
<td>none</td>
</tr>
</tbody>
</table>
### remote-peering-from

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>REMOTE_PEERING_CONNECTION_READ</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>ConnectRemotePeeringConnections (acceptor in the peering relationship must also grant the requestor manage remote-peering-to in the compartment where the acceptor's RPC resides. See Remote VCN Peering (Across Regions) on page 3280.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: The above operation in this cell is totally covered with just manage virtual-network-family.</td>
</tr>
</tbody>
</table>

### remote-peering-to

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>REMOTE_PEERING_CONNECTION_READ</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>
### manage

<table>
<thead>
<tr>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>USE +</td>
<td>no extra</td>
<td></td>
</tr>
<tr>
<td>REMOTE_PEERING_CONNECTION_CONNECT_TO</td>
<td></td>
<td>ConnectRemotePeeringConnection</td>
</tr>
</tbody>
</table>

(requestor in the peering relationship must also have manage remote-peering-from in the compartment where the requestor's RPC resides. See Remote VCN Peering (Across Regions) on page 3280.)

**Note:** The above operation in this cell is totally covered with just manage virtual-network-family.

---

### drgs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DRG_READ</td>
<td>ListDrgs</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DRG_ATTACHMENT_READ</td>
<td>ListDrg</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>CreateDrgAttachment</td>
</tr>
<tr>
<td></td>
<td>DRG_ATTACH</td>
<td>CreateDrg</td>
<td>(also need manage</td>
</tr>
<tr>
<td></td>
<td>DRG_DETACH</td>
<td>UpdateDrg</td>
<td>route-tables if you</td>
</tr>
<tr>
<td></td>
<td>DRG_UPDATE</td>
<td>DeleteDrg</td>
<td>associate a route table</td>
</tr>
<tr>
<td></td>
<td>DRG_ATTACHMENT_UPDATE</td>
<td>UpdateDrgAttachment</td>
<td>during creation)</td>
</tr>
<tr>
<td></td>
<td>DRG_CREATE</td>
<td></td>
<td>DeleteDrgAttachment</td>
</tr>
<tr>
<td></td>
<td>DRG_DELETE</td>
<td></td>
<td>(also need manage</td>
</tr>
<tr>
<td></td>
<td>DRG_MOVE</td>
<td></td>
<td>route-tables if you</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage internet-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gateways, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>private-ips, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>internet-gateways,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage peering-gateways,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>use nat-gateways,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>use service-gateways)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UpdateRouteTable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>route-tables, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>internet-gateways,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage private-ips,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage internet-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage internet-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gateways, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>virtual-circuits,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and if you're also</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>changing which</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cross-connect or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cross-connect group the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>virtual circuit uses,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cross-connects)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateVirtualCircuit,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteVirtualCircuit,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage virtual-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>circuits, and if you're</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>also adding or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>removing the virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>circuit to/from a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cross-connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>group, also need</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage cross-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connect)</td>
</tr>
</tbody>
</table>

Note: All of the above operations in this cell are totally covered with just manage virtual-network-family.
### cpes

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>CPE_READ</td>
<td>ListCpes, GetCpe</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>CreateIPSecConnection, DeleteIPSecConnection</td>
</tr>
<tr>
<td></td>
<td>CPE_ATTACH</td>
<td>CreateCpe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPE_DETACH</td>
<td>UpdateCpe, DeleteCpe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPE_UPDATE</td>
<td>DeleteCpe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPE_CREATE</td>
<td>ChangeCpeCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPE_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPERESOURCE_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ipsec

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>IPSEC_CONNECTION_READ</td>
<td>ListIPSecConnections, GetIPSecConnection, GetIPSecConnectionStatus, ListIPSecConnectionTunnels, GetIPSecConnectionTunnel, GetTunnelCpeDeviceConfig, GetTunnelCpeDeviceTemplateContent, GetCpeDeviceTemplateContent, GetIpsecCpeDeviceTemplateContent</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>IPSEC_CONNECTION_DEVICE_CONFIG_READ</td>
<td>GetIPSecConnectionTunnelSharedSecret</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td><strong>manage</strong></td>
<td>USE +</td>
<td><strong>CreateIPSecConnection, DeleteIPSecConnection</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(both also need <strong>manage</strong> <strong>cpes</strong> and <strong>manage</strong> <strong>drgs</strong>)</td>
<td></td>
</tr>
<tr>
<td>IPSEC_CONNECTION_CREATE</td>
<td></td>
<td><strong>UpdateIPSecConnection</strong></td>
<td></td>
</tr>
<tr>
<td>IPSEC_CONNECTION_UPDATE</td>
<td></td>
<td><strong>UpdateTunnelCpeDeviceConfig</strong></td>
<td></td>
</tr>
<tr>
<td>IPSEC_CONNECTION_DELETE</td>
<td></td>
<td><strong>UpdateIPSecConnectionTunnel</strong></td>
<td></td>
</tr>
<tr>
<td>IPSEC_CONNECTION_DEVICE_CONFIG_UPDATE</td>
<td></td>
<td><strong>CreateIPSecConnection, DeleteIPSecConnection</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(both also need <strong>manage</strong> <strong>cpes</strong> and <strong>manage</strong> <strong>drgs</strong>)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td>All of the above operations in this cell are totally covered with just manage <strong>virtual-network-family</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### cross-connects

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inspect</strong></td>
<td>CROSS_CONNECT_READ</td>
<td><strong>ListCrossConnects</strong></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>GetCrossConnect</strong></td>
<td></td>
</tr>
<tr>
<td><strong>read</strong></td>
<td>no extra</td>
<td><strong>GetCrossConnect</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>no extra</td>
<td><strong>GetCrossConnect</strong></td>
<td>no extra</td>
</tr>
<tr>
<td><strong>manage</strong></td>
<td>USE +</td>
<td><strong>UpdateCrossConnect</strong></td>
<td><strong>UpdateVirtualCircuit</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(also need use <strong>virtual-circuits</strong>)</td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_UPDATE</td>
<td></td>
<td><strong>CreateCrossConnect</strong></td>
<td><strong>DeleteCrossConnect</strong></td>
</tr>
<tr>
<td>CROSS_CONNECT_CREATE</td>
<td></td>
<td><strong>DeleteCrossConnect</strong></td>
<td><strong>ChangeCrossConnectCompartment</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>CreateVirtualCircuit</strong>, <strong>DeleteVirtualCircuit</strong> (also need manage <strong>virtual-circuits</strong>)</td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_DELETE</td>
<td></td>
<td><strong>ChangeCrossConnectCompartment</strong></td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_RESOURCE_MOVE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_ATTACH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_DETACH</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### cross-connect-groups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inspect</strong></td>
<td>CROSS_CONNECT_GROUP_READ</td>
<td><strong>ListCrossConnectGroup</strong></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>GetCrossConnectGroup</strong></td>
<td></td>
</tr>
<tr>
<td><strong>read</strong></td>
<td>no extra</td>
<td><strong>GetCrossConnectGroup</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>no extra</td>
<td><strong>GetCrossConnectGroup</strong></td>
<td>no extra</td>
</tr>
<tr>
<td><strong>manage</strong></td>
<td>USE +</td>
<td><strong>UpdateCrossConnectGroup</strong></td>
<td><strong>UpdateVirtualCircuit</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(also need use <strong>virtual-circuits</strong>)</td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_GROUP_UPDATE</td>
<td></td>
<td><strong>CreateCrossConnectGroup</strong></td>
<td><strong>DeleteCrossConnectGroup</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>DeleteCrossConnectGroup</strong></td>
<td><strong>ChangeCrossConnectGroupCompartment</strong></td>
</tr>
<tr>
<td>CROSS_CONNECT_GROUP_CREATE</td>
<td></td>
<td></td>
<td><strong>CreateVirtualCircuit</strong>, <strong>DeleteVirtualCircuit</strong> (also need manage <strong>virtual-circuits</strong>)</td>
</tr>
<tr>
<td>CROSS_CONNECT_GROUP_DELETE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CROSS_CONNECT_GROUP_RESOURCE_MOVE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### virtual-circuits

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VIRTUAL_CIRCUIT_READ</td>
<td>ListVirtualCircuits, GetVirtualCircuit</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>UpdateVirtualCircuit (also need manage drgs, and if you're also changing which cross-connect or cross-connect group the virtual circuit uses, also need manage cross-connects)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeVirtualCircuitCompartment</td>
<td>VIRTUAL_CIRCUIT_CREATE, VIRTUAL_CIRCUIT_DELETE, VIRTUAL_CIRCUIT_RESOURCE_MOVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateVirtualCircuit, DeleteVirtualCircuit (both also need manage drgs, and if you're also creating/deleting the virtual circuit with a mapping to a specific cross-connect or cross-connect group, also need manage cross-connects)</td>
</tr>
</tbody>
</table>

**Note:** All of the above operations in this cell are totally covered with just manage virtual-network-family.

### vnics

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VNIC_READ</td>
<td>GetVnic</td>
<td>CreateInstanceConfiguration (if using the subtype. Also need read instances, inspect vnic-attachments, inspect volumes, and inspect volume-attachments.)</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 2206
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ + no extra</td>
<td>READ +</td>
<td></td>
</tr>
<tr>
<td>VNIC_ATTACH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNIC_DETACH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNIC_CREATE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNIC_DELETE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNIC_UPDATE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNIC_DISASSOCIATE_NETWORK_SECURITY_GROUP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

manage no extra no extra no extra

**vnic-attachments**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VNIC_ATTACHMENT_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra none</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>no extra none</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>no extra none</td>
<td>no extra</td>
<td>no extra</td>
</tr>
</tbody>
</table>
### vlans

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><strong>VLAN_READ</strong></td>
<td>ListVlans</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetVlan</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td><strong>READ +</strong></td>
<td>UpdateVlan</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td><strong>USE +</strong></td>
<td>no extra</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td><strong>VLAN_CREATE</strong></td>
<td>ChangeVlanCompartment</td>
<td>CreateVlan,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteVlan (both also</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>need manage vcns,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>manage route-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>tables, manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>security-lists)</td>
</tr>
<tr>
<td></td>
<td><strong>VLAN_DELETE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>VLAN_ASSOCIATE_NETWORK_SECURITY_GROUP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>VLAN_DISASSOCIATE_NETWORK_SECURITY_GROUP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>VLAN_MOVE</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The above operations in this cell are covered with just manage virtual-network-family.

---

**For instance-family Resource Types**

The instance-family aggregate resource-type includes extra permissions beyond the sum of the permissions for the individual resource-types included in instance-family. For example: It includes a few permissions for vnics and volumes, even though those resource-types aren’t generally considered part of the instance-family. Why are there extras included? So you can write fewer policy statements to cover general use cases, like working with an instance that has an attached block volume. You can write one statement for instance-family instead of multiple statements covering instances, vnics, and volumes.

Here’s a list of the extra permissions:

**For inspect instance-family:**
- **VNIC_READ**
- **VNIC_ATTACHMENT_READ**
- **VOLUME_ATTACHMENT_INSPECT**

**For read instance-family:**
- **VOLUME_ATTACHMENT_READ**

**For use instance-family:**
- **VNIC_ATTACH**
- **VNIC_DETACH**
- **VOLUME_ATTACHMENT_UPDATE**

**For manage instance-family:**
- **VOLUME_ATTACHMENT_CREATE**
- **VOLUME_ATTACHMENT_DELETE**

The following tables list the permissions and API operations covered by each of the individual resource-types included in instance-family.
### instances

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_INSPECT</td>
<td>none</td>
<td>GetConsoleHistory, ListConsoleHistories (both also need inspect console-histories)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ListVnicAttachments (also need inspect vnic-attachments)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ListVolumeAttachments (also need inspect volumes and inspect volume-attachments)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GetVolumeAttachments (also need inspect volumes and inspect volume-attachments)</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>ListInstances</td>
<td>INSPECT +</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_READ</td>
<td>GetInstance</td>
<td>CaptureConsoleHistory (also need manage console-histories and read instance-images)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ShowConsoleHistoryData (also need read console-histories and read instance-images)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateInstanceConfiguration (if using the CreateInstanceConfigurationFromInstanceDetails subtype. Also need inspect vnics, inspect vnic-attachments, inspect volumes, and inspect volume-attachments.)</td>
</tr>
</tbody>
</table>

**Note:** ListInstances and GetInstance include any user-provided metadata added to the instance.
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>READ +</td>
</tr>
<tr>
<td>INSTANCE_UPDATE</td>
<td>UpdateInstance</td>
<td></td>
<td>CreateImage (also need manage instance-images)</td>
</tr>
<tr>
<td>INSTANCE_CREATE_IMAGE</td>
<td>InstanceAction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INSTANCE_POWER_ACTIONS</td>
<td></td>
<td></td>
<td>AttachVolume (also need manage volume-attachments and use volumes)</td>
</tr>
<tr>
<td>INSTANCE_ATTACH_VOLUME</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INSTANCE_DETACH_VOLUME</td>
<td></td>
<td></td>
<td>DetachVolume (also need manage volume-attachments and use volumes)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>INSTANCE_CREATE</td>
<td>![LaunchInstance](also need read instance-images, use vnics, use subnets, use network-security-groups, and read app-catalog-listing. To launch instances using the Console, also need inspect vcns.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTANCE_DELETE</td>
<td>![TerminateInstance](also need use vnics and use subnets; also need manage volume-attachments and use volumes if a volume is attached)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTANCE_ATTACH_SECONDARY_VNIC</td>
<td>![AttachVnic](also need use subnets, use network-security-groups, and either use vnics or use instance-family)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTANCE_DETACH_SECONDARY_VNIC</td>
<td>![DetachVnic](also need use subnets and either use vnics or use instance-family)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTANCE_MOVE</td>
<td>![GetWorkRequest](inspect instances)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>![ListWorkRequestErrors](ListConsoleHistories, GetConsoleHistory)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>(both also need inspect instances)</em></td>
</tr>
</tbody>
</table>

**console-histories**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>CONSOLE_HISTORY_INSPECT</td>
<td></td>
<td>ListConsoleHistories, GetConsoleHistory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>(both also need inspect instances)</em></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>none</td>
<td>INSPECT +</td>
</tr>
<tr>
<td></td>
<td>CONSOLE_HISTORY_READ</td>
<td></td>
<td>ShowConsoleHistoryData</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also need read instances and read instance-images)</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>none</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DeleteConsoleHistory</td>
<td>CaptureConsoleHistory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also need read instances and read instance-images)</td>
</tr>
</tbody>
</table>

instance-console-connection

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_CONSOLE_CONNECTION_INSPECT</td>
<td>ListInstanceConsoleConnections</td>
<td>ListInstanceConsoleConnections (also need inspect instances and read instances)</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>none</td>
<td>INSPECT +</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONSOLE_CONNECTION_READ</td>
<td></td>
<td>GetInstanceConsoleConnection (also need read instances)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>none</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DeleteInstanceConsoleConnection</td>
<td>UpdateInstanceConsoleConnection (also need read instances)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

instance-images

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_IMAGE_INSPECT</td>
<td>ListImages, getImage</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + no extra</td>
<td>INSTANCE_IMAGE_READ</td>
<td>INSPECT +</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LaunchInstance (also need manage instances, use vnics, use subnets, and use network-security-groups)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CaptureConsoleHistory (also need read instances and manage console-histories)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ShowConsoleHistoryData (also need read instances and read console-histories)</td>
</tr>
<tr>
<td>use</td>
<td>READ + UpdateImage</td>
<td>INSTANCE_IMAGE_UPDATE</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE + DeleteImage</td>
<td>INSTANCE_IMAGE_CREATE, INSTANCE_IMAGE_DELETE, INSTANCE_IMAGE_MOVE</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ChangeImageCompartment, CreateImage</td>
<td>GetWorkRequest, ListWorkRequestErrors, and ListWorkRequestLogs (for work requests related to instance-images resource types. All also need the permissions for CreateImage)</td>
</tr>
</tbody>
</table>

**app-catalog-listing**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>APP_CATALOG_LISTING_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + no extra</td>
<td>APP_CATALOG_LISTING_READ</td>
<td>INSPECT +</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LaunchInstance (Also need use instances, read instance-images, use vnics, use subnets, and use network-security-groups)</td>
</tr>
</tbody>
</table>
### IAM

#### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>APP_CATALOG_LISTING_SUBSCRIBE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CreateAppCatalogSubscription</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DeleteAppCatalogSubscription</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### For compute-management-family Resource Types

The following tables list the permissions and API operations covered by each of the individual resource-types included in compute-management-family.

### instance-configurations

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_CONFIGURATION_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONFIGURATION_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONFIGURATION_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONFIGURATION_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONFIGURATION_LAUNCH</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONFIGURATION_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CONFIGURATION_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CreateInstanceConfiguration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UpdateInstanceConfiguration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LaunchInstanceConfiguration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DeleteInstanceConfiguration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ChangeInstanceConfigurationCompartment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### instance-pools

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_POOL_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_POOL_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListInstancePools</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListInstancePoolInstances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>ResetInstancePool</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_POOL_POWER_ACTIONS</td>
<td></td>
<td>StartInstancePool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>StopInstancePool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All also need use instances.</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>--------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_POOL_CREATE</td>
<td>UpdateInstancePool</td>
<td>CreateInstancePool (also need manage instances, read instance-images, use vnics, and use subnets)</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_POOL_UPDATE</td>
<td>ChangeInstancePoolCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_POOL_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_POOL_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TerminateInstancePool (also need manage instances, use vnics, use subnets, manage volume-attachments, and use volumes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest, ListWorkRequestErrors, and ListWorkRequestLogs (for work requests related to instance-pools resource types. All also need the permissions for CreateInstancePool or TerminateInstancePool, depending on the operation that spawns the work request)</td>
<td></td>
</tr>
</tbody>
</table>

**cluster-networks**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>CLUSTER_NETWORK_INSPECT</td>
<td>ListClusterNetworks</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>ListClusterNetworkInstances (also need read instance-pools)</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateClusterNetwork</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLUSTER_NETWORK_CREATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLUSTER_NETWORK_UPDATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLUSTER_NETWORK_DELETE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLUSTER_NETWORK_MOVE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(also need manage instances, manage instance-pools,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>read instance-images, use vnics, and use subnets)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TerminateClusterNetwork</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(also need manage instances, manage instance-pools,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>use vnics, use subnets, manage volume-attachments,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and use volumes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest, ListWorkRequestErrors, and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestLogs (for work requests related to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>cluster-networks resource types. All also need the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>permissions for CreateClusterNetwork or TerminateClusterNetwork, depending on the operation that spawns the work request)</td>
<td></td>
</tr>
</tbody>
</table>

For instance-agent-command-family Resource Types

The following table lists the permissions and API operations covered by each of the individual resource-types included in instance-agent-command-family.

### instance-agent-commands

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_AGENT_COMMAND_INSPECT</td>
<td>ListInstanceAgentCommands (to view commands in the Console, also need read instances)</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_AGENT_COMMAND_READ</td>
<td>ListInstanceAgentCommand</td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_AGENT_COMMAND_EXECUTION_INSPECT</td>
<td>ListInstanceAgentCommandExecution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_AGENT_COMMAND_EXECUTION_READ</td>
<td>ListInstanceAgentCommandExecution</td>
<td></td>
</tr>
</tbody>
</table>
## IAM

### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_AGENT_COMMAND_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INSTANCE_AGENT_COMMAND_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

### For instance-agent-family Resource Types

The following table lists the permissions and API operations covered by each of the individual resource-types included in `instance-agent-family`.

#### instance-agent-plugins

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSTANCE_AGENT_PLUGIN_INSPECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListInstanceAgentPlugins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_AGENT_PLUGIN_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(to view plugins in the Console, also need read instances)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

### For Additional Compute Individual Resource Types

The following tables list the permissions and API operations covered by other Compute resource-types that aren't included in any aggregate resource-types.

#### auto-scaling-configurations

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTO_SCALING_CONFIGURATION_INSPECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListAutoScalingConfigurations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListAutoScalingPolicies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>AUTO_SCALING_CONFIGURATION_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GetAutoScalingPolicy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE + AUTO_SCALING_CONFIGURATION_CREATE</td>
<td>USE + UpdateAutoScalingConfiguration</td>
<td>AUTO_SCALING_CONFIGURATION_UPDATE DeleteAutoScalingConfiguration AUTO_SCALING_CONFIGURATION_DELETE CreateAutoScalingPolicy AUTO_SCALING_CONFIGURATION_MOVE UpdateAutoScalingPolicy DeleteAutoScalingPolicy</td>
</tr>
</tbody>
</table>

**dedicated-vm-hosts**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DEDICATED_VM_HOST_INSPECT INSPECT +</td>
<td>none</td>
<td>ListDedicatedVmHostInstances</td>
</tr>
<tr>
<td>read</td>
<td>DEDICATED_VM_HOST_READ</td>
<td>none</td>
<td>ListDedicatedVmHostInstances</td>
</tr>
<tr>
<td>use</td>
<td>DEDICATED_VM_HOST_LAUNCH_INSTANCE DEDICATED_VM_HOST_UPDATE</td>
<td>INSPECT +</td>
<td>LaunchInstance</td>
</tr>
<tr>
<td>manage</td>
<td>USE + DEDICATED_VM_HOST_CREATE DEDICATED_VM_HOST_MOVE DEDICATED_VM_HOST_DELETE</td>
<td>USE +</td>
<td>CreateDedicatedVmHost DeleteDedicatedVmHostChangeDedicatedVmHostCompartment</td>
</tr>
</tbody>
</table>

**work-requests**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>WORKREQUEST_INSPECT</td>
<td>ListWorkRequests</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
For volume-family Resource Types

The following tables list the permissions and API operations covered by each of the individual resource-types included in volume-family.

### volumes

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VOLUME_INSPECT</td>
<td>ListVolumes, GetVolume</td>
<td>ListVolumeBackups, GetVolumeBackup, UpdateVolumeBackup, DeleteVolumeBackup, GetVolumeAttachment (also need inspect instances and inspect volume-attachments). If you need to get the CHAP secret if it exists, read volume-attachments is required. CreateInstanceConfiguration (if using the CreateInstanceConfigurationFromInstanceDetails subtype. Also need read instances, inspect vnic, inspect vnic-attachments, and inspect volume-attachments.)</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>READ + CreateVolumeBackup and DetachVolume (both also need manage volume-attachments, use instances)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
### IAM

#### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>manage</strong></td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>VOLUME_CREATE</td>
<td>CreateVolume</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VOLUME_DELETE</td>
<td>DeleteVolume</td>
<td>If creating a volume <em>from a backup</em>, also need read volume-backups.</td>
</tr>
<tr>
<td></td>
<td>VOLUME_MOVE</td>
<td>ChangeVolumeCompartment</td>
<td>If creating a volume <em>encrypted with a Vault service master encryption key</em>, also need use key-delegate (for the caller) and read keys (for the service principal). For more information, see Details for the Vault Service on page 2347.</td>
</tr>
</tbody>
</table>

When moving volumes between compartments, the move volume permission is needed for both source and destination compartments.

#### volume-attachments

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inspect</strong></td>
<td>VOLUME_ATTACHMENT_INSPECT</td>
<td></td>
<td>SetVolumeAttachment (also need inspect volumes and inspect instances)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: The CHAP secret (if it exists) is NOT included with inspect volume-attachments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateInstanceConfiguration (if using the CreateInstanceConfigurationFromInstanceDetails subtype. Also need read instances, inspect vnics, inspect vnic-attachments, and inspect volumes.)</td>
</tr>
<tr>
<td><strong>read</strong></td>
<td>INSPECT +</td>
<td>no extra</td>
<td>Same as for inspect volume-attachments, except that GetVolumeAttachment also includes the CHAP secret, if it exists.</td>
</tr>
<tr>
<td></td>
<td>VOLUME_ATTACHMENT_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>READ +</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>VOLUME_ATTACHMENT_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>VOLUME_ATTACHMENT_CREATE</td>
<td></td>
<td>AttachVolume, DetachVolume (both also need use volumes and use instances)</td>
</tr>
<tr>
<td></td>
<td>VOLUME_ATTACHMENT_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### volume-backups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VOLUME_BACKUP_INSPECT</td>
<td>none</td>
<td>ListVolumeBackups, GetVolumeBackup (both also need inspect volumes)</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>none</td>
<td>INSPECT +</td>
</tr>
<tr>
<td></td>
<td>VOLUME_BACKUP_READ</td>
<td></td>
<td>CreateVolume when creating volume from an backup (also need manage volumes)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>none</td>
<td>READ +</td>
</tr>
<tr>
<td></td>
<td>VOLUME_BACKUP_COPY</td>
<td></td>
<td>UpdateVolumeBackup (also need inspect volumes)</td>
</tr>
<tr>
<td></td>
<td>VOLUME_BACKUP_UPDATE</td>
<td></td>
<td>CopyVolumeBackup (also need create volume backups in destination region)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeVolumeBackupCompartment</td>
<td>CreateVolumeBackup (also need use volumes)</td>
</tr>
<tr>
<td></td>
<td>VOLUME_BACKUP_CREATE</td>
<td></td>
<td>DeleteVolumeBackup (also need inspect volumes)</td>
</tr>
<tr>
<td></td>
<td>VOLUME_BACKUP_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VOLUME_BACKUP_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### boot-volume-backups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>BOOT_VOLUME_BACKUP_INSPECT</td>
<td></td>
<td>ListBootVolumeBackups, GetBootVolumeBackup (both also need inspect volumes)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------</td>
<td>---------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + BOOT_VOLUME_BACKUP_READ</td>
<td>none</td>
<td>INSPECT + CreateBootVolume when creating volume from an backup (also need manage volumes)</td>
</tr>
<tr>
<td>use</td>
<td>READ + BOOT_VOLUME_BACKUP_UPDATE</td>
<td>none</td>
<td>READ + UpdateBootVolumeBackup (also need inspect volumes)</td>
</tr>
<tr>
<td></td>
<td>USE + BOOT_VOLUME_BACKUP_CREATE</td>
<td>none</td>
<td>USE + ChangeVolumeBackupCompartment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>backup-policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>inspect</td>
<td>BACKUP_POLICY_INSPECT</td>
<td>ListVolumeBackupPolicies</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>GetVolumeBackupPolicy</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td></td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td></td>
<td>USE +</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BACKUP_POLICIES_CREATE</td>
<td>CreateVolumeBackupPolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BACKUP_POLICIES_DELETE</td>
<td>DeleteVolumeBackupPolicy</td>
<td></td>
</tr>
<tr>
<td>backup-policy-assignments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>inspect</td>
<td>BACKUP_POLICY_ASSIGNMENT_INSPECT</td>
<td>GetVolumeBackupPolicyAssetAssignment</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>(also need inspect volumes)</td>
<td></td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>use</strong></td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td><strong>manage</strong></td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><strong>BACKUP_POLICY_ASSIGNMENT_CREATE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>BACKUP_POLICY_ASSIGNMENT_DELETE</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**volume-groups**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inspect</strong></td>
<td><strong>VOLUME_GROUP_INSPECT</strong></td>
<td>ListVolumeGroups</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetVolumeGroup</td>
<td></td>
</tr>
<tr>
<td><strong>read</strong></td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td><strong>use</strong></td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_UPDATE</td>
<td>DeleteVolumeGroup</td>
<td>UpdateVolumeGroup</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_CREATE</td>
<td></td>
<td>(also need inspect volume for the volumes in the request)</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_DELETE</td>
<td></td>
<td>CreateVolumeGroup</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If creating a volume group from a list of volumes, also need inspect volume for the volumes to include in the group.

If creating a volume group from another volume group, also need the following:

- inspect volume group for the source volume group
- create volume group for the destination volume group
- write volume for the source volumes
- create volume for the destination volumes
- write volume for the destination volumes

If creating a volume group from a volume group backup, also need the following:

- inspect volume group backup for the source volume group
- create volume group for the destination volume group
- read volume backup or read boot volume backup for the source volumes
- create volume for the destination volumes
- write volume for the destination volumes

When moving volume groups between compartments, the move volume group and move volume permissions are needed for both source and destination compartments.
volume-group-backups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VOLUME_GROUP_BACKUP_INSPECT</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_BACKUP_UPDATE</td>
<td>also need the following:</td>
<td>also need delete</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_BACKUP_CREATE</td>
<td>DeleteVolumeGroupBackup</td>
<td>volume backup or delete boot volume backup</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_BACKUP_DELETE</td>
<td>also need move volume backup or move boot volume backup for the volumes in the request</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_BACKUP_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Permissions Required for Each API Operation

The following tables list the API operations grouped by resource type. The resource types are listed in alphabetical order.

For information about permissions, see Permissions on page 2162.

Core Services API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateVolumeBackupPolicy</td>
<td>BACKUP_POLICIES_CREATE</td>
</tr>
<tr>
<td>DeleteVolumeBackupPolicy</td>
<td>BACKUP_POLICIES_DELETE</td>
</tr>
<tr>
<td>GetVolumeBackupPolicy</td>
<td>BACKUP_POLICIES_INSPECT</td>
</tr>
<tr>
<td>ListVolumeBackupPolicies</td>
<td>BACKUP_POLICIES_INSPECT</td>
</tr>
<tr>
<td>CreateVolumeBackupPolicyAssignment</td>
<td>BACKUP_POLICY_ASSIGNMENT_CREATE</td>
</tr>
<tr>
<td>DeleteVolumeBackupPolicyAssignment</td>
<td>BACKUP_POLICY_ASSIGNMENT_DELETE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GetVolumeBackupPolicyAssetAssignment</td>
<td>BACKUP_POLICY_ASSIGNMENT_INSPECT and VOLUME_INSPECT</td>
</tr>
<tr>
<td>GetVolumeBackupPolicyAssignment</td>
<td>BACKUP_POLICY_ASSIGNMENT_INSPECT</td>
</tr>
<tr>
<td>ListClusterNetworks</td>
<td>CLUSTER_NETWORK_INSPECT and INSTANCE_POOL_INSPECT</td>
</tr>
<tr>
<td>ListClusterNetworkInstances</td>
<td>CLUSTER_NETWORK_READ and INSTANCE_POOL_READ</td>
</tr>
<tr>
<td>GetClusterNetwork</td>
<td>CLUSTER_NETWORK_READ and INSTANCE_POOL_READ</td>
</tr>
<tr>
<td>UpdateClusterNetwork</td>
<td>CLUSTER_NETWORK_UPDATE</td>
</tr>
<tr>
<td>CreateClusterNetwork</td>
<td>CLUSTER_NETWORK_CREATE and INSTANCE_POOL_CREATE</td>
</tr>
<tr>
<td>ChangeClusterNetworkCompartment</td>
<td>CLUSTER_NETWORK_MOVE</td>
</tr>
<tr>
<td>TerminateClusterNetwork</td>
<td>CLUSTER_NETWORK_DELETE and INSTANCE_POOL_DELETE</td>
</tr>
<tr>
<td>ListConsoleHistories</td>
<td>CONSOLE_HISTORY_READ and INSTANCE_INSPECT</td>
</tr>
<tr>
<td>GetConsoleHistory</td>
<td>CONSOLE_HISTORY_READ and INSTANCE_INSPECT</td>
</tr>
<tr>
<td>ShowConsoleHistoryData</td>
<td>CONSOLE_HISTORY_READ and INSTANCE_READ and INSTANCE_IMAGE_READ</td>
</tr>
<tr>
<td>CaptureConsoleHistory</td>
<td>CONSOLE_HISTORY_CREATE and INSTANCE_READ and INSTANCE_IMAGE_READ</td>
</tr>
<tr>
<td>DeleteConsoleHistory</td>
<td>CONSOLE_HISTORY_DELETE</td>
</tr>
<tr>
<td>ListCpes</td>
<td>CPE_READ</td>
</tr>
<tr>
<td>GetCpe</td>
<td>CPE_READ</td>
</tr>
<tr>
<td>UpdateCpe</td>
<td>CPE_UPDATE</td>
</tr>
<tr>
<td>CreateCpe</td>
<td>CPE_CREATE</td>
</tr>
<tr>
<td>DeleteCpe</td>
<td>CPE_DELETE</td>
</tr>
<tr>
<td>ChangeCpeCompartment</td>
<td>CPE_RESOURCE_MOVE</td>
</tr>
<tr>
<td>UpdateTunnelCpeDeviceConfig</td>
<td>IPSEC_CONNECTION_MOVE</td>
</tr>
<tr>
<td>GetTunnelCpeDeviceConfig</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>GetTunnelCpeDeviceTemplateContent</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>GetCpeDeviceTemplateContent</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>GetIpsecCpeDeviceTemplateContent</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>ListCrossConnects</td>
<td>CROSS_CONNECT_READ</td>
</tr>
<tr>
<td>GetCrossConnect</td>
<td>CROSS_CONNECT_READ</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UpdateCrossConnect</td>
<td>CROSS_CONNECT_UPDATE</td>
</tr>
<tr>
<td>CreateCrossConnect</td>
<td>CROSS_CONNECT_CREATE if not creating cross-connect in a cross-connect group.</td>
</tr>
<tr>
<td></td>
<td>If creating the cross-connect in a cross-connect group, also need CROSS_CONNECT_CREATE and CROSS_CONNECT_ATTACH</td>
</tr>
<tr>
<td>DeleteCrossConnect</td>
<td>CROSS_CONNECT_DELETE if cross-connect is not in a cross-connect group.</td>
</tr>
<tr>
<td></td>
<td>If the cross-connect is in a cross-connect group, also need CROSS_CONNECT_DELETE and CROSS_CONNECT_DETACH</td>
</tr>
<tr>
<td>ChangeCrossConnectCompartment</td>
<td>CROSS_CONNECT_RESOURCE_MOVE</td>
</tr>
<tr>
<td>ListCrossConnectGroups</td>
<td>CROSS_CONNECT_GROUP_READ</td>
</tr>
<tr>
<td>GetCrossConnectGroup</td>
<td>CROSS_CONNECT_GROUP_READ</td>
</tr>
<tr>
<td>UpdateCrossConnectGroup</td>
<td>CROSS_CONNECT_GROUP_UPDATE</td>
</tr>
<tr>
<td>CreateCrossConnectGroup</td>
<td>CROSS_CONNECT_GROUP_CREATE</td>
</tr>
<tr>
<td>DeleteCrossConnectGroup</td>
<td>CROSS_CONNECT_GROUP_DELETE</td>
</tr>
<tr>
<td>ChangeCrossConnectGroupCompartment</td>
<td>CROSS_CONNECT_GROUP_RESOURCE_MOVE</td>
</tr>
<tr>
<td>ListDhcpOptions</td>
<td>DHCP_READ</td>
</tr>
<tr>
<td>GetDhcpOptions</td>
<td>DHCP_READ</td>
</tr>
<tr>
<td>UpdateDhcpOptions</td>
<td>DHCP_UPDATE</td>
</tr>
<tr>
<td>CreateDhcpOptions</td>
<td>DHCP_CREATE and VCN_ATTACH</td>
</tr>
<tr>
<td>DeleteDhcpOptions</td>
<td>DHCP_DELETE and VCN_DETACH</td>
</tr>
<tr>
<td>ChangeDhcpOptionsCompartment</td>
<td>DHCP_MOVE</td>
</tr>
<tr>
<td>ListDrgs</td>
<td>DRG_READ</td>
</tr>
<tr>
<td>GetDrg</td>
<td>DRG_READ</td>
</tr>
<tr>
<td>UpdateDrg</td>
<td>DRG_UPDATE</td>
</tr>
<tr>
<td>CreateDrg</td>
<td>DRG_CREATE</td>
</tr>
<tr>
<td>DeleteDrg</td>
<td>DRG_DELETE</td>
</tr>
<tr>
<td>ChangeDrgCompartment</td>
<td>DRG_MOVE</td>
</tr>
<tr>
<td>ListDrgAttachments</td>
<td>DRG_ATTACHMENT_READ</td>
</tr>
<tr>
<td>GetDrgAttachment</td>
<td>DRG_ATTACHMENT_READ</td>
</tr>
<tr>
<td>UpdateDrgAttachment</td>
<td>DRG_ATTACHMENT.UPDATE</td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_ATTACH is necessary to associate a route table with the DRG attachment during the update.</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>CreateDrgAttachment</td>
<td>DRG_ATTACH and VCN_ATTACH</td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_ATTACH is necessary to associate a route table with the DRG attachment during creation.</td>
</tr>
<tr>
<td>DeleteDrgAttachment</td>
<td>DRG_DETACH and VCN_DETACH</td>
</tr>
<tr>
<td>CreateInstanceConsoleConnection</td>
<td>INSTANCE_CONSOLE_CONNECTION_CREATE and INSTANCE_READ</td>
</tr>
<tr>
<td>DeleteInstanceConsoleConnection</td>
<td>INSTANCE_CONSOLE_CONNECTION_DELETE</td>
</tr>
<tr>
<td>GetInstanceConsoleConnection</td>
<td>INSTANCE_CONSOLE_CONNECTION_READ and INSTANCE_READ</td>
</tr>
<tr>
<td>UpdateInstanceConsoleConnection</td>
<td>INSTANCE_CONSOLE_CONNECTION_CREATE and INSTANCE_CONSOLE_CONNECTION_DELETE</td>
</tr>
<tr>
<td>ListInstanceConsoleConnections</td>
<td>INSTANCE_CONSOLE_CONNECTION_INSPECT and INSTANCE_INSPECT and INSTANCE_READ</td>
</tr>
<tr>
<td>ListImages</td>
<td>INSTANCE_IMAGE_READ</td>
</tr>
<tr>
<td>GetImage</td>
<td>INSTANCE_IMAGE_READ</td>
</tr>
<tr>
<td>UpdateImage</td>
<td>INSTANCE_IMAGE_UPDATE</td>
</tr>
<tr>
<td>CreateImage</td>
<td>INSTANCE_IMAGE_CREATE and INSTANCE_CREATE_IMAGE</td>
</tr>
<tr>
<td></td>
<td>The first permission is related to the instance-image; the second is related to the instance.</td>
</tr>
<tr>
<td>ChangeImageCompartment</td>
<td>INSTANCE_IMAGE_MOVE</td>
</tr>
<tr>
<td>DeleteImage</td>
<td>INSTANCE_IMAGE_DELETE</td>
</tr>
<tr>
<td>ListInstances</td>
<td>INSTANCE_READ</td>
</tr>
<tr>
<td>GetInstance</td>
<td>INSTANCE_READ</td>
</tr>
<tr>
<td>LaunchInstance</td>
<td>INSTANCE_CREATE and INSTANCE_IMAGE_READ and VNIC_CREATE and VNIC_ATTACH and SUBNET_ATTACH</td>
</tr>
<tr>
<td></td>
<td>If putting the instance in a network security group during instance creation, also need NETWORK_SECURITY_GROUP_UPDATE_MEMBERS and VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP</td>
</tr>
<tr>
<td>UpdateInstance</td>
<td>INSTANCE_UPDATE</td>
</tr>
<tr>
<td>InstanceAction</td>
<td>INSTANCE_POWER_ACTIONS</td>
</tr>
<tr>
<td>ChangeInstanceCompartment</td>
<td>INSTANCE_MOVE</td>
</tr>
<tr>
<td>TerminateInstance</td>
<td>INSTANCE_DELETE and VNIC_DELETE and SUBNET_DETACH</td>
</tr>
<tr>
<td>ListInstanceConfigurations</td>
<td>INSTANCE_CONFIGURATION_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>GetInstanceConfiguration</td>
<td>INSTANCE_CONFIGURATION_READ</td>
</tr>
<tr>
<td>LaunchInstanceConfiguration</td>
<td>INSTANCE_CONFIGURATION_LAUNCH</td>
</tr>
<tr>
<td>UpdateInstanceConfiguration</td>
<td>INSTANCE_CONFIGURATION_UPDATE</td>
</tr>
<tr>
<td>CreateInstanceConfiguration</td>
<td>INSTANCE_CONFIGURATION_CREATE (if using the CreateInstanceConfigurationDetails subtype)</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_READ and VNIC_READ and VNIC_ATTACHMENT_READ and VOLUME_INSPECT and VOLUME_ATTACHMENT_INSPECT (if using the CreateInstanceConfigurationFromInstanceDetails subtype)</td>
</tr>
<tr>
<td>ChangeInstanceConfigurationCompartment</td>
<td>INSTANCE_CONFIGURATION_MOVE</td>
</tr>
<tr>
<td>DeleteInstanceConfiguration</td>
<td>INSTANCE_CONFIGURATION_DELETE</td>
</tr>
<tr>
<td>ListInstancePools</td>
<td>INSTANCE_POOL_INSPECT</td>
</tr>
<tr>
<td>ListInstancePoolInstances</td>
<td>INSTANCE_POOL_READ</td>
</tr>
<tr>
<td>GetInstancePool</td>
<td>INSTANCE_POOL_READ</td>
</tr>
<tr>
<td>UpdateInstancePool</td>
<td>INSTANCE_POOL_UPDATE</td>
</tr>
<tr>
<td>ResetInstancePool</td>
<td>INSTANCE_POOL_POWER_ACTIONS</td>
</tr>
<tr>
<td>SoftresetInstancePool</td>
<td>INSTANCE_POOL_POWER_ACTIONS</td>
</tr>
<tr>
<td>StartInstancePool</td>
<td>INSTANCE_POOL_POWER_ACTIONS</td>
</tr>
<tr>
<td>StopInstancePool</td>
<td>INSTANCE_POOL_POWER_ACTIONS</td>
</tr>
<tr>
<td>CreateInstancePool</td>
<td>INSTANCE_POOL_CREATE and INSTANCE_CREATE and IMAGE_READ and VNIC_CREATE and SUBNET_ATTACH</td>
</tr>
<tr>
<td>ChangeInstancePoolCompartment</td>
<td>INSTANCE_POOL_MOVE</td>
</tr>
<tr>
<td>TerminateInstancePool</td>
<td>INSTANCE_POOL_DELETE and INSTANCE_DELETE and VNIC_DELETE and SUBNET_DETACH and VOLUME_ATTACHMENT_DELETE and VOLUME_WRITE</td>
</tr>
<tr>
<td>ListInternetGateways</td>
<td>INTERNET_GATEWAY_READ</td>
</tr>
<tr>
<td>GetInternetGateway</td>
<td>INTERNET_GATEWAY_READ</td>
</tr>
<tr>
<td>UpdateInternetGateway</td>
<td>INTERNET_GATEWAY_UPDATE</td>
</tr>
<tr>
<td>CreateInternetGateway</td>
<td>INTERNET_GATEWAY_CREATE and VCN_ATTACH</td>
</tr>
<tr>
<td>DeleteInternetGateway</td>
<td>INTERNET_GATEWAY_DELETE and VCN_DETACH</td>
</tr>
<tr>
<td>ChangeInternetGatewayCompartment</td>
<td>INTERNET_GATEWAY_MOVE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>ListIPSecConnections</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>GetIPSecConnection</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>UpdateIpSecConnection</td>
<td>IPSEC_CONNECTION_UPDATE</td>
</tr>
<tr>
<td>CreateIPSecConnection</td>
<td>DRG_ATTACH and CPE_ATTACH and</td>
</tr>
<tr>
<td></td>
<td>IPSEC_CONNECTION_CREATE</td>
</tr>
<tr>
<td>DeleteIPSecConnection</td>
<td>DRG_DETACH and CPE_DETACH and</td>
</tr>
<tr>
<td></td>
<td>IPSEC_CONNECTION_DELETE</td>
</tr>
<tr>
<td>GetIPSecConnectionDeviceConfig</td>
<td>IPSEC_CONNECTION_DEVICE_CONFIG_READ</td>
</tr>
<tr>
<td>GetIPSecConnectionDeviceStatus</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>ListIPSecConnectionTunnels</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>GetIPSecConnectionTunnel</td>
<td>IPSEC_CONNECTION_READ</td>
</tr>
<tr>
<td>UpdateIPSecConnectionTunnel</td>
<td>IPSEC_CONNECTION_UPDATE</td>
</tr>
<tr>
<td>GetIPSecConnectionTunnelSharedSecret</td>
<td>IPSEC_CONNECTION_DEVICE_CONFIG_READ</td>
</tr>
<tr>
<td>UpdateIPSecConnectionTunnelSharedSecret</td>
<td>IPSEC_CONNECTION_DEVICE_CONFIG_UPDATE</td>
</tr>
<tr>
<td>ListIpv6s</td>
<td>IPV6_READ and SUBNET_READ (if listing by subnet) and VNIC_READ (if listing by VNIC)</td>
</tr>
<tr>
<td>GetIpv6</td>
<td>IPV6_READ</td>
</tr>
<tr>
<td>UpdateIpv6</td>
<td>IPV6_UPDATE and VNIC_UNASSIGN and VNIC_ASSIGN (if moving IPv6 to a different VNIC)</td>
</tr>
<tr>
<td>CreateIpv6</td>
<td>IPV6_CREATE and SUBNET_ATTACH and VNIC_ASSIGN</td>
</tr>
<tr>
<td>DeleteIpv6</td>
<td>IPV6_DELETE and SUBNET_DETACH and VNIC_UNASSIGN</td>
</tr>
<tr>
<td>ListLocalPeeringGateways</td>
<td>LOCAL_PEERING_GATEWAY_READ</td>
</tr>
<tr>
<td>GetLocalPeeringGateway</td>
<td>LOCAL_PEERING_GATEWAY_READ</td>
</tr>
<tr>
<td>UpdateLocalPeeringGateway</td>
<td>LOCAL_PEERING_GATEWAY_UPDATE</td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_ATTACH is necessary to associate a route table with the LPG during the update.</td>
</tr>
<tr>
<td>CreateLocalPeeringGateway</td>
<td>LOCAL_PEERING_GATEWAY_CREATE and VCN_ATTACH</td>
</tr>
<tr>
<td></td>
<td>ROUTE_TABLE_ATTACH is necessary to associate a route table with the LPG during creation.</td>
</tr>
<tr>
<td>DeleteLocalPeeringGateway</td>
<td>LOCAL_PEERING_GATEWAY_DELETE and VCN_DETACH</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConnectLocalPeeringGateway</td>
<td>LOCAL_PEERING_GATEWAY_CONNECT_FROM and LOCAL_PEERING_GATEWAY_CONNECT_TO</td>
</tr>
<tr>
<td>ChangeLocalPeeringGatewayCompartment</td>
<td>LOCAL_PEERING_GATEWAY_MOVE</td>
</tr>
<tr>
<td>ListNatGateways</td>
<td>NAT_GATEWAY_READ</td>
</tr>
<tr>
<td>GetNatGateway</td>
<td>NAT_GATEWAY_READ</td>
</tr>
<tr>
<td>UpdateNatGateway</td>
<td>NAT_GATEWAY_UPDATE</td>
</tr>
<tr>
<td>CreateNatGateway</td>
<td>NAT_GATEWAY_CREATE and VCN_READ and VCN_ATTACH</td>
</tr>
<tr>
<td>DeleteNatGateway</td>
<td>NAT_GATEWAY_DELETE and VCN_READ and VCN_DETACH</td>
</tr>
<tr>
<td>ChangeNatGatewayCompartment</td>
<td>NAT_GATEWAY_MOVE</td>
</tr>
<tr>
<td>ListNetworkSecurityGroups</td>
<td>NETWORK_SECURITY_GROUP_READ</td>
</tr>
<tr>
<td>GetNetworkSecurityGroup</td>
<td>NETWORK_SECURITY_GROUP_READ</td>
</tr>
<tr>
<td>UpdateNetworkSecurityGroup</td>
<td>NETWORK_SECURITY_GROUP_UPDATE</td>
</tr>
<tr>
<td>CreateNetworkSecurityGroup</td>
<td>NETWORK_SECURITY_GROUP_CREATE and VCN_ATTACH</td>
</tr>
<tr>
<td>DeleteNetworkSecurityGroup</td>
<td>NETWORK_SECURITY_GROUP_DELETE and VCN_DETACH</td>
</tr>
<tr>
<td>ChangeNetworkSecurityGroupCompartment</td>
<td>NETWORK_SECURITY_GROUP_MOVE</td>
</tr>
<tr>
<td>ListNetworkSecurityGroupSecurityRules</td>
<td>NETWORK_SECURITY_GROUP_LIST_SECURITY_RULES</td>
</tr>
<tr>
<td>UpdateNetworkSecurityGroupSecurityRules</td>
<td>NETWORK_SECURITY_GROUP_UPDATE_SECURITY_RULES and NETWORK_SECURITY_GROUP_INSPECT if writing a rule that specifies a network security group as the source (for ingress rules) or destination (for egress rules)</td>
</tr>
<tr>
<td>AddNetworkSecurityGroupSecurityRules</td>
<td>NETWORK_SECURITY_GROUP_UPDATE_SECURITY_RULES and NETWORK_SECURITY_GROUP_INSPECT if writing a rule that specifies a network security group as the source (for ingress rules) or destination (for egress rules)</td>
</tr>
<tr>
<td>RemoveNetworkSecurityGroupSecurityRules</td>
<td>NETWORK_SECURITY_GROUP_UPDATE_SECURITY_RULES</td>
</tr>
<tr>
<td>ListPrivateIps</td>
<td>PRIVATE_IP_READ</td>
</tr>
<tr>
<td>GetPrivateIp</td>
<td>PRIVATE_IP_READ</td>
</tr>
<tr>
<td>UpdatePrivateIp</td>
<td>PRIVATE_IP_UPDATE and VNIC_ASSIGN and VNIC_UNASSIGN</td>
</tr>
<tr>
<td>CreatePrivateIp</td>
<td>PRIVATE_IP_CREATE and PRIVATE_IP_ASSIGN and VNIC_ASSIGN and SUBNET_ATTACH</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DeletePrivateIp</td>
<td>PRIVATE_IP_DELETE and PRIVATE_IP_UNASSIGN and VNIC_UNASSIGN and SUBNET_DETACH</td>
</tr>
<tr>
<td>ListRemotePeeringConnections</td>
<td>REMOTE_PEERING_CONNECTION_READ</td>
</tr>
<tr>
<td>GetRemotePeeringConnection</td>
<td>REMOTE_PEERING_CONNECTION_READ</td>
</tr>
<tr>
<td>UpdateRemotePeeringConnection</td>
<td>REMOTE_PEERING_CONNECTION_UPDATE</td>
</tr>
<tr>
<td>CreateRemotePeeringConnection</td>
<td>REMOTE_PEERING_CONNECTION_CREATE and DRG_ATTACH</td>
</tr>
<tr>
<td>DeleteRemotePeeringConnection</td>
<td>REMOTE_PEERING_CONNECTION_DELETE and DRG_DETACH</td>
</tr>
<tr>
<td>ChangeRemotePeeringConnectionCompartment</td>
<td>REMOTE_PEERING_CONNECTION_RESOURCE_MOVE and REMOTE_PEERING_CONNECTION_CONNECT_FROM and REMOTE_PEERING_CONNECTION_CONNECT_TO</td>
</tr>
<tr>
<td>ConnectRemotePeeringConnections</td>
<td></td>
</tr>
<tr>
<td>ListPublicIps</td>
<td>For ephemeral public IPs: PRIVATE_IP_READ</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_READ</td>
</tr>
<tr>
<td>GetPublicIp</td>
<td>For ephemeral public IPs: PRIVATE_IP_READ</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_READ</td>
</tr>
<tr>
<td>GetPublicIpByPrivateIpId</td>
<td>For ephemeral public IPs: PRIVATE_IP_READ</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_READ</td>
</tr>
<tr>
<td>GetPublicIpByIpAddress</td>
<td>For ephemeral public IPs: PRIVATE_IP_READ</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_READ</td>
</tr>
<tr>
<td>UpdatePublicIP</td>
<td>For ephemeral public IPs: PRIVATE_IP_UPDATE</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_UPDATE and PRIVATE_IP_ASSIGN_PUBLIC_IP and PUBLIC_IP_ASSIGN_PRIVATE_IP and PRIVATE_IP_UNASSIGN_PUBLIC_IP and PUBLIC_IP_UNASSIGN_PRIVATE_IP</td>
</tr>
<tr>
<td>CreatePublicIp</td>
<td>For ephemeral public IPs: PRIVATE_IP_ASSIGN_PUBLIC_IP</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_CREATE and PUBLIC_IP_ASSIGN_PRIVATE_IP and PRIVATE_IP_ASSIGN_PUBLIC_IP</td>
</tr>
<tr>
<td>DeletePublicIp</td>
<td>For ephemeral public IPs: PRIVATE_IP_UNASSIGN_PUBLIC_IP</td>
</tr>
<tr>
<td></td>
<td>For reserved public IPs: PUBLIC_IP_DELETE and PUBLIC_IP_UNASSIGN_PRIVATE_IP and PRIVATE_IP_UNASSIGN_PUBLIC_IP</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>ChangePublicIpCompartment</td>
<td>PUBLIC_IP_MOVE</td>
</tr>
<tr>
<td></td>
<td>Note: This operation applies only to reserved public IPs.</td>
</tr>
<tr>
<td>ListRouteTables</td>
<td>ROUTE_TABLE_READ</td>
</tr>
<tr>
<td>GetRouteTable</td>
<td>ROUTE_TABLE_READ</td>
</tr>
<tr>
<td>UpdateRouteTable</td>
<td>ROUTE_TABLE_UPDATE and</td>
</tr>
<tr>
<td></td>
<td>INTERNET_GATEWAY_ATTACH (if creating a route rule that uses an internet gateway as a target) and</td>
</tr>
<tr>
<td></td>
<td>INTERNET_GATEWAY_DETACH (if deleting a route rule that uses an internet gateway as a target) and</td>
</tr>
<tr>
<td></td>
<td>DRG_ATTACH (if creating a route rule that uses a DRG as a target) and</td>
</tr>
<tr>
<td></td>
<td>DRG_DETACH (if deleting a route rule that uses a DRG as a target) and</td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_ROUTE_TABLE_ATTACH (if creating a route rule that uses a private IP as a target) and</td>
</tr>
<tr>
<td></td>
<td>PRIVATE_IP_ROUTE_TABLE_DETACH (if deleting a route rule that uses a private IP as a target) and</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_ATTACH (if creating a route rule that uses an LPG as a target) and</td>
</tr>
<tr>
<td></td>
<td>LOCAL_PEERING_GATEWAY_DETACH (if deleting a route rule that uses an LPG as a target) and</td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_ATTACH (if creating a route rule that uses a NAT gateway as a target) and</td>
</tr>
<tr>
<td></td>
<td>NAT_GATEWAY_DETACH (if deleting a route rule that uses a NAT gateway as a target) and</td>
</tr>
<tr>
<td></td>
<td>SERVICE_GATEWAY_ATTACH (if creating a route rule that uses a service gateway as a target) and</td>
</tr>
<tr>
<td></td>
<td>SERVICE_GATEWAY_DETACH (if deleting a route rule that uses a service gateway as a target)</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CreateRouteTable</td>
<td>ROUTE_TABLE_CREATE and VCN_ATTACH and INTERNET_GATEWAY_ATTACH (if creating a route rule that uses an internet gateway as a target) and DRG_ATTACH (if creating a route rule that uses a DRG as a target) and PRIVATE_IP_ROUTE_TABLE_ATTACH (if creating a route rule that uses a private IP as a target) and LOCAL_PEERING_GATEWAY_ATTACH (if creating a route rule that uses an LPG as a target) and NAT_GATEWAY_ATTACH (if creating a route rule that uses a NAT gateway as a target) and SERVICE_GATEWAY_ATTACH (if creating a route rule that uses a service gateway as a target)</td>
</tr>
<tr>
<td>DeleteRouteTable</td>
<td>ROUTE_TABLE_DELETE and VCN_DETACH and INTERNET_GATEWAY_DETACH (if deleting a route rule that uses an internet gateway as a target) and DRG_DETACH (if deleting a route rule that uses a DRG as a target) and PRIVATE_IP_ROUTE_TABLE_DETACH (if deleting a route rule that uses a private IP as a target) and LOCAL_PEERING_GATEWAY_DETACH (if deleting a route rule that uses an LPG as a target) and NAT_GATEWAY_DETACH (if deleting a route rule that uses a NAT gateway as a target) and SERVICE_GATEWAY_DETACH (if deleting a route rule that uses a service gateway as a target)</td>
</tr>
<tr>
<td>ChangeRouteTableCompartment</td>
<td>ROUTE_TABLE_MOVE</td>
</tr>
<tr>
<td>ListSecurityLists</td>
<td>SECURITY_LIST_READ</td>
</tr>
<tr>
<td>GetSecurityList</td>
<td>SECURITY_LIST_READ</td>
</tr>
<tr>
<td>UpdateSecurityList</td>
<td>SECURITY_LIST_UPDATE</td>
</tr>
<tr>
<td>ChangeSecurityListCompartment</td>
<td>SECURITY_LIST_MOVE</td>
</tr>
<tr>
<td>CreateSecurityList</td>
<td>SECURITY_LIST_CREATE and VCN_ATTACH</td>
</tr>
<tr>
<td>DeleteSecurityList</td>
<td>SECURITY_LIST_DELETE and VCN_DETACH</td>
</tr>
<tr>
<td>ListServiceGateways</td>
<td>SERVICE_GATEWAY_READ</td>
</tr>
<tr>
<td>GetServiceGateway</td>
<td>SERVICE_GATEWAY_READ</td>
</tr>
<tr>
<td>UpdateServiceGateway</td>
<td>SERVICE_GATEWAY_UPDATE</td>
</tr>
<tr>
<td>ChangeServiceGatewayCompartment</td>
<td>SERVICE_GATEWAY_MOVE</td>
</tr>
</tbody>
</table>

ROUTE_TABLE_ATTACH is necessary to associate a route table with the service gateway during the update.
<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
</table>
| CreateServiceGateway    | SERVICE_GATEWAY_CREATE and VCN_READ and VCN_ATTACH
ROUTE_TABLE_ATTACH is necessary to associate a route table with the service gateway during creation.                                                                                                                                 |
| DeleteServiceGateway    | SERVICE_GATEWAY_DELETE and VCN_READ and VCN_DETACH                                                                                                                                                                                        |
| AttachServiceId         | SERVICE_GATEWAY_ADD_SERVICE                                                                                                                                                                                                               |
| DetachServiceId         | SERVICE_GATEWAY_DELETE_SERVICE                                                                                                                                                                                                            |
| ListShapes              | INSTANCE_INSPECT                                                                                                                                                                                                                         |
| ListSubnets             | SUBNET_READ                                                                                                                                                                                                                              |
| GetSubnet               | SUBNET_READ                                                                                                                                                                                                                                |
| UpdateSubnet            | SUBNET_UPDATE
If changing which route table is associated with the subnet, also need ROUTE_TABLE_ATTACH and ROUTE_TABLE_DETACH
If changing which security lists are associated with the subnet, also need SECURITY_LIST_ATTACH and SECURITY_LIST_DETACH
If changing which set of DHCP options are associated with the subnet, also need DHCP_ATTACH and DHCP_DETACH |
<p>| CreateSubnet            | SUBNET_CREATE and VCN_ATTACH and ROUTE_TABLE_ATTACH and SECURITY_LIST_ATTACH and DHCP_ATTACH                                                                                                                                              |
| DeleteSubnet            | SUBNET_DELETE and VCN_DETACH and ROUTE_TABLE_DETACH and SECURITY_LIST_DETACH and DHCP_DETACH                                                                                                                                              |
| ChangeSubnetCompartment | SUBNET_MOVE                                                                                                                                                                                                                                |
| ListVcns                | VCN_READ                                                                                                                                                                                                                                  |
| GetVcn                  | VCN_READ                                                                                                                                                                                                                                  |
| UpdateVcn               | VCN_UPDATE                                                                                                                                                                                                                                |
| CreateVcn               | VCN_CREATE                                                                                                                                                                                                                                |
| DeleteVcn               | VCN_DELETE                                                                                                                                                                                                                                |
| AddVcnCidr              | VCN_UPDATE                                                                                                                                                                                                                                |
| ModifyVcnCidr           | VCN_UPDATE                                                                                                                                                                                                                                |
| RemoveVcnCidr           | VCN_UPDATE                                                                                                                                                                                                                                |
| ChangeVcnCompartment    | VCN_MOVE                                                                                                                                                                                                                                |
| ListVirtualCircuits     | VIRTUAL_CIRCUIT_READ                                                                                                                                                                                                                      |
| GetVirtualCircuit       | VIRTUAL_CIRCUIT_READ                                                                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdateVirtualCircuit</td>
<td>VIRTUAL_CIRCUIT_UPDATE and DRG_ATTACH and DRG_DETACH&lt;br&gt;If updating which cross-connect or cross-connect group the virtual circuit is using, also need CROSS_CONNECT_DETACH and CROSS_CONNECT_ATTACH</td>
</tr>
<tr>
<td>CreateVirtualCircuit</td>
<td>VIRTUAL_CIRCUIT_CREATE and DRG_ATTACH&lt;br&gt;If creating the virtual circuit with a mapping to a specific cross-connect or cross-connect group, also need CROSS_CONNECT_ATTACH</td>
</tr>
<tr>
<td>DeleteVirtualCircuit</td>
<td>VIRTUAL_CIRCUIT_DELETE and DRG_DETACH&lt;br&gt;If deleting a virtual circuit that's currently using a cross-connect or cross-connect group, also need CROSS_CONNECT_DETACH</td>
</tr>
<tr>
<td>changeVirtualCircuitCompartment</td>
<td>VIRTUAL_CIRCUIT_RESOURCE_MOVE</td>
</tr>
<tr>
<td>ListVlans</td>
<td>VLAN_READ</td>
</tr>
<tr>
<td>GetVlan</td>
<td>VLAN_READ</td>
</tr>
<tr>
<td>CreateVlan</td>
<td>VLAN_CREATE and VCN_ATTACH and ROUTE_TABLE_ATTACH and SECURITY_LIST_ATTACH and VLAN_ASSOCIATE_NETWORK_SECURITY_GROUP</td>
</tr>
<tr>
<td>UpdateVlan</td>
<td>VLAN_UPDATE</td>
</tr>
<tr>
<td>DeleteVlan</td>
<td>VLAN_DELETE and VCN_DETACH and ROUTE_TABLE_DETACH and SECURITY_LIST_DETACH and VLAN_DISASSOCIATE_NETWORK_SECURITY_GROUP</td>
</tr>
<tr>
<td>ChangeVlanCompartment</td>
<td>VLAN_MOVE</td>
</tr>
<tr>
<td>GetVnic</td>
<td>VNIC_READ</td>
</tr>
<tr>
<td>AttachVnic</td>
<td>INSTANCE_ATTACHMENT_SECONDARY_VNIC and VNIC_ATTACH and VNIC_CREATE and SUBNET_ATTACH&lt;br&gt;If putting the secondary VNIC in a network security group during VNIC creation, also need NETWORK_SECURITY_GROUP_UPDATE_MEMBERS and VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP</td>
</tr>
<tr>
<td>DetachVnic</td>
<td>INSTANCE_DETACH_SECONDARY_VNIC and VNIC_DETACH and VNIC_DELETE and SUBNET_DETACH</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| UpdateVnic                    | VNIC_UPDATE  
If adding or removing the VNIC from  
a network security group, also need  
NETWORK_SECURITY_GROUP_UPDATE_MEMBERS  
and VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP |
| ListVnicAttachments           | VNIC_ATTACHMENT_READ and INSTANCE_INSPECT                                                                |
| GetVnicAttachment             | VNIC_ATTACHMENT_READ                                                                                      |
| ListVolumes                   | VOLUME_INSPECT                                                                                           |
| GetVolume                     | VOLUME_INSPECT                                                                                           |
| UpdateVolume                  | VOLUME_UPDATE                                                                                           |
| CreateVolume                  | VOLUME_CREATE (and VOLUME_BACKUP_READ if creating volume from a backup)                                    |
| DeleteVolume                  | VOLUME_DELETE                                                                                           |
| ChangeVolumeCompartment       | VOLUME_MOVE                                                                                              |
| ListVolumeAttachments         | VOLUME_ATTACHMENT_INSPECT and VOLUME_INSPECT and INSTANCE_INSPECT                                          |
| GetVolumeAttachment           | VOLUME_ATTACHMENT_INSPECT and VOLUME_INSPECT and INSTANCE_INSPECT  
**Note:** To also get the CHAP secret for the volume, then VOLUME_ATTACHMENT_READ is required instead of VOLUME_ATTACHMENT_INSPECT |
<p>| AttachVolume                  | VOLUME_ATTACHMENT_CREATE and VOLUME_WRITE and INSTANCE_ATTACH_VOLUME                                        |
| DetachVolume                  | VOLUME_ATTACHMENT_DELETE and VOLUME_WRITE and INSTANCE_DETACH_VOLUME                                        |
| ListVolumeBackups             | VOLUME_BACKUP_INSPECT and VOLUME_INSPECT                                                                  |
| GetVolumeBackup               | VOLUME_BACKUP_INSPECT and VOLUME_INSPECT                                                                  |
| UpdateVolumeBackup            | VOLUME_BACKUP_UPDATE and VOLUME_INSPECT                                                                   |
| CreateVolumeBackup            | VOLUME_BACKUP_CREATE and VOLUME_WRITE                                                                     |
| DeleteVolumeBackup            | VOLUME_BACKUP_DELETE and VOLUME_INSPECT                                                                   |
| ChangeVolumeBackupCompartment | VOLUME_BACKUP_MOVE                                                                                         |</p>
<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetBootVolume</td>
<td>VOLUME_INSPECT</td>
</tr>
<tr>
<td>ListBootVolumes</td>
<td>VOLUME_INSPECT</td>
</tr>
<tr>
<td>UpdateBootVolume</td>
<td>VOLUME_UPDATE</td>
</tr>
<tr>
<td>DeleteBootVolume</td>
<td>VOLUME_DELETE</td>
</tr>
<tr>
<td>ChangeBootVolumeCompartment</td>
<td>BOOT_VOLUME_MOVE</td>
</tr>
<tr>
<td>CreateBootVolumeBackup</td>
<td>BOOT_VOLUME_BACKUP_CREATE, VOLUME_WRITE</td>
</tr>
<tr>
<td>ListBootVolumeBackups</td>
<td>BOOT_VOLUME_BACKUP_INSPECT, VOLUME_INSPECT</td>
</tr>
<tr>
<td>GetBootVolumeBackup</td>
<td>BOOT_VOLUME_BACKUP_INSPECT, VOLUME_INSPECT</td>
</tr>
<tr>
<td>UpdateBootVolumeBackup</td>
<td>BOOT_VOLUME_BACKUP_UPDATE, VOLUME_INSPECT</td>
</tr>
<tr>
<td>DeleteBootVolumeBackup</td>
<td>BOOT_VOLUME_BACKUP_DELETE, VOLUME_INSPECT</td>
</tr>
<tr>
<td>ChangeBootVolumeBackupCompartment</td>
<td>BOOT_VOLUME_BACKUP_MOVE</td>
</tr>
<tr>
<td>CreateVolumeGroup</td>
<td>VOLUME_GROUP_CREATE, VOLUME_INSPECT if creating the volume group from a list of volumes.</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_CREATE, VOLUME_GROUP_INSPECT, VOLUME_CREATE, VOLUME_WRITE if cloning a volume group.</td>
</tr>
<tr>
<td></td>
<td>VOLUME_GROUP_CREATE, VOLUME_GROUP_BACKUP_INSPECT, VOLUME_BACKUP_READ/BOOT_VOLUME_BACKUP_READ,</td>
</tr>
<tr>
<td></td>
<td>VOLUME_CREATE, VOLUME_WRITE if restoring from a volume group backup.</td>
</tr>
<tr>
<td>DeleteVolumeGroup</td>
<td>VOLUME_GROUP_DELETE</td>
</tr>
<tr>
<td>GetVolumeGroup</td>
<td>VOLUME_GROUP_INSPECT</td>
</tr>
<tr>
<td>ListVolumeGroups</td>
<td>VOLUME_GROUP_INSPECT</td>
</tr>
<tr>
<td>UpdateVolumeGroup</td>
<td>VOLUME_GROUP_UPDATE, VOLUME_INSPECT</td>
</tr>
<tr>
<td>ChangeVolumeGroupCompartment</td>
<td>VOLUME_GROUP_MOVE, VOLUME_MOVE/BOOT_VOLUME_MOVE</td>
</tr>
<tr>
<td>CreateVolumeGroupBackup</td>
<td>VOLUME_GROUP_BACKUP_CREATE, VOLUME_GROUP_INSPECT, VOLUME_WRITE, VOLUME_BACKUP_CREATE/BOOT_VOLUME_BACKUP_CREATE</td>
</tr>
<tr>
<td>DeleteVolumeGroupBackup</td>
<td>VOLUME_GROUP_BACKUP_DELETE, VOLUME_BACKUP_DELETE/BOOT_VOLUME_BACKUP_DELETE</td>
</tr>
<tr>
<td>GetVolumeGroupBackup</td>
<td>VOLUME_GROUP_BACKUP_INSPECT</td>
</tr>
</tbody>
</table>
### IAM API Operation Permissions

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListVolumeGroupBackups</td>
<td>VOLUME_GROUP_BACKUP_INSPECT</td>
</tr>
<tr>
<td>UpdateVolumeGroupBackup</td>
<td>VOLUME_GROUP_BACKUP_UPDATE</td>
</tr>
<tr>
<td>ChangeVolumeGroupBackupCompartment</td>
<td>VOLUME_GROUP_BACKUP_MOVE, VOLUME_BACKUP_MOVE/BOOT_VOLUME_BACKUP_MOVE</td>
</tr>
</tbody>
</table>

### Dedicated Virtual Machine Host API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateDedicatedVmHost</td>
<td>DEDICATED_VM_HOST_CREATE</td>
</tr>
<tr>
<td>ChangeDedicatedVmHostCompartment</td>
<td>DEDICATED_VM_HOST_MOVE</td>
</tr>
<tr>
<td>DeleteDedicatedVmHost</td>
<td>DEDICATED_VM_HOST_DELETE</td>
</tr>
<tr>
<td>GetDedicatedVmHost</td>
<td>DEDICATED_VM_HOST_READ</td>
</tr>
<tr>
<td>ListDedicatedVmHosts</td>
<td>DEDICATED_VM_HOST_READ</td>
</tr>
<tr>
<td>ListDedicatedVmHostInstances</td>
<td>DEDICATED_VM_HOST_READ</td>
</tr>
<tr>
<td>ListDedicatedVmHostInstanceShapes</td>
<td>None</td>
</tr>
<tr>
<td>ListDedicatedVmHostShapes</td>
<td>None</td>
</tr>
<tr>
<td>LaunchInstance</td>
<td>DEDICATED_VM_HOST_LAUNCH_INSTANCE in dedicated virtual machine host compartment</td>
</tr>
<tr>
<td></td>
<td>INSTANCE_CREATE in compartment for the instance launched on the dedicated virtual machine host</td>
</tr>
<tr>
<td>UpdateDedicatedVmHost</td>
<td>AUTO_SCALING_CONFIGURATION_CREATE and INSTANCE_POOL_UPDATE</td>
</tr>
</tbody>
</table>

### Autoscaling API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListAutoScalingConfigurations</td>
<td>AUTO_SCALING_CONFIGURATION_INSPECT</td>
</tr>
<tr>
<td>GetAutoScalingConfiguration</td>
<td>AUTO_SCALING_CONFIGURATION_READ</td>
</tr>
<tr>
<td>UpdateAutoScalingConfiguration</td>
<td>AUTO_SCALING_CONFIGURATION_UPDATE and INSTANCE_POOL_UPDATE</td>
</tr>
<tr>
<td>CreateAutoScalingConfiguration</td>
<td>AUTO_SCALING_CONFIGURATION_CREATE and INSTANCE_POOL_UPDATE</td>
</tr>
<tr>
<td>ChangeAutoScalingConfigurationCompartment</td>
<td>AUTO_SCALING_CONFIGURATION_MOVE</td>
</tr>
<tr>
<td>DeleteAutoScalingConfiguration</td>
<td>AUTO_SCALING_CONFIGURATION_DELETE and INSTANCE_POOL_UPDATE</td>
</tr>
<tr>
<td>ListAutoScalingPolicies</td>
<td>AUTO_SCALING_CONFIGURATION_READ</td>
</tr>
<tr>
<td>GetAutoScalingPolicy</td>
<td>AUTO_SCALING_CONFIGURATION_READ</td>
</tr>
<tr>
<td>UpdateAutoScalingPolicy</td>
<td>AUTO_SCALING_CONFIGURATION_UPDATE and INSTANCE_POOL_UPDATE</td>
</tr>
</tbody>
</table>
### API Operation Permissions Required to Use the Operation

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateAutoScalingPolicy</td>
<td>AUTO_SCALING_CONFIGURATION_CREATE and INSTANCE_POOL_UPDATE</td>
</tr>
<tr>
<td>DeleteAutoScalingPolicy</td>
<td>AUTO_SCALING_CONFIGURATION_DELETE and INSTANCE_POOL_UPDATE</td>
</tr>
</tbody>
</table>

### Oracle Cloud Agent API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateInstanceAgentCommand</td>
<td>INSTANCE_AGENT_COMMAND_CREATE</td>
</tr>
<tr>
<td>GetInstanceAgentCommand</td>
<td>INSTANCE_AGENT_COMMAND_READ</td>
</tr>
<tr>
<td>GetInstanceAgentCommandExecution</td>
<td>INSTANCE_AGENT_COMMAND_EXECUTION_INSPECT</td>
</tr>
<tr>
<td>ListInstanceAgentCommands</td>
<td>INSTANCE_AGENT_COMMAND_INSPECT</td>
</tr>
<tr>
<td>ListInstanceAgentCommandExecutions</td>
<td>INSTANCE_AGENT_COMMAND_EXECUTION_INSPECT</td>
</tr>
<tr>
<td>CancelInstanceAgentCommand</td>
<td>INSTANCE_AGENT_COMMAND_DELETE</td>
</tr>
<tr>
<td>GetInstanceAgentPlugin</td>
<td>INSTANCE_AGENT_PLUGIN_READ</td>
</tr>
<tr>
<td>ListInstanceAgentPlugins</td>
<td>INSTANCE_AGENT_PLUGIN_INSPECT</td>
</tr>
<tr>
<td>ListInstanceAgentAvailablePlugins</td>
<td>INSTANCE_AGENT_PLUGIN_INSPECT</td>
</tr>
</tbody>
</table>

### Work Requests API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListWorkRequests</td>
<td>WORKREQUEST_INSPECT</td>
</tr>
<tr>
<td>GetWorkRequests</td>
<td>Work requests inherit the permissions of the operation that spawns the work request. Generally, <code>&lt;RESOURCE&gt;_CREATE</code> permissions for the associated resource are required.</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>Work requests inherit the permissions of the operation that spawns the work request. Generally, <code>&lt;RESOURCE&gt;_CREATE</code> permissions for the associated resource are required.</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>Work requests inherit the permissions of the operation that spawns the work request. Generally, <code>&lt;RESOURCE&gt;_CREATE</code> permissions for the associated resource are required.</td>
</tr>
</tbody>
</table>

### Details for the Database Service

See the following topics for details for writing policies to control access to Oracle Cloud Infrastructure Database service resources:

- Policy Details for Autonomous Database on page 2241
- Policy Details for Bare Metal, Virtual Machine, and Exadata DB Systems on page 2246
- Policy Details for Exadata Cloud@Customer
- Policy Details for External Database on page 2252
Policy Details for Autonomous Database

This topic covers details for writing policies to control access to Autonomous Database resources.

Tip:

For a sample policy, see Let database and fleet admins manage Autonomous Databases on page 2151.

Resource-Types

An aggregate resource-type covers the list of individual resource-types that directly follow. For example, writing one policy to allow a group to have access to the autonomous-database-family is equivalent to writing four separate policies for the group that would grant access to the autonomous-databases, autonomous-backups, autonomous-container-databases, and autonomous-exadata-infrastructures resource-types. For more information, see Resource-Types on page 2139.

Resource-Types for Autonomous Database

Aggregate Resource-Type

autonomous-database-family

Individual Resource-Types:

autonomous-databases
autonomous-backups
autonomous-container-databases
autonomous-exadata-infrastructures

Supported Variables

Only the general variables are supported (see General Variables for All Requests on page 2169).

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the autonomous-databases resource-type covers the same permissions and API operations as the inspect verb, plus the AUTONOMOUS_DATABASE_CONTENT_READ permission. The read verb partially covers the CreateAutonomousDatabaseBackup operation, which also needs manage permissions for autonomous-backups.

For autonomous-database-family Resource Types

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTONOMOUS_DATABASE_INSPECT</td>
<td>GetAutonomousDatabase</td>
<td>ListAutonomousDatabases</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>no extra</td>
<td>CreateAutonomousDatabaseBackup (also needs manage autonomous-backups)</td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DATABASE_CONTENT_READ</td>
<td></td>
<td>RestoreAutonomousDatabase (also needs read autonomous-backups)</td>
</tr>
<tr>
<td></td>
<td>READ +</td>
<td></td>
<td>ChangeAutonomousDatabaseCompartment (also needs read autonomous-backups)</td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DATABASE_CONTENT_WRITE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DATABASE_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>USE +</td>
<td>CreateAutonomousDatabaseBackup (also needs use autonomous-databases)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DATABASE_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DATABASE_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTONOMOUS_DB.BACKUP_INSPECT</td>
<td>ListAutonomousDatabaseBackups, GetAutonomousDatabaseBackup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>no extra</td>
<td>RestoreAutonomousDatabase (also needs use autonomous-databases)</td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DB.BACKUP_CONTENT_READ</td>
<td></td>
<td>ChangeAutonomousDatabaseCompartment (also needs use autonomous-databases)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DeleteAutonomousDatabaseBackup (also needs read autonomous-databases)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DB.BACKUP_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DB.BACKUP_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTONOMOUS_CONTAINER_DATABASE_INSPECT</td>
<td>ListAutonomousContainerDatabases, GetAutonomousContainerDatabase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>AUTONOMOUS_CONTAINER_DATABASE_UPDATE</td>
<td>UpdateAutonomousContainerDatabase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ChangeAutonomousContainerDatabaseCompartment (also needs manage autonomous-databases)</td>
</tr>
</tbody>
</table>
autonomous-exadata-infrastructures

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_INSPECT</td>
<td>GetAutonomousExadataInfrastructures</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_UPDATE</td>
<td>UpdateAutonomousExadataInfrastructures</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>LaunchAutonomousExadataInfrastructure, TerminateAutonomousExadataInfrastructure (both also need use autonomous-exadata-infrastructure)</td>
</tr>
</tbody>
</table>

For autonomous-data-warehouse-family Resource Types

Note:
The autonomous-data-warehouse-family permissions are deprecated. You can use the resource family autonomous-database-family to grant access to the Autonomous Database resources used by both Autonomous Data Warehouse databases and Autonomous Transaction Processing databases.
### IAM

#### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateAutonomousDataWarehouse</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DW_CREATE</td>
<td>CreateAutonomousDataWarehouse</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>AUTONOMOUS_DW_DELETE</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

#### autonomous-data-warehouse-backups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permission</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTONOMOUS_DW_BACKUP_INSPECT</td>
<td>AutonomousDataWarehouseBackup</td>
<td>RestoreAutonomousDataWarehouseBackup (also requires use autonomous-data-warehouses)</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + no extra</td>
<td>no extra</td>
<td>RestoreAutonomousDataWarehouseBackup (also requires use autonomous-data-warehouses)</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>READ + AUTONOMOUS_DW_BACKUP_CREATE</td>
<td>CreateAutonomousDataWarehouseBackup (also requires read autonomous-data-warehouses)</td>
<td>none</td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following tables list the API operations for Autonomous Database resources in a logical order, grouped by resource type.

For information about permissions, see [Permissions](#) on page 2162.

#### Autonomous Database API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListAutonomousExadataInfrastructureShapes</td>
<td>permission required</td>
</tr>
<tr>
<td>ListAutonomousExadataInfrastructures</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_INSPECT</td>
</tr>
<tr>
<td>LaunchAutonomousExadataInfrastructure</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_CREATE and VNIC_CREATE and SUBNET_ATTACH and VNIC_ATTACH</td>
</tr>
<tr>
<td>GetAutonomousExadataInfrastructure</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_INSPECT</td>
</tr>
<tr>
<td>TerminateAutonomousExadataInfrastructure</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_DELETE and VNIC_DELETE and SUBNET_DETACH and VNIC_DETACH</td>
</tr>
<tr>
<td>UpdateAutonomousExadataInfrastructure</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_UPDATE and AUTONOMOUS_DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>ChangeAutonomousExadataInfrastructureCompartment</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_INSPECT</td>
</tr>
<tr>
<td>ListAutonomousContainerDatabases</td>
<td>AUTONOMOUS_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>GetAutonomousContainerDatabase</td>
<td>AUTONOMOUS_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>CreateAutonomousContainerDatabase</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_UPDATE</td>
</tr>
<tr>
<td></td>
<td>and AUTONOMOUS_CONTAINER_DATABASE_CREATE</td>
</tr>
<tr>
<td>TerminateAutonomousContainerDatabase</td>
<td>AUTONOMOUS_EXADATA_INFRASTRUCTURE_UPDATE</td>
</tr>
<tr>
<td></td>
<td>and AUTONOMOUS_CONTAINER_DATABASE_DELETE</td>
</tr>
<tr>
<td>UpdateAutonomousContainerDatabase</td>
<td>AUTONOMOUS_CONTAINER_DATABASE_UPDATE</td>
</tr>
<tr>
<td>ChangeAutonomousContainerDatabase</td>
<td>AUTONOMOUS_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td></td>
<td>and AUTONOMOUS_CONTAINER_DATABASE_UPDATE</td>
</tr>
<tr>
<td>GetAutonomousDatabase</td>
<td>AUTONOMOUS_DATABASE_INSPECT</td>
</tr>
<tr>
<td>ListAutonomousDatabases</td>
<td>AUTONOMOUS_DATABASE_INSPECT</td>
</tr>
<tr>
<td>CreateAutonomousDatabase</td>
<td>AUTONOMOUS_DATABASE_CREATE</td>
</tr>
<tr>
<td>To use the private endpoint feature for a database on shared Exadata infrastructure, also need the following:</td>
<td></td>
</tr>
<tr>
<td>• In the compartment of the new Autonomous Database: VNIC_CREATE and VNIC_DELETE and NETWORK_SECURITY_GROUP_UPDATE_MEMBERS and VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP</td>
<td></td>
</tr>
<tr>
<td>• In the compartment of the specified subnet: SUBNET_ATTACH and SUBNET_DETACH</td>
<td></td>
</tr>
<tr>
<td>UpdateAutonomousDatabase</td>
<td>AUTONOMOUS_DATABASE_UPDATE</td>
</tr>
<tr>
<td>To update a database on shared Exadata infrastructure that uses the private endpoint feature, also need the following In the compartment of the Autonomous Database:</td>
<td></td>
</tr>
<tr>
<td>• VNIC_UPDATE and NETWORK_SECURITY_GROUP_UPDATE_MEMBERS and VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP</td>
<td></td>
</tr>
<tr>
<td>ChangeAutonomousDatabaseCompartment</td>
<td>AUTONOMOUS_DATABASE_UPDATE and AUTONOMOUS_DB_BACKUP_INSPECT and AUTONOMOUS_DB_BACKUP_CONTENT_READ and AUTONOMOUS_DATABASE_CONTENT_WRITE</td>
</tr>
</tbody>
</table>
IAM

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteAutonomousDatabase</td>
<td>AUTONOMOUS_DATABASE_DELETE</td>
</tr>
<tr>
<td></td>
<td>To update a database on shared Exadata infrastructure that uses the private endpoint feature, also need the following In the compartment of the Autonomous Database:</td>
</tr>
<tr>
<td></td>
<td>• In the compartment of the new Autonomous Database: VNIC_DELETE and NETWORK_SECURITY_GROUP_UPDATE_MEMBERS</td>
</tr>
<tr>
<td></td>
<td>• In the compartment of the configured subnet: SUBNET_DETACH</td>
</tr>
<tr>
<td>Start Autonomous Database</td>
<td>AUTONOMOUS_DATABASE_UPDATE</td>
</tr>
<tr>
<td>Stop Autonomous Database</td>
<td>AUTONOMOUS_DATABASE_UPDATE</td>
</tr>
<tr>
<td>Restore Autonomous Database</td>
<td>AUTONOMOUS_DB_BACKUP_CONTENT_READ and AUTONOMOUS_DATABASE_CONTENT_WRITE</td>
</tr>
<tr>
<td>Create Autonomous Database Backup</td>
<td>AUTONOMOUS_DB_BACKUP_CREATE and AUTONOMOUS_DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>Delete Autonomous Database Backup</td>
<td>AUTONOMOUS_DB_BACKUP_DELETE</td>
</tr>
<tr>
<td>List Autonomous Database Backups</td>
<td>AUTONOMOUS_DB_BACKUP_INSPECT</td>
</tr>
<tr>
<td>Get Autonomous Database Backup</td>
<td>AUTONOMOUS_DB_BACKUP_INSPECT</td>
</tr>
</tbody>
</table>

Autonomous Data Warehouse API Operations (Deprecated)

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_INSPECT</td>
</tr>
<tr>
<td>List Autonomous Data Warehouses</td>
<td>AUTONOMOUS_DW_INSPECT</td>
</tr>
<tr>
<td>Create Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_CREATE</td>
</tr>
<tr>
<td>Update Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_UPDATE</td>
</tr>
<tr>
<td>Delete Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_DELETE</td>
</tr>
<tr>
<td>Start Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_UPDATE</td>
</tr>
<tr>
<td>Stop Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_UPDATE</td>
</tr>
<tr>
<td>Restore Autonomous Data Warehouse</td>
<td>AUTONOMOUS_DW_BACKUP_CONTENT_READ and AUTONOMOUS_DW_CONTENT_WRITE</td>
</tr>
<tr>
<td>List Autonomous Data Warehouse Backups</td>
<td>AUTONOMOUS_DW_BACKUP_INSPECT</td>
</tr>
<tr>
<td>Get Autonomous Data Warehouse Backup</td>
<td>AUTONOMOUS_DW_BACKUP_INSPECT</td>
</tr>
<tr>
<td>Create Autonomous Data Warehouse Backup</td>
<td>AUTONOMOUS_DW_BACKUP_CREATE and AUTONOMOUS_DW_CONTENT_READ</td>
</tr>
</tbody>
</table>

Policy Details for Bare Metal, Virtual Machine, and Exadata DB Systems

This topic covers details for writing policies to control access to bare metal, virtual machine, and Exadata DB system resources.
**Tip:**
For a sample policy, see Let database admins manage Oracle Cloud database systems on page 2150.

**Resource-Types**
An aggregate resource-type covers the list of individual resource-types that directly follow. For example, writing one policy to allow a group to have access to the database-family is equivalent to writing five separate policies for the group that would grant access to the db-systems, db-nodes, db-homes, databases, and backups resource-types. For more information, see Resource-Types on page 2139.

**Resource-Types for Bare Metal, Virtual Machine, and Exadata DB Systems**

**Aggregate Resource-Type**
database-family

**Individual Resource-Types:**
db-systems
db-nodes
db-homes
databases
backups

**Supported Variables**
Only the general variables are supported (see General Variables for All Requests on page 2169).

**Details for Verb + Resource-Type Combinations**
The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read and use verbs for the db-systems resource-type cover no extra permissions or API operations compared to the inspect verb. However, the manage verb includes two more permissions and partially covers two more API operations.

**For database-family Resource Types**
db-systems

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DB_SYSTEM_INSPECT</td>
<td>ListDbSystems</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDbSystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListDbSystemPatches</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListDbSystemPatchHistoryEntries</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDbSystemPatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDbSystemPatchHistoryEntry</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
### Verbs and Permissions

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>DB_SYSTEM_UPDATE</td>
<td>no extra</td>
<td>ChangeDbSystemCompartment (also needs use db-homes, use databases, and inspect db-backups)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>UpdateDBSystem</td>
<td>LaunchDBSystem, TerminateDbSystem (both also need manage db-homes, manage databases, use vnics, and use subnets)</td>
</tr>
</tbody>
</table>

#### db-nodes

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DB_NODE_INSPECT</td>
<td>GetDbNode</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DB_NODE_QUERY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DbNodeAction</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DB_NODE_POWER_ACTIONS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### db-homes

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DB_HOME_INSPECT</td>
<td>ListDBHome</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDBHome</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListDbHomePatches</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListDbHomePatchHistoryEntries</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDbHomePatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDbHomePatchHistoryEntry</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>DB_HOME_UPDATE</td>
<td>UpdateDBHome</td>
<td>ChangeDbSystemCompartment (also needs use db-systems, use databases, and inspect backups)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| manage | USE +       | no extra           | LaunchDBSystem,
|        | DB_HOME_CREATE |                   | TerminateDbSystem |
|        | DB_HOME_DELETE |                   | (both also need manage
db-systems, manage
databases, use
vnics, and use
subnets). If automatic
backups are enabled on the
default database, also needs
manage backups
CreateDbHome,
(also needs use db-
systems and manage
databases). If creating
the Database Home
by restoring from a
backup, also needs read
backups
DeleteDbHome,
(also needs use db-
systems and manage
databases). If automatic
backups are enabled on the
default database, also needs
manage backups. If the
performFinalBackup
option is selected, also
needs manage backups
and read databases.
|        |             |                   |                        |

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DATABASE_INSPECT</td>
<td>ListDatabases</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDatabase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListDataGuardAssociations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDataGuardAssociation</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>no extra</td>
<td>DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateDatabase</td>
<td>CreateDataGuardAssociation</td>
</tr>
<tr>
<td></td>
<td>DATABASE_CONTENT_WRITE</td>
<td>ChangeDbSystemCompartment</td>
<td></td>
</tr>
</tbody>
</table>
|        | DATABASE_UPDATE | FailoverDataGuardAssociation | (also needs use db-
systems, use db-
homes, inspect
db-backups) |
<p>|        |              | ReinstatesDataGuardAssociation |               |
|        |              | RotateVaultKey     |                        |
|        |              | MigrateVaultKey    |                        |</p>
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>LaunchDBSystem, TerminateDbSystem (both also need manage db-systems, manage db-homes, use vnics, and use subnets)</td>
</tr>
<tr>
<td></td>
<td>DATABASE_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DATABASE_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following tables list the API operations for DB systems in a logical order, grouped by resource type. For information about permissions, see Permissions on page 2162.

#### Database API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListDbSystems</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>GetDbSystem</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>LaunchDbSystem</td>
<td>DB_SYSTEM_CREATE and DB_HOME_CREATE and DATABASE_CREATE and VNIC_CREATE and VNIC_ATTACH and SUBNET_ATTACH To enable automatic backups for the initial database, also need DB_BACKUP_CREATE and DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>UpdateDbSystem</td>
<td>DB_SYSTEM_INSPECT and DB_SYSTEM_UPDATE</td>
</tr>
<tr>
<td>ChangeDbSystemCompartment</td>
<td>DB_SYSTEM_UPDATE and DB_HOME_UPDATE and DATABASE_UPDATE and DB_BACKUP_INSPECT</td>
</tr>
<tr>
<td>ListDbSystemPatches</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ListDbSystemPatchHistoryEntries</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>GetDbSystemPatch</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>GetDbSystemPatchHistoryEntry</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>TerminateDbSystem</td>
<td>DB_SYSTEM_DELETE and DB_HOME_DELETE and DATABASE_DELETE and VNIC_DETACH and VNIC_DELETE and SUBNET_DETACH</td>
</tr>
<tr>
<td></td>
<td>If automatic backups are enabled for any database in the DB System, also need DELETE_BACKUP</td>
</tr>
<tr>
<td>GetDbNode</td>
<td>DB_NODE_INSPECT</td>
</tr>
<tr>
<td>DbNodeAction</td>
<td>DB_NODE_POWER_ACTIONS</td>
</tr>
<tr>
<td>ListDbHomes</td>
<td>DB_HOME_INSPECT</td>
</tr>
<tr>
<td>GetDbHome</td>
<td>DB_HOME_INSPECT</td>
</tr>
<tr>
<td>ListDbHomePatches</td>
<td>DB_HOME_INSPECT</td>
</tr>
<tr>
<td>ListDbHomePatchHistoryEntries</td>
<td>DB_HOME_INSPECT</td>
</tr>
<tr>
<td>GetDbHomePatch</td>
<td>DB_HOME_INSPECT</td>
</tr>
<tr>
<td>GetDbHomePatchHistoryEntry</td>
<td>DB_HOME_INSPECT</td>
</tr>
<tr>
<td>CreateDbHome</td>
<td>DB_SYSTEM_INSPECT and DB_SYSTEM_UPDATE and DB_HOME_CREATE and DATABASE_CREATE</td>
</tr>
<tr>
<td></td>
<td>To enable automatic backups for the database, also need DB_BACKUP_CREATE and DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>UpdateDbHome</td>
<td>DB_HOME_UPDATE</td>
</tr>
<tr>
<td>DeleteDbHome</td>
<td>DB_SYSTEM_UPDATE and DB_HOME_DELETE and DATABASE_DELETE</td>
</tr>
<tr>
<td></td>
<td>If automatic backups are enabled, also need DELETE_BACKUP</td>
</tr>
<tr>
<td></td>
<td>If performing a final backup on termination, also need DB_BACKUP_CREATE and DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>ListDatabases</td>
<td>DATABASE_INSPECT</td>
</tr>
<tr>
<td>GetDatabase</td>
<td>DATABASE_INSPECT</td>
</tr>
<tr>
<td>UpdateDatabase</td>
<td>DATABASE_UPDATE</td>
</tr>
<tr>
<td></td>
<td>To enable automatic backups, also need DB_BACKUP_CREATE and DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>ListDbSystemShapes</td>
<td>(no permissions required; available to anyone)</td>
</tr>
<tr>
<td>ListDbVersions</td>
<td>(no permissions required; available to anyone)</td>
</tr>
<tr>
<td>GetDataGuardAssociation</td>
<td>DATABASE_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ListDataGuardAssociations</td>
<td>DATABASE_INSPECT</td>
</tr>
<tr>
<td>CreateDataGuardAssociation</td>
<td>DB_SYSTEM_UPDATE and DB_HOME_CREATE and DB_HOME_UPDATE and DATABASE_CREATE and DATABASE_UPDATE</td>
</tr>
<tr>
<td>SwitchoverDataGuardAssociation</td>
<td>DATABASE_UPDATE</td>
</tr>
<tr>
<td>FailoverDataGuardAssociation</td>
<td>DATABASE_UPDATE</td>
</tr>
<tr>
<td>ReinstallDataGuardAssociation</td>
<td>DATABASE_UPDATE</td>
</tr>
<tr>
<td>MigrateVaultKey</td>
<td>DATABASE_UPDATE</td>
</tr>
<tr>
<td>RotateVaultKey</td>
<td>DATABASE_UPDATE</td>
</tr>
<tr>
<td>GetBackup</td>
<td>DB_BACKUP_INSPECT</td>
</tr>
<tr>
<td>ListBackups</td>
<td>DB_BACKUP_INSPECT</td>
</tr>
<tr>
<td>CreateBackup</td>
<td>DB_BACKUP_CREATE and DATABASE_CONTENT_READ</td>
</tr>
<tr>
<td>DeleteBackup</td>
<td>DB_BACKUP_DELETE and DB_BACKUP_INSPECT</td>
</tr>
<tr>
<td>RestoreDatabase</td>
<td>DB_BACKUP_INSPECT and DB_BACKUP_CONTENT_READ and DATABASE_CONTENT_WRITE</td>
</tr>
</tbody>
</table>

**Policy Details for External Database**

This topic covers details for writing policies to control access to external database resources.

**Tip:**

For a sample policy, see Let database admins manage Oracle Cloud external database resources on page 2150.

**Resource-Types**

An aggregate resource-type covers the list of individual resource-types that directly follow. For example, writing one policy to allow a group to have access to the external-database-family is equivalent to writing four separate policies for the group that would grant access to the external-container-databases, external-pluggable-databases, external-non-container-databases, and external-database-connectors resource-types. For more information, see Resource-Types on page 2139.

**Aggregate Resource-Type**

external-database-family

**Individual Resource-Types:**

external-container-databases
external-pluggable-databases
external-non-container-databases
external-database-connectors

**Supported Variables**

Only the general variables are supported (see General Variables for All Requests on page 2169).
**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the use verb for the `external-container-databases` resource-type covers the same permissions and API operations as the read verb, plus the `EXTERNAL_CONTAINER_DATABASE_UPDATE` permission. The use verb partially covers the `ScanPluggableDatabases` operation, which also needs read permissions for `external-pluggable-databases`.

**external-container-databases**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><code>EXTERNAL_CONTAINER_DATABASE_INSPECT</code></td>
<td><code>ListExternalContainerDatabases</code></td>
<td><code>GetExternalContainerDatabase</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td><code>USE +</code> <code>EXTERNAL_CONTAINER_DATABASE_CREATE</code> <code>EXTERNAL_CONTAINER_DATABASE_UPDATE</code></td>
<td><code>CreateExternalContainerDatabase</code> <code>DeleteExternalContainerDatabase</code> <code>CreateExternalContainerDatabase</code> <code>DeleteExternalContainerDatabase</code></td>
<td><code>CreateExternalContainerDatabase</code> <code>DeleteExternalContainerDatabase</code> <code>CreateExternalContainerDatabase</code> <code>DeleteExternalContainerDatabase</code></td>
</tr>
</tbody>
</table>
### external-pluggable-databases

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>EXTERNAL_PLUGGABLE_DATABASE_INSPECT</td>
<td>ListExternalPluggableDatabases, GetExternalPluggableDatabase</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + EXTERNAL_PLUGGABLE_DATABASE_CONTENT_READ</td>
<td>none</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>READ + EXTERNAL_PLUGGABLE_DATABASE_UPDATE, EXTERNAL_PLUGGABLE_DATABASE_CREATE, EXTERNAL_PLUGGABLE_DATABASE_DESTROY</td>
<td>UpdateExternalPluggableDatabase, CreateExternalPluggableDatabase (both also need manage external-connectors)</td>
<td>EnableExternalPluggableDatabase, DisableExternalPluggableDatabase (both also need use external-connectors)</td>
</tr>
<tr>
<td>manage</td>
<td>USE + EXTERNAL_PLUGGABLE_DATABASE_CREATE, EXTERNAL_PLUGGABLE_DATABASE_DESTROY</td>
<td>CreateExternalPluggableDatabase</td>
<td></td>
</tr>
</tbody>
</table>

### external-non-container-databases

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT</td>
<td>ListExternalNonContainerDatabases, GetExternalNonContainerDatabase</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + EXTERNAL_NON_CONTAINER_DATABASE_CONTENT_READ</td>
<td>none</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>READ + EXTERNAL_NON_CONTAINER_DATABASE_UPDATE, EXTERNAL_NON_CONTAINER_DATABASE_CREATE, EXTERNAL_NON_CONTAINER_DATABASE_DESTROY</td>
<td>UpdateExternalNonContainerDatabase, CreateExternalNonContainerDatabase (both also need manage external-connectors)</td>
<td>EnableExternalNonContainerDatabase, DisableExternalNonContainerDatabase (both also need use external-connectors)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>$USE +$</td>
<td>CreateExternalNonContainerDatabase</td>
<td>CreateExternalDatabase</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_CREATE</td>
<td>CreateExternalNonContainerDatabaseCreate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_DELETE</td>
<td>CreateExternalNonContainerDatabaseDelete</td>
<td></td>
</tr>
</tbody>
</table>

**external-database-connectors**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>EXTERNAL_DATABASE_CONNECTOR_INSPECT</td>
<td>CreateExternalDatabaseConnector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetExternalDatabaseConnector</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>$INSPECT +$</td>
<td>none</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTORCONTENT_READ</td>
<td>UpdateExternalDatabaseConnector</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>$READ +$</td>
<td>EnableExternalContainerDatabaseManagementService</td>
<td>DisableExternalContainerDatabaseManagementService (both also need use external-container-databases)</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTORCONTENT_WRITE</td>
<td>EnableExternalPluggableDatabaseManagementService (also needs use external-pluggable-databases)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTORUPDATE</td>
<td>EnableExternalNonContainerDatabaseManagementService (both also need use external-non-container-databases)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DisableExternalNonContainerDatabaseManagementService (also needs use external-non-container-databases)</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>$USE +$</td>
<td>CreateExternalDatabaseConnectorCreate</td>
<td>CreateExternalDatabaseConnectorCreate</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTOR_CREATE</td>
<td>CreateExternalDatabaseConnectorCreate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTOR_DELETE</td>
<td>CreateExternalDatabaseConnectorDelete</td>
<td></td>
</tr>
</tbody>
</table>
Permissions Required for Each API Operation

External Container Database API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListExternalContainerDatabases</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>GetExternalContainerDatabase</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>UpdateExternalContainerDatabase</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_CONTAINER_DATABASE_UPDATE</td>
</tr>
<tr>
<td>ChangeExternalContainerDatabaseCompartment</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_CONTAINER_DATABASE_UPDATE</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTOR_UPDATE</td>
</tr>
<tr>
<td>ScanPluggableDatabases</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_PLUGGABLE_DATABASE_INSPECT</td>
</tr>
<tr>
<td>CreateExternalContainerDatabase</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_CONTAINER_DATABASE_CREATE</td>
</tr>
<tr>
<td>DeleteExternalContainerDatabase</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_CONTAINER_DATABASE_DELETE</td>
</tr>
<tr>
<td>EnableExternalContainerDatabaseDatabaseManagement</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>and</td>
<td>EXTERNAL_CONTAINER_DATABASE_UPDATE</td>
</tr>
<tr>
<td>DisableExternalContainerDatabaseDatabaseManagement</td>
<td>EXTERNAL_DATABASE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td></td>
<td>EXTERNAL_DATABASE_CONNECTOR_UPDATE</td>
</tr>
</tbody>
</table>

External Pluggable Database API Operations

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListExternalPluggableDatabases</td>
<td>EXTERNAL_PLUGGABLE_DATABASE_INSPECT</td>
</tr>
<tr>
<td>GetExternalPluggableDatabase</td>
<td>EXTERNAL_PLUGGABLE_DATABASE_INSPECT</td>
</tr>
<tr>
<td>UpdateExternalPluggableDatabase</td>
<td>EXTERNAL_PLUGGABLE_DATABASE.UPDATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ChangeExternalPluggableDatabaseCompartment</td>
<td>EXTERNAL_PLUGGABLE_DATABASE_INSPECT, EXTERNAL_PLUGGABLE_DATABASE_UPDATE, EXTERNAL_DATABASE_CONNECTOR_INSPECT, EXTERNAL_DATABASE_CONNECTOR_UPDATE</td>
</tr>
<tr>
<td>CreateExternalPluggableDatabase</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT, EXTERNAL_CONTAINER_DATABASE_UPDATE, EXTERNAL_PLUGGABLE_DATABASE_CREATE</td>
</tr>
<tr>
<td>DeleteExternalPluggableDatabase</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT, EXTERNAL_CONTAINER_DATABASE_UPDATE, EXTERNAL_PLUGGABLE_DATABASE_DELETE</td>
</tr>
<tr>
<td>EnableExternalPluggableDatabaseDatabaseManagementService and DisableExternalPluggableDatabaseDatabaseManagementService</td>
<td>EXTERNAL_CONTAINER_DATABASE_INSPECT, EXTERNAL_CONTAINER_DATABASE_UPDATE, EXTERNAL_PLUGGABLE_DATABASE_UPDATE</td>
</tr>
</tbody>
</table>

**External Non-Container Database API Operations**

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListExternalNonContainerDatabases</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>GetExternalNonContainerDatabase</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT</td>
</tr>
<tr>
<td>UpdateExternalNonContainerDatabase</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT, EXTERNAL_NON_CONTAINER_DATABASE_UPDATE</td>
</tr>
<tr>
<td>ChangeExternalNonContainerDatabaseCompartment</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT, EXTERNAL_NON_CONTAINER_DATABASE_UPDATE, EXTERNAL_DATABASE_CONNECTOR_INSPECT, EXTERNAL_DATABASE_CONNECTOR_UPDATE</td>
</tr>
<tr>
<td>CreateExternalNonContainerDatabase</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT, EXTERNAL_NON_CONTAINER_DATABASE_CREATE</td>
</tr>
<tr>
<td>DeleteExternalNonContainerDatabase</td>
<td>EXTERNAL_NON_CONTAINER_DATABASE_INSPECT, EXTERNAL_NON_CONTAINER_DATABASE_DELETE</td>
</tr>
</tbody>
</table>
API Operation | Permissions Required to Use the Operation
--- | ---
EnableExternalNonContainerDatabaseDatabaseManagementService and DisableExternalNonContainerDatabaseDatabaseManagementService | EXTERNAL_NON_CONTAINER_DATABASE_INSPECT, EXTERNAL_NON_CONTAINER_DATABASE_UPDATE, EXTERNAL_DATABASE_CONNECTOR_DELETE, EXTERNAL_DATABASE_CONNECTOR_UPDATE

**External Database Connector API Operations**

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListExternalDatabaseConnectors</td>
<td>EXTERNAL_DATABASE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>GetExternalDatabaseConnector</td>
<td>EXTERNAL_DATABASE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>UpdateExternalDatabaseConnector</td>
<td>EXTERNAL_DATABASE_CONNECTOR_UPDATE</td>
</tr>
<tr>
<td>CreateExternalDatabaseConnector</td>
<td>One or more of the following three permissions: - EXTERNAL_CONTAINER_DATABASE_UPDATE - EXTERNAL_CONTAINER_DATABASE_UPDATE - EXTERNAL_PLUGGABLE_DATABASE_UPDATE and - EXTERNAL_DATABASE_CONNECTOR_CREATE</td>
</tr>
<tr>
<td>DeleteExternalDatabaseConnector</td>
<td>One or more of the following three permissions: - EXTERNAL_CONTAINER_DATABASE_UPDATE - EXTERNAL_CONTAINER_DATABASE_UPDATE - EXTERNAL_PLUGGABLE_DATABASE_UPDATE and - EXTERNAL_DATABASE_CONNECTOR_DELETE</td>
</tr>
<tr>
<td>CheckExternalDatabaseConnectorConnectionStatus</td>
<td>EXTERNAL_DATABASE_CONNECTOR_UPDATE</td>
</tr>
</tbody>
</table>

**Details for Database Management**

This topic covers details for writing policies to control access to the Database Management service.

**Resource-Types**

**Aggregate Resource-Type**

dbmgmt-family

**Individual Resource-Types**

- dbmgmt-jobs
- dbmgmt-managed-database-groups
- dbmgmt-managed-databases
**Comments**

A policy that uses `<verb> dbmgmt-family` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types in the family.

See the table in **Details for Verb + Resource-Type Combinations** on page 2259 for details of the API operations covered by each verb, for each individual resource-type.

**Supported Variables**

Only the general variables are supported (see **General Variables for All Requests** on page 2169).

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

### dbmgmt-jobs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><code>DBMGMT_JOB_INSPECT</code></td>
<td><code>ListJobs</code></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td><code>INSPECT</code> +</td>
<td><code>GetJob</code></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_JOB_READ</code></td>
<td><code>ListJobRuns</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>GetJobRun</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ListJobExecutions</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>GetJobExecution</code></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td><code>READ</code> +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><code>USE</code> +</td>
<td><code>ChangeJobCompartment</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>CreateJob</code> (also needs <code>manage dbmgmt-jobs</code>)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_JOB_CREATE</code></td>
<td><code>DeleteJob</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_JOB_DELETE</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_JOB_MOVE</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### dbmgmt-managed-database-groups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><code>DBMGMT_MANAGED_DB_GROUP_INSPECT</code></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td><code>INSPECT</code> +</td>
<td><code>GetManagedDatabaseGroupFleetHealthMetrics</code> for a fleet in a specified compartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_MANAGED_DB_GROUP_READ</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>GetManagedDatabaseGroupFleetHealthMetrics</code> for a fleet in a specified managed group (also needs <code>read dbmgmt-managed-databases</code>)</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td><code>READ</code> +</td>
<td><code>UpdateManagedDatabaseGroup</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_MANAGED_DB_GROUP_DB_CONTENT_READ</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_MANAGED_DB_GROUP_DB_CONTENT_WRITE</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>DBMGMT_MANAGED_DB_GROUP_DB_GROUP_UPDATE</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DBMGMT_MANAGED_DB_GROUP_ADD_DATABASE</td>
<td>AddManagedDatabaseToManagedDatabaseGroup (both also need use dbmgmt-managed-databases)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DBMGMT_MANAGED_DB_GROUP_CREATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DBMGMT_MANAGED_DB_GROUP_DELETE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DBMGMT_MANAGED_DB_GROUP_MOVE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DBMGMT_MANAGED_DB_GROUP_REMOVE_DATABASE</td>
<td></td>
</tr>
</tbody>
</table>

### dbmgmt-managed-databases

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>DBMGMT_MANAGED_DB_INSPECT</td>
<td>ListManagedDatabases</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetManagedDatabase</td>
<td>GetDatabaseFleetHealthMetrics (also needs read dbmgmt-managed-database-groups)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>GetDatabaseHomeMetrics</td>
<td>AddManagedDatabaseToManagedDatabaseGroup (both also need use dbmgmt-managed-database-groups)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDatabaseHomeMetrics</td>
<td>CreateJob (also needs manage dbmgmt-jobs)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td>no extra</td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in alphabetical order.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddManagedDatabaseToManagedDatabaseGroup</td>
<td>DBMGMT_MANAGED_DB_GROUP_ADD_DATABASE and DBMGMT_MANAGED_DB_GROUP_UPDATE</td>
</tr>
<tr>
<td>ChangeJobCompartment</td>
<td>DBMGMT_JOB_MOVE</td>
</tr>
<tr>
<td>ChangeManagedDatabaseGroupCompartment</td>
<td>DBMGMT_MANAGED_DB_GROUP_MOVE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>CreateJob</td>
<td>The permissions required depend on the SQLType for SQL Jobs and the resource-type.</td>
</tr>
<tr>
<td></td>
<td>• Query: Along with the DBMGMT_JOB_CREATE permission, the following CONTENT_READ permission is required:</td>
</tr>
<tr>
<td></td>
<td>• For a Managed Database: DBMGMT_MANAGED_DB_CONTENT_READ</td>
</tr>
<tr>
<td></td>
<td>• For a Database Group: DBMGMT_MANAGED_DB_GROUP_DB_CONTENT_READ</td>
</tr>
<tr>
<td></td>
<td>• DDL/DML/PLSQL: Along with the DBMGMT_JOB_CREATE permission, the following CONTENT_READ and CONTENT_WRITE permissions are required:</td>
</tr>
<tr>
<td></td>
<td>• For a Managed Database: DBMGMT_MANAGED_DB_CONTENT_READ and DBMGMT_MANAGED_DB_CONTENT_WRITE</td>
</tr>
<tr>
<td></td>
<td>• For a Database Group: DBMGMT_MANAGED_DB_GROUP_DB_CONTENT_READ and DBMGMT_MANAGED_DB_GROUP_DB_CONTENT_WRITE</td>
</tr>
<tr>
<td>CreateManagedDatabaseGroup</td>
<td>DBMGMT_MANAGED_DB_GROUP_CREATE</td>
</tr>
<tr>
<td>DeleteJob</td>
<td>DBMGMT_JOB_DELETE</td>
</tr>
<tr>
<td>DeleteManagedDatabaseGroup</td>
<td>DBMGMT_MANAGED_DB_GROUP_DELETE</td>
</tr>
<tr>
<td>GetDatabaseFleetHealthMetrics</td>
<td>For a fleet in a specified compartment: DBMGMT_MANAGED_DB_READ</td>
</tr>
<tr>
<td></td>
<td>For a fleet in a specified managed group: DBMGMT_MANAGED_DB_READ and DBMGMT_MANAGED_DB_GROUP_READ</td>
</tr>
<tr>
<td>GetDatabaseHomeMetrics</td>
<td>DBMGMT_MANAGED_DB_READ</td>
</tr>
<tr>
<td>GetJob</td>
<td>DBMGMT_JOB_READ</td>
</tr>
<tr>
<td>GetJobExecution</td>
<td>DBMGMT_JOB_READ</td>
</tr>
<tr>
<td>GetJobRun</td>
<td>DBMGMT_JOB_READ</td>
</tr>
<tr>
<td>Get Managed Database</td>
<td>DBMGMT_MANAGED_DB_READ</td>
</tr>
<tr>
<td>Get Managed Database Group</td>
<td>DBMGMT_MANAGED_DB_GROUP_READ</td>
</tr>
<tr>
<td>List Job Executions</td>
<td>DBMGMT_JOB_READ</td>
</tr>
<tr>
<td>List Job Runs</td>
<td>DBMGMT_JOB_READ</td>
</tr>
<tr>
<td>List Jobs</td>
<td>DBMGMT_JOB_INSPECT</td>
</tr>
<tr>
<td>List Managed Database Groups</td>
<td>DBMGMT_MANAGED_DB_GROUP_INSPECT</td>
</tr>
<tr>
<td>List Managed Databases</td>
<td>DBMGMT_MANAGED_DB_INSPECT</td>
</tr>
</tbody>
</table>
Details for the DNS Service

This topic covers details for writing policies to control access to the DNS service.

Aggregate Resource-Type
dns

Individual Resource-Types
dns-zones
dns-records
dns-steering-policies
dns-steering-policy-attachments
dns-tsig-keys
dns-views
dns-resolvers

Comments

A policy that uses `<verb> dns` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2265 for details of the API operations covered by each verb, for each individual resource-type included in `dns`.

Supported Variables

The DNS service supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

The `dns-zones` resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.dns-zone.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific DNS zones by OCID.</td>
</tr>
<tr>
<td>target.dns-zone.name</td>
<td>String</td>
<td>Use this variable to control access to specific DNS zones by name.</td>
</tr>
<tr>
<td>target.dns-zone.apex-label</td>
<td>String</td>
<td>The most significant DNS label for the target zone. Example: If the target zone's name is &quot;service.example.com&quot;, the value of this variable would be &quot;service&quot;.</td>
</tr>
<tr>
<td>target.dns-zone.parent-domain</td>
<td>String</td>
<td>The domain name of the target zone's parent zone.</td>
</tr>
<tr>
<td>target.dns.scope</td>
<td>String</td>
<td>Valid values are &quot;public&quot; and &quot;private&quot;.</td>
</tr>
</tbody>
</table>
The **dns-records** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.dns-zone.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific DNS zones by OCID.</td>
</tr>
<tr>
<td>target.dns-zone.name</td>
<td>String</td>
<td>Use this variable to control access to specific DNS zones by name.</td>
</tr>
<tr>
<td>target.dns-record.type</td>
<td>List (String)</td>
<td>Use this variable to control access to specific DNS records by type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values in the list can be any supported DNS resource type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, &quot;A&quot;, &quot;AAAA&quot;, &quot;TXT&quot;, and so on. See Supported Resource Records on page 1686.</td>
</tr>
<tr>
<td>target.dns-domain.name</td>
<td>List (String)</td>
<td>Use this variable to control access to specific domain names.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applicable to the following API operations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GetDomainRecords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PatchDomainRecords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UpdateDomainRecords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DeleteRRSet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GetRRSet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PatchRRSet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UpdateRRSet</td>
</tr>
<tr>
<td>target.dns-zone.source-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the current compartment of the DNS zone by OCID.</td>
</tr>
<tr>
<td>target.dns-zone.destination-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the destination compartment of the DNS zone by OCID.</td>
</tr>
</tbody>
</table>

**Note:**

Use the target.dns-record.type and target.dns-domain.name variables in your authorization policy to restrict users when modifying records of a specific type in a specific subdomain. A policy like this would allow a specific group of users to modify "A" records in the "example.com" domain: Allow group <GroupName> to use dns in compartment <CompartmentName> where all {target.dns-record.type='A', target.dns-domain.name = 'example.com'} Users will only be authorized to use RRSet API operations with this type of authorization policy.

The **dns-steering-policies** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.dns-steering-policy.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific steering policies by OCID.</td>
</tr>
<tr>
<td>Variable</td>
<td>Variable Type</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>target.dns-steering-policy.display-name</td>
<td>String</td>
<td>Use this variable to control access to specific steering policies by name.</td>
</tr>
<tr>
<td>target.dns-steering-policy.source-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the current compartment of the steering policy by OCID.</td>
</tr>
<tr>
<td>target.dns-steering-policy.destination-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the destination compartment of the steering policy by OCID.</td>
</tr>
</tbody>
</table>

The **dns-tsig-keys** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.dns-tsig-key.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific TSIG keys by OCID.</td>
</tr>
<tr>
<td>target.dns-tsig-key.name</td>
<td>String</td>
<td>Use this variable to control access to specific TSIG keys by name.</td>
</tr>
<tr>
<td>target.dns-tsig-key.source-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the current compartment of a specific TSIG key by OCID.</td>
</tr>
<tr>
<td>target.dns-tsig-key.destination-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the destination compartment of the specific TSIG key by OCID.</td>
</tr>
</tbody>
</table>

The **dns-view** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.dns-view.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific view by OCID.</td>
</tr>
<tr>
<td>target.dns-view.display-name</td>
<td>String</td>
<td>Use this variable to control access to specific view by name.</td>
</tr>
<tr>
<td>target.dns-view.source-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the current compartment of a specific view by OCID.</td>
</tr>
<tr>
<td>target.dns-view.destination-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the destination compartment of the specific view by OCID.</td>
</tr>
</tbody>
</table>

The **dns-resolver** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.dns-resolver.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific resolver by OCID.</td>
</tr>
<tr>
<td>target.dns-resolver.display-name</td>
<td>String</td>
<td>Use this variable to control access to specific resolver by name.</td>
</tr>
<tr>
<td>target.dns-resolver.source-compartment.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to the current compartment of a specific resolver by OCID.</td>
</tr>
</tbody>
</table>
The `target.dns-resolver.destination-compartment.id` variable type is used to control access to the destination compartment of the specific resolver by OCID.

The `target.dns-resolver-endpoint.name` variable allows you to control access to specific resolver endpoints by name.

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the manage verb for the `dns-records` resource-type covers no extra permissions or API operations compared to the use verb.

### dns-zones

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_ZONE_INSPECT</td>
<td>ListZones</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td></td>
<td>GetZone</td>
</tr>
<tr>
<td></td>
<td>DNS_ZONE_READ</td>
<td></td>
<td>GetZoneRecords</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateZone</td>
<td>UpdateZoneRecords</td>
</tr>
<tr>
<td></td>
<td>DNS_ZONE_UPDATE</td>
<td></td>
<td>PatchZoneRecords</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateSteeringPolicyAttachment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteSteeringPolicyAttachment</td>
</tr>
<tr>
<td>manage</td>
<td>UPDATE +</td>
<td>CreateZone</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_ZONE_CREATE</td>
<td>DeleteZone</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_ZONE_DELETE</td>
<td>ChangeZoneCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_ZONE_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### dns-records

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_RECORD_INSPECT</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td></td>
<td>GetDomainRecords</td>
</tr>
<tr>
<td></td>
<td>DNS_RECORD_READ</td>
<td>GetRRSet</td>
<td>GetZoneRecords</td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>PatchDomainRecords UpdateZoneRecords</td>
<td>UpdateSteeringPolicyAttachment</td>
</tr>
<tr>
<td></td>
<td>DNS_RECORD_UPDATE</td>
<td>UpdateDomainRecords PatchZoneRecords</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteRRSet PatchRRSet UpdateRRSet</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>UPDATE + no extra</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RECORD_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_RECORD_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dns-steering-policies**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_STEERING_POLICY_INSPECT</td>
<td>ListSteeringPolicies</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + DNS_STEERING_POLICY_READ</td>
<td>GetSteeringPolicy</td>
<td>UpdateSteeringPolicyAttachment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DeleteSteeringPolicyAttachment</td>
</tr>
<tr>
<td>use</td>
<td>READ + UpdateSteeringPolicy</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_POLICY_STEERING_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>UPDATE + CreateSteeringPolicy</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_STEERING_POLICY_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_STEERING_POLICY_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_STEERING_POLICY_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dns-steering-policy-attachments**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_STEERING_ATTACHMENT_INSPECT</td>
<td>ListSteeringPolicyAttachments</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + DNS_STEERING_ATTACHMENT_READ</td>
<td>GetSteeringPolicyAttachment</td>
<td></td>
</tr>
</tbody>
</table>

**dns-tsig-keys**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_TSIG_KEY_INSPECT</td>
<td>ListTsigKeys</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + DNS_TSIG_KEY_READ</td>
<td>GetTsigKey</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ + UpdateTsigKey</td>
<td>UpdateTsigKey</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_TSIG_KEY_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE+</td>
<td>CreateTsigKey</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_TSIG_KEY_CREATE</td>
<td>DeleteTsigKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_TSIG_KEY_DELETE</td>
<td>ChangeTsigKeyCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_TSIG_KEY_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dns-views**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_VIEW_INSPECT</td>
<td>ListViews</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSPECT +</td>
<td>GetView</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_VIEW_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateView</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_VIEW_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE+</td>
<td>CreateView</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_VIEW_CREATE</td>
<td>DeleteView</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_VIEW_DELETE</td>
<td>ChangeViewCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_VIEW_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dns-resolvers**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_RESOLVER_INSPECT</td>
<td>ListResolvers</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSPECT +</td>
<td>GetResolver</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateResolver</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE+</td>
<td>CreateResolver</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_CREATE</td>
<td>DeleteResolver</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_DELETE</td>
<td>ChangeResolverCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dns-resolver-endpoint**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DNS_RESOLVER_ENDPOINT_INSPECT</td>
<td>ListResolverEndpoints</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSPECT +</td>
<td>GetResolverEndpoint</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_ENDPOINT_READ</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ + UpdateResolverEndpoint</td>
<td>UpdateResolverEndpoint</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_ENDPOINT_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE + CreateResolverEndpoint</td>
<td>CreateResolverEndpoint</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_ENDPOINT_CREATE</td>
<td>DeleteResolverEndpoint</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DNS_RESOLVER_ENDPOINT_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListZones</td>
<td>DNS_ZONE_INSPECT</td>
</tr>
<tr>
<td>CreateZone</td>
<td>DNS_ZONE_CREATE</td>
</tr>
<tr>
<td>CreateChildZone</td>
<td>DNS_ZONE_CREATE</td>
</tr>
<tr>
<td>InspectParentZone</td>
<td>DNS_ZONE_INSPECT</td>
</tr>
<tr>
<td>DeleteZone</td>
<td>DNS_ZONE_DELETE</td>
</tr>
<tr>
<td>GetZone</td>
<td>DNS_ZONE_READ</td>
</tr>
<tr>
<td>UpdateZone</td>
<td>DNS_ZONE_UPDATE</td>
</tr>
<tr>
<td>ChangeZoneCompartment</td>
<td>DNS_ZONE_MOVE</td>
</tr>
<tr>
<td>GetZoneRecords</td>
<td>DNS_ZONE_READ and DNS_RECORD_READ</td>
</tr>
<tr>
<td>PatchZoneRecords</td>
<td>DNS_ZONE_UPDATE and DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>UpdateZoneRecords</td>
<td>DNS_ZONE_UPDATE and DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>GetDomainRecords</td>
<td>DNS_RECORD_READ</td>
</tr>
<tr>
<td>PatchDomainRecords</td>
<td>DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>UpdateDomainRecords</td>
<td>DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>DeleteRRSet</td>
<td>DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>GetRRSet</td>
<td>DNS_RECORD_READ</td>
</tr>
<tr>
<td>PatchRRSet</td>
<td>DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>UpdateRRSet</td>
<td>DNS_RECORD_UPDATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>ListSteeringPolicies</td>
<td>DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>CreateSteeringPolicy</td>
<td>DNS_STEERING_POLICY_CREATE</td>
</tr>
<tr>
<td>GetSteeringPolicy</td>
<td>DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>UpdateSteeringPolicy</td>
<td>DNS_STEERING_POLICY_UPDATE</td>
</tr>
<tr>
<td>DeleteSteeringPolicy</td>
<td>DNS_STEERING_POLICY_DELETE</td>
</tr>
<tr>
<td>ChangeSteeringPolicyCompartment</td>
<td>DNS_STEERING_POLICY_MOVE</td>
</tr>
<tr>
<td>ListSteeringPolicyAttachments</td>
<td>DNS_ZONE_UPDATE and DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>CreateSteeringPolicyAttachment</td>
<td>DNS_ZONE_UPDATE and DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>GetSteeringPolicyAttachment</td>
<td>DNS_ZONE_UPDATE and DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>UpdateSteeringPolicyAttachment</td>
<td>DNS_ZONE_UPDATE and DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>DeleteSteeringPolicyAttachment</td>
<td>DNS_ZONE_UPDATE and DNS_STEERING_POLICY_READ</td>
</tr>
<tr>
<td>ListTsigKeys</td>
<td>DNS_TSIG_KEY_INSPECT</td>
</tr>
<tr>
<td>CreateTsigKey</td>
<td>DNS_TSIG_KEY_CREATE</td>
</tr>
<tr>
<td>GetTsigKey</td>
<td>DNS_TSIG_KEY_READ</td>
</tr>
<tr>
<td>UpdateTsigKey</td>
<td>DNS_TSIG_KEY_UPDATE</td>
</tr>
<tr>
<td>DeleteTsigKey</td>
<td>DNS_TSIG_KEY_DELETE</td>
</tr>
<tr>
<td>ChangeTsigKeyCompartment</td>
<td>DNS_TSIG_KEY_MOVE</td>
</tr>
<tr>
<td>ListViews</td>
<td>DNS_VIEW_INSPECT</td>
</tr>
<tr>
<td>CreateView</td>
<td>DNS_VIEW_CREATE</td>
</tr>
<tr>
<td>GetView</td>
<td>DNS_VIEW_READ</td>
</tr>
<tr>
<td>UpdateView</td>
<td>DNS_VIEW_UPDATE</td>
</tr>
<tr>
<td>DeleteView</td>
<td>DNS_VIEW_DELETE</td>
</tr>
<tr>
<td>ChangeViewCompartment</td>
<td>DNS_VIEW_MOVE</td>
</tr>
<tr>
<td>ListResolvers</td>
<td>DNS_RESOLVER_INSPECT</td>
</tr>
<tr>
<td>GetResolver</td>
<td>DNS_RESOLVER_READ</td>
</tr>
<tr>
<td>UpdateResolver</td>
<td>DNS_RESOLVER_UPDATE</td>
</tr>
<tr>
<td>ChangeResolverCompartment</td>
<td>DNS_RESOLVER_MOVE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>ListResolverEndpoints</td>
<td>DNS_RESOLVER_ENDPOINT_READ and DNS_RESOLVER_ENDPOINT_INSPECT</td>
</tr>
<tr>
<td>CreateResolverEndpoint</td>
<td>DNS_RESOLVER_UPDATE and DNS_RESOLVER_ENDPOINT_CREATE</td>
</tr>
<tr>
<td>GetResolverEndpoint</td>
<td>DNS_RESOLVER_READ and DNS_RESOLVER_ENDPOINT_READ</td>
</tr>
<tr>
<td>UpdateResolverEndpoint</td>
<td>DNS_RESOLVER_UPDATE and DNS_RESOLVER_ENDPOINT_UPDATE</td>
</tr>
<tr>
<td>DeleteResolverEndpoint</td>
<td>DNS_RESOLVER_UPDATE and DNS_RESOLVER_ENDPOINT_DELETE</td>
</tr>
</tbody>
</table>

**Details for the Email Service**

This topic covers details for writing policies to control access to the Email service.

**Resource-Types**

- approved-senders
- suppressions

**Supported Variables**

The Email Service supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

The approved-senders resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.approved-sender.id</td>
<td>Entity (OCID)</td>
<td></td>
</tr>
<tr>
<td>target.approved-sender.emailaddress</td>
<td>String</td>
<td>Use this variable with the APPROVED_SENDER_USE permissions only.</td>
</tr>
</tbody>
</table>

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the use verb for the suppressions resource-type covers no extra permissions or API operations compared to the read verb.
approved-senders

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>APPROVED_SENDER_INSPECT</td>
<td>ListSenders</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetSender</td>
<td>None</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>SmtpSend</td>
<td>None</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateSender</td>
<td>none</td>
</tr>
</tbody>
</table>

suppressions

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SUPPRESSION_INSPECT</td>
<td>ListSuppression</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetSuppression</td>
<td>None</td>
</tr>
<tr>
<td>use</td>
<td>No extra</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateSuppression</td>
<td>none</td>
</tr>
</tbody>
</table>

Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListSenders</td>
<td>APPROVED_SENDER_INSPECT</td>
</tr>
<tr>
<td>GetSender</td>
<td>APPROVED_SENDER_READ</td>
</tr>
<tr>
<td>CreateSender</td>
<td>APPROVED_SENDER_CREATE</td>
</tr>
<tr>
<td>DeleteSender</td>
<td>APPROVED_SENDER_DELETE</td>
</tr>
<tr>
<td>MoveSender</td>
<td>APPROVED_SENDER_MOVE</td>
</tr>
<tr>
<td>SmtpSend</td>
<td>APPROVED_SENDER_USE</td>
</tr>
<tr>
<td>ListSuppression</td>
<td>SUPPRESSION_INSPECT</td>
</tr>
</tbody>
</table>
## Details for the Events Service

This topic covers details for writing user IAM policies that control access to rules for the Events service.

### Resource-Types

cloadevents-rules

### Supported Variables

Only the general variables are supported (see General Variables for All Requests on page 2169).

### Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for cloadevents-rules includes the same permissions and API operations as the inspect verb, plus the EVENTRULE_READ permissions and the corresponding API operation GetEventRule. The use verb adds no extra permissions or API operations compared to read. However, manage adds more permissions and operations compared to use.

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListRules</td>
<td>EVENTRULE_LIST</td>
</tr>
<tr>
<td>CreateRule</td>
<td>EVENTRULE_CREATE</td>
</tr>
</tbody>
</table>
### API Operation | Permissions Required to Use the Operation
---|---
GetRule | EVENTRULE_READ
DeleteRule | EVENTRULE_DELETE
UpdateRule | EVENTRULE_MODIFY
ChangeRuleCompartment | EVENTRULE_MODIFY

## Details for the File Storage Service

This topic covers details for writing policies to control access to the File Storage Service.

### Aggregate Resource-Type

- file-family

### Individual Resource-Types

- file-systems
- mount-targets
- export-sets

### Comments

A policy that uses `<verb> file-family` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in [Details for Verb + Resource-Type Combinations](#) on page 2273 for details of the API operations covered by each verb, for each individual resource-type included in file-family.

### Supported Variables

Only the general variables are supported (see [General Variables for All Requests](#) on page 2169).

### Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the file-systems resource-type includes the same permissions and API operations as the inspect verb, plus the FILE_SYSTEM_READ permission and a number of API operations (e.g., GetFileSystem, ListMountTargets, etc.). The use verb covers still another permission and set of API operations compared to read. Lastly, manage covers two more permissions and operations compared to use.

### export-sets

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>EXPORT_SET_INSPECT</td>
<td>ListExportSets</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>EXPORT_SET_READ</td>
<td>GetExportSet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListExports</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
## IAM

### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>CreateExport</td>
</tr>
<tr>
<td></td>
<td>EXPORT_SET_CREATE</td>
<td>CreateExportSet</td>
<td>DeleteExport</td>
</tr>
<tr>
<td></td>
<td>EXPORT_SET_UPDATE</td>
<td>UpdateExportSet</td>
<td>(both also need use file-systems.)</td>
</tr>
<tr>
<td></td>
<td>EXPORT_SET_DELETE</td>
<td>DeleteExportSet</td>
<td></td>
</tr>
</tbody>
</table>

### file-systems

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>FILE_SYSTEM_INSPECT</td>
<td>ListFileSystems</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_READ</td>
<td>GetFileSystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetSnapshot</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListSnapshots</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>DeleteExport</td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_NFSv3_EXPORT</td>
<td>(both also need manage export-sets.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_NFSv3_UNEXPORT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_CREATE</td>
<td>CreateFileSystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_UPDATE</td>
<td>UpdateFileSystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_DELETE</td>
<td>DeleteFileSystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_MOVE</td>
<td>ChangeFileSystemCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_CREATE_SNAPSHOT</td>
<td>CreateSnapshot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FILE_SYSTEM_DELETE_SNAPSHOT</td>
<td>DeleteSnapshot</td>
<td></td>
</tr>
</tbody>
</table>

If creating a file system or clone encrypted with a Key Management master encryption key, also need use key-delegate (for the caller) and read keys (for the service principal). For more information, see Details for the Vault Service on page 2347.

### mount-targets

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>MOUNT_TARGET_INSPECT</td>
<td>ListMountTargets</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>MOUNT_TARGET_READ</td>
<td>GetMountTarget</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>--------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td></td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>MOUNT_TARGET_CREATE</td>
<td></td>
<td>CreateMountTarget,</td>
</tr>
<tr>
<td></td>
<td>MOUNT_TARGET_UPDATE</td>
<td></td>
<td>DeleteMountTarget</td>
</tr>
<tr>
<td></td>
<td>MOUNT_TARGET_DELETE</td>
<td></td>
<td>(both also need</td>
</tr>
<tr>
<td></td>
<td>MOUNT_TARGET_MOVE</td>
<td></td>
<td>use vnics, use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>private-ips, and use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnets.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ChangeMountTargetCompartment</td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListExports</td>
<td>EXPORT_SET_READ</td>
</tr>
<tr>
<td>CreateExport</td>
<td>EXPORT_SET_UPDATE + FILE_SYSTEM_NFSv3_EXPORT</td>
</tr>
<tr>
<td>GetExport</td>
<td>EXPORT_SET_READ</td>
</tr>
<tr>
<td>DeleteExport</td>
<td>EXPORT_SET_UPDATE + FILE_SYSTEM_NFSv3_UNEXPORT</td>
</tr>
<tr>
<td>ListExportSets</td>
<td>EXPORT_SET_INSPECT</td>
</tr>
<tr>
<td>CreateExportSet</td>
<td>EXPORT_SET_CREATE</td>
</tr>
<tr>
<td>GetExportSet</td>
<td>EXPORT_SET_READ</td>
</tr>
<tr>
<td>UpdateExportSet</td>
<td>EXPORT_SET_UPDATE</td>
</tr>
<tr>
<td>DeleteExportSet</td>
<td>EXPORT_SET_DELETE</td>
</tr>
<tr>
<td>ListFileSystems</td>
<td>FILE_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>CreateFileSystem</td>
<td>FILE_SYSTEM_CREATE</td>
</tr>
<tr>
<td>GetFileSystem</td>
<td>FILE_SYSTEM_READ</td>
</tr>
<tr>
<td>UpdateFileSystem</td>
<td>FILE_SYSTEM_UPDATE</td>
</tr>
<tr>
<td>DeleteFileSystem</td>
<td>FILE_SYSTEM_DELETE</td>
</tr>
<tr>
<td>ChangeFileSystemCompartment</td>
<td>FILE_SYSTEM_MOVE</td>
</tr>
<tr>
<td>ListMountTargets</td>
<td>MOUNT_TARGET_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CreateMountTarget</td>
<td>MOUNT_TARGET_CREATE + VNIC_CREATE(vnicCompartment) + SUBNET_ATTACH(subnetCompartment) + VNIC_ATTACH(vnicCompartment) + PRIVATE_IP_CREATE(subnetCompartment) + PRIVATE_IP_ASSIGN(subnetCompartment) + VNIC_ASSIGN(subnetCompartment)</td>
</tr>
<tr>
<td>GetMountTarget</td>
<td>MOUNT_TARGET_READ</td>
</tr>
<tr>
<td>UpdateMountTarget</td>
<td>MOUNT_TARGET_UPDATE</td>
</tr>
<tr>
<td>DeleteMountTarget</td>
<td>MOUNT_TARGET_DELETE + VNIC_DELETE(vnicCompartment) + SUBNET_DETACH(subnetCompartment) + VNIC_DETACH(vnicCompartment) + PRIVATE_IP_DELETE(subnetCompartment) + PRIVATE_IP_UNASSIGN(subnetCompartment) + VNIC_UNASSIGN(vnicCompartment)</td>
</tr>
<tr>
<td>ChangeMountTargetCompartment</td>
<td>MOUNT_TARGET_MOVE</td>
</tr>
<tr>
<td>ListSnapshots</td>
<td>FILE_SYSTEM_READ</td>
</tr>
<tr>
<td>CreateSnapshot</td>
<td>FILE_SYSTEM_CREATE_SNAPSHOT</td>
</tr>
<tr>
<td>GetSnapshot</td>
<td>FILE_SYSTEM_READ</td>
</tr>
<tr>
<td>DeleteSnapshot</td>
<td>FILE_SYSTEM_DELETE_SNAPSHOT</td>
</tr>
</tbody>
</table>

### Details for Functions

This topic covers details for writing policies to control access to Oracle Functions.

#### Resource-Types

**Aggregate Resource-Type**
- functions-family

**Individual Resource-Types**
- fn-app
- fn-function
- fn-invocation

#### Comments

A policy that uses `<verb> functions-family` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2277 for details of the API operations covered by each verb, for each individual resource-type included in functions-family.

#### Supported Variables

Oracle Functions supports all the general variables (see General Variables for All Requests on page 2169).
**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the `read` verb for the `fn-app` resource-type includes the same permissions and API operations as the `inspect` verb, plus the `FN_APP_READ` permission and the `GetApp` API operation. In the case of the `fn-app` resource-type, the `use` verb covers no additional permissions or API operations compared to `read`. Lastly, `manage` covers more permissions and operations compared to `use`.

### fn-app

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>FN_APP_LIST</td>
<td>ListApp</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>FN_APP_READ</td>
<td>GetApp</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>FN_APP_CREATE</td>
<td>CreateApp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FN_APP_DELETE</td>
<td>DeleteApp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FN_APP_UPDATE</td>
<td>UpdateApp</td>
<td></td>
</tr>
</tbody>
</table>

### fn-function

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>FN_FUNCTION_LIST</td>
<td>ListFunctions</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>FN_FUNCTION_READ</td>
<td>GetFunction</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>FN_FUNCTION_CREATE</td>
<td>CreateFunction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FN_FUNCTION_DELETE</td>
<td>DeleteFunction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FN_FUNCTION_UPDATE</td>
<td>UpdateFunction</td>
<td></td>
</tr>
</tbody>
</table>

### fn-invocation

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>FN_INVOCATION</td>
<td>InvokeFunction</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type. For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateApp</td>
<td>FN_APP_CREATE</td>
</tr>
<tr>
<td>DeleteApp</td>
<td>FN_APP_DELETE</td>
</tr>
<tr>
<td>ListApp</td>
<td>FN_APP_LIST</td>
</tr>
<tr>
<td>GetApp</td>
<td>FN_APP_READ</td>
</tr>
<tr>
<td>UpdateApp</td>
<td>FN_APP_UPDATE</td>
</tr>
<tr>
<td>CreateFunction</td>
<td>FN_FUNCTION_CREATE</td>
</tr>
<tr>
<td>DeleteFunction</td>
<td>FN_FUNCTION_DELETE</td>
</tr>
<tr>
<td>ListFunctions</td>
<td>FN_FUNCTION_LIST</td>
</tr>
<tr>
<td>GetFunction</td>
<td>FN_FUNCTION_READ</td>
</tr>
<tr>
<td>UpdateFunction</td>
<td>FN_FUNCTION_UPDATE</td>
</tr>
<tr>
<td>InvokeFunction</td>
<td>FN_INVOCATION</td>
</tr>
</tbody>
</table>

Details for the Health Checks Service

This topic covers details for writing policies to control access to the Health Checks service.

Resource-Types

- health-check-monitor
- health-check-results
- on-demand-probe
- vantage-points
- health-check-family

Supported Variables

The Health Checks Service supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here. Values in the list can be any valid test type. For example, HTTP, HTTPS, ICMP, etc.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.health-check-monitor.test-type</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>target.on-demand-probe.test-type</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>target.health-check-results.test-type</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.
For example, the `use` verb for the `health-check-monitor` resource-type covers no extra permissions or API operations compared to the `read` verb.

### health-check-monitor

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>HEALTH_CHECK_MONITOR_INSPECT</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetOHCMonitor</td>
<td>None</td>
</tr>
<tr>
<td>use</td>
<td><strong>No extra</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateOHCMonitor</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteOHCMonitor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MoveOHCMonitor</td>
<td></td>
</tr>
</tbody>
</table>

### health-check-results

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><strong>No extra</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>read</td>
<td>HEALTH_CHECK_RESULTS_READ</td>
<td>ListOHCProbeResults</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListOHCProbeResultsForTarget</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>No extra</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>manage</td>
<td>No extra</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

### vantage-points

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VANTAGE_POINTS_INSPECT</td>
<td>ListVantagePoints</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>No extra</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>use</td>
<td>No extra</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>manage</td>
<td>No extra</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

### on-demand-probe

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><strong>No extra</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>read</td>
<td><strong>No extra</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>use</td>
<td><strong>No extra</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateOnDemandOHCProbeNone</td>
<td>ON_DEMAND_PROBE_MANAGE</td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListOHCMonitors</td>
<td>HEALTH_CHECK_MONITOR_INSPECT</td>
</tr>
<tr>
<td>CreateOHCMonitor</td>
<td>HEALTH_CHECK_MONITOR_MANAGE</td>
</tr>
<tr>
<td>GetOHCMonitor</td>
<td>HEALTH_CHECK_MONITOR_READ</td>
</tr>
<tr>
<td>UpdateOHCMonitor</td>
<td>HEALTH_CHECK_MONITOR_MANAGE</td>
</tr>
<tr>
<td>DeleteOHCMonitor</td>
<td>HEALTH_CHECK_MONITOR_MANAGE</td>
</tr>
<tr>
<td>ListOHCProbeResults</td>
<td>HEALTH_CHECK_RESULTS_READ</td>
</tr>
<tr>
<td>ListOHCProbeResultsForTarget</td>
<td>HEALTH_CHECK_RESULTS_READ</td>
</tr>
<tr>
<td>ListVantagePoints</td>
<td>VANTAGE_POINTS_INSPECT</td>
</tr>
<tr>
<td>CreateOnDemandOHCProbe</td>
<td>ON_DEMAND_PROBE_MANAGE</td>
</tr>
<tr>
<td>MoveOHCMonitor</td>
<td>HEALTH_CHECK_MONITOR_MOVE</td>
</tr>
</tbody>
</table>

**Details for IAM**

This topic covers details for writing policies to control access to IAM.

**Resource-Types**

authentication-policies  
compartments  
credentials  
dynamic-groups  
groups  
identity-providers  
network-sources  
policies  
tag-defaults  
tag-namespaces  
tenancies  
users  
workrequest
**Supported Variables**

IAM supports all the general variables (see [General Variables for All Requests](#) on page 2169), plus additional ones listed here:

<table>
<thead>
<tr>
<th>Operations for This Resource-Type...</th>
<th>Can Use These Variables...</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>users</strong></td>
<td>target.user.id</td>
<td>Entity (OCID)</td>
<td>Not available to use with CreateUser.</td>
</tr>
<tr>
<td></td>
<td>target.user.name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td><strong>groups</strong></td>
<td>target.group.id</td>
<td>Entity (OCID)</td>
<td>Not available to use with CreateGroup.</td>
</tr>
<tr>
<td></td>
<td>target.group.name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>target.group.member</td>
<td>Boolean</td>
<td>True if request.user is a member of target.group.</td>
</tr>
<tr>
<td><strong>policies</strong></td>
<td>target.policy.id</td>
<td>Entity (OCID)</td>
<td>Not available to use with CreatePolicy.</td>
</tr>
<tr>
<td></td>
<td>target.policy.name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td><strong>compartments</strong></td>
<td>target.compartment.id</td>
<td>Entity (OCID)</td>
<td>For CreateCompartment, this will be the value of the parent compartment (e.g., the root compartment). This is a universal variable available to use with any request across all services (see <a href="#">General Variables for All Requests</a> on page 2169).</td>
</tr>
<tr>
<td></td>
<td>target.compartment.name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td><strong>tag-namespace</strong></td>
<td>target.tag-namespace.id</td>
<td>Entity (OCID)</td>
<td>This variable is supported only in statements granting permissions for the tag-namespaces resource-type. For an example, see <a href="#">Required Permissions for Working with Defined Tags</a> on page 3915. Not available to use with CreateTagNamespace.</td>
</tr>
<tr>
<td></td>
<td>target.tag-namespace.name</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>

**Details for Verbs + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for compartments covers no extra permissions or API operations compared to the inspect verb. The use verb includes the same ones as the read verb, plus the COMPARTMENT_UPDATE permission and UpdateCompartment API operation. The manage verb includes the same permissions and
API operations as the use verb, plus the COMPARTMENT_CREATE permission and two API operations: CreateCompartment and DeleteCompartment.

**authentication-policies**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>AUTHENTICATION_POLICY_INSPECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE + AUTHENTICATION_POLICY_UPDATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**compartments**

To move a compartment (that is, use the MoveCompartment operation) you must belong to a group that has manage all-resources permissions on the lowest shared parent compartment of the current compartment and the destination compartment.

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>COMPARTMENT_INSPECT</td>
<td>ListCompartments</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListAvailabilityDomains</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListFaultDomains</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ + COMPARTMENT_UPDATE</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE + COMPARTMENT_CREATE</td>
<td>USE + COMPARTMENT_DELETE</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMPARTMENT_CREATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMPARTMENT_DELETE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMPARTMENT_RECOVER</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RecoverCompartment</td>
<td></td>
</tr>
</tbody>
</table>

**credentials**

The credentials resource type refers to only the SMTP credentials. Permissions to work with other credentials that can be added to a user (such as auth tokens, API keys, and customer secret keys) are included with users resource permissions.

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>CREDENTIAL_INSPECT</td>
<td>ListSmtpCredentials</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-----------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>CREDENTIAL_ADD</td>
<td>CreateSmtpCredential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CREDENTIAL_UPDATE</td>
<td>UpdateSmtpCredential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CREDENTIAL_REMOVE</td>
<td>DeleteSmtpCredential</td>
<td></td>
</tr>
</tbody>
</table>

`dynamic-groups`

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>DYNAMIC_GROUP_INSPECT</td>
<td>ListDynamicGroups, GetDynamicGroup</td>
<td>No extra</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>No extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>DYNAMIC_GROUP_CREATE</td>
<td>CreateDynamicGroup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DYNAMIC_GROUP_DELETE</td>
<td>DeleteDynamicGroup</td>
<td></td>
</tr>
</tbody>
</table>

`groups`

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>GROUP_INSPECT</td>
<td>ListGroups, GetGroup</td>
<td>GetUserGroupMembership (also need inspect users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ListIdpGroupMappings, GetIdpGroupMapping (both also need inspect identity-providers)</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>READ +</td>
</tr>
<tr>
<td></td>
<td>GROUP_UPDATE</td>
<td>UpdateGroup</td>
<td>AddUserToGroup (also need use users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RemoveUserFromGroup (also need use users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AddIdpGroupMapping, DeleteIdpGroupMapping (both also need manage identity-providers)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>GROUP_CREATE</td>
<td>CreateGroup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GROUP_DELETE</td>
<td>DeleteGroup</td>
<td></td>
</tr>
</tbody>
</table>

**identity-providers**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>IDENTITY_PROVIDER_INSPECT</td>
<td>IdentitiesProvider</td>
<td>ListIdpGroupMappings,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetIdentityProvider</td>
<td>GetIdpGroupMapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>inspect groups)</td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>IDENTITY_PROVIDER_UPDATE</td>
<td>UpdateIdentityProvider</td>
<td>ListIdpGroupMappings,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetIdentityProvider</td>
<td>GetIdpGroupMapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IdentityProvider groups)</td>
</tr>
</tbody>
</table>

**network-sources**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>NETWORK_SOURCE_INSPECT</td>
<td>NetworkSources</td>
<td>No extra</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetNetworkSource</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>No extra</td>
</tr>
<tr>
<td></td>
<td>NETWORK_SOURCE_UPDATE</td>
<td>UpdateNetworkSource</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>NETWORK_SOURCE_CREATE</td>
<td>CreateNetworkSource</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NETWORK_SOURCE_DELETE</td>
<td>DeleteNetworkSource</td>
<td></td>
</tr>
</tbody>
</table>

**policies**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>POLICY_READ</td>
<td>ListPolicies</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetPolicy</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>
### IAM

**Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
--- | --- | --- | ---
**use** | no extra | no extra | none

**Note:** The ability to update policies is available only with manage policies.

**manage**

<table>
<thead>
<tr>
<th>Implmed</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>USE + POLICY_UPDATE</td>
<td>UpdatePolicy</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>POLICY_CREATE</td>
<td>CreatePolicy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLICY_DELETE</td>
<td>DeletePolicy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### tag-namespaces

**Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
--- | --- | --- | ---
**inspect** | TAG_NAMESPACE_INSPECT | none |

- ListTagNamespaces
- GetTagName
- ListTags
- ListCostTrackingTags
- GetTag
- GetTaggingWorkRequest
- ListTaggingWorkRequest
- ListTaggingWorkRequestErrors
- ListTaggingWorkRequestLogs

**read**

<table>
<thead>
<tr>
<th>Implmed</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**use**

<table>
<thead>
<tr>
<th>Implmed</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ + TAG_NAMESPACE_USE</td>
<td>CreateTag</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** To apply, update, or remove defined tags for a resource, a user must be granted permissions on the resource and permissions to use the tag namespace.
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>TAG_NAMESPACE_UPDATE</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TAG_NAMESPACE_CREATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TAG_NAMESPACE_MOVE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TAG_NAMESPACE_DELETE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>USE +</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateTagNamespace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateTagNamespace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ChangeTagNamespaceCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CascadeDeleteTagNamespace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteTagNamespace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteTag</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BulkDeleteTags</td>
<td></td>
</tr>
</tbody>
</table>

**Tag-Defaults**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>TAG_DEFAULT_INSPECT</td>
<td>ListTagDefaults</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetTagDefault</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>INSPECT +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TAG_DEFAULT_CREATE</td>
<td>CreateTagDefault</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TAG_DEFAULT_UPDATE</td>
<td>UpdateTagDefault</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TAG_DEFAULT_DELETE</td>
<td>DeleteTagDefault</td>
</tr>
</tbody>
</table>

**Tenancies**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>TENANCY_INSPECT</td>
<td>ListRegionSubscription</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetTenancy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListRegions</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>TENANCY_UPDATE</td>
<td>CreateRegionSubscription</td>
</tr>
</tbody>
</table>
users

Note that to work with the SMTP credentials for a user, you must have permissions for the credentials resource type.

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>USER_INSPECT</td>
<td>ListUsers</td>
<td>GetUserGroupMembership (also need inspect groups)</td>
</tr>
<tr>
<td>use</td>
<td>READ + USER_UPDATE</td>
<td>UpdateUser</td>
<td>AddUserToGroup (also need use groups), RemoveUserFromGroup (also need use groups)</td>
</tr>
</tbody>
</table>
## IAM

### Verbs

<table>
<thead>
<tr>
<th>Verb</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>no extra</td>
</tr>
<tr>
<td></td>
<td>USER_CREATE</td>
<td>CreateUser</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_DELETE</td>
<td>DeleteUser</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_UNBLOCK</td>
<td>UpdateUserState</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_APIKEY_ADD</td>
<td>UploadApiKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_APIKEY_REMOVE</td>
<td>DeleteApiKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_UIPASS_SET</td>
<td>CreateOrResetUIPassword</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_UIPASS_RESET</td>
<td>UpdateSwiftPassword</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SWIFTPASS_SET</td>
<td>CreateSwiftPassword</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SWIFTPASS_RESET</td>
<td>DeleteSwiftPassword</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_AUTHTOKEN_SET</td>
<td>UpdateAuthToken</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_AUTHTOKEN_RESET</td>
<td>CreateUser</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_AUTHTOKEN_REMOVE</td>
<td>DeleteAuthToken</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_OAUTH2_CLIENT_CRED_CREATE</td>
<td>UpdateOAuthClientCredential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_OAUTH2_CLIENT_CRED_UPDATE</td>
<td>CreateOAuthClientCredential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_OAUTH2_CLIENT_CRED_REMOVE</td>
<td>DeleteOAuthClientCredential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SECRETKEY_ADD</td>
<td>CreateSecretKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SECRETKEY_UPDATE</td>
<td>DeleteCustomerSecretKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SECRETKEY_REMOVE</td>
<td>CreateCustomerSecretKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SUPPORT_ACCOUNT_LINK</td>
<td>DeleteOAuthClientCredential</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_SUPPORT_ACCOUNT_UNLINK</td>
<td>CreateSupportAccount</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_TOTPDEVICE_ADD</td>
<td>DeleteMfaTotpDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_TOTPDEVICE_REMOVE</td>
<td>CreateMfaTotpDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USER_TOTPDEVICE_UPDATE</td>
<td>ActivateMfaTotpDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteMfaTotpDevice</td>
<td></td>
</tr>
</tbody>
</table>

## Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListRegions</td>
<td>TENANCY_INSPECT</td>
</tr>
<tr>
<td>ListRegionSubscriptions</td>
<td>TENANCY_INSPECT</td>
</tr>
<tr>
<td>CreateRegionSubscription</td>
<td>TENANCY_UPDATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>GetTenancy</td>
<td>TENANCY_INSPECT</td>
</tr>
<tr>
<td>GetAuthenticationPolicy</td>
<td>AUTHENTICATION_POLICY_INSPECT</td>
</tr>
<tr>
<td>UpdateAuthenticationPolicy</td>
<td>AUTHENTICATION_POLICY_UPDATE</td>
</tr>
<tr>
<td>ListAvailabilityDomains</td>
<td>COMPARTMENT_INSPECT</td>
</tr>
<tr>
<td>ListFaultDomains</td>
<td>COMPARTMENT_INSPECT</td>
</tr>
<tr>
<td>ListCompartments</td>
<td>COMPARTMENT_INSPECT</td>
</tr>
<tr>
<td>GetCompartment</td>
<td>COMPARTMENT_INSPECT</td>
</tr>
<tr>
<td>UpdateCompartment</td>
<td>COMPARTMENT_UPDATE</td>
</tr>
<tr>
<td>CreateCompartment</td>
<td>COMPARTMENT_CREATE</td>
</tr>
<tr>
<td>RecoverCompartment</td>
<td>COMPARTMENT_RECOVER</td>
</tr>
<tr>
<td>DeleteCompartment</td>
<td>COMPARTMENT_DELETE</td>
</tr>
<tr>
<td>MoveCompartment</td>
<td>There is not a single permission associated with the MoveCompartment operation. This operation requires manage all-resources permissions on the lowest shared parent compartment of the current compartment and the destination compartment.</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>COMPARTMENT_READ</td>
</tr>
<tr>
<td>ListUsers</td>
<td>USER_INSPECT</td>
</tr>
<tr>
<td>GetUser</td>
<td>USER_INSPECT</td>
</tr>
<tr>
<td>UpdateUser</td>
<td>USER_UPDATE</td>
</tr>
<tr>
<td>UpdateUserState</td>
<td>USER_UPDATE and USER_UNBLOCK</td>
</tr>
<tr>
<td>CreateUser</td>
<td>USER_CREATE</td>
</tr>
<tr>
<td>DeleteUser</td>
<td>USER_DELETE</td>
</tr>
<tr>
<td>CreateOrResetUIPassword</td>
<td>USER_UPDATE and USER_UIPASS_RESET</td>
</tr>
<tr>
<td>ListApiKeys</td>
<td>USER_READ</td>
</tr>
<tr>
<td>UploadApiKey</td>
<td>USER_UPDATE and USER_APIKEY_ADD</td>
</tr>
<tr>
<td>DeleteApiKey</td>
<td>USER_UPDATE and USER_APIKEY_REMOVE</td>
</tr>
<tr>
<td>ListAuthToken</td>
<td>USER_READ</td>
</tr>
<tr>
<td>UpdateAuthToken</td>
<td>USER_UPDATE and USER_AUTHTOKEN_RESET</td>
</tr>
<tr>
<td>CreateAuthToken</td>
<td>USER_UPDATE and USER_AUTHTOKEN_SET</td>
</tr>
<tr>
<td>DeleteAuthToken</td>
<td>USER_UPDATE and USER_AUTHTOKEN_REMOVE</td>
</tr>
<tr>
<td>ListSwiftPasswords</td>
<td>USER_READ</td>
</tr>
<tr>
<td>UpdateSwiftPassword</td>
<td>USER_UPDATE and USER_SWIFTPASS_RESET</td>
</tr>
<tr>
<td>CreateSwiftPassword</td>
<td>USER_UPDATE and USER_SWIFTPASS_SET</td>
</tr>
<tr>
<td>DeleteSwiftPassword</td>
<td>USER_UPDATE and USER_SWIFTPASS_REMOVE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>ListCustomerSecretKeys</td>
<td>USER_READ</td>
</tr>
<tr>
<td>CreateSecretKey</td>
<td>USER_UPDATE and USER_SECRETKEY_ADD</td>
</tr>
<tr>
<td>UpdateCustomerSecretKey</td>
<td>USER_UPDATE and USER_SECRETKEY_UPDATE</td>
</tr>
<tr>
<td>DeleteCustomerSecretKey</td>
<td>USER_UPDATE and USER_SECRETKEY_REMOVE</td>
</tr>
<tr>
<td>CreateOAuthClientCredential</td>
<td>USER_UPDATE and USER_OAUTH2_CLIENT_CRED_CREATE</td>
</tr>
<tr>
<td>UpdateOAuthClientCredential</td>
<td>USER_UPDATE and USER_OAUTH2_CLIENT_CRED_UPDATE</td>
</tr>
<tr>
<td>ListOAuthClientCredentials</td>
<td>USER_READ</td>
</tr>
<tr>
<td>DeleteOAuthClientCredential</td>
<td>USER_UPDATE and USER_OAUTH2_CLIENT_CRED_REMOVE</td>
</tr>
<tr>
<td>LinkSupportAccount</td>
<td>USER_SUPPORTACCOUNT_LINK</td>
</tr>
<tr>
<td>UnlinkSupportAccount</td>
<td>USER_SUPPORTACCOUNT_UNLINK</td>
</tr>
<tr>
<td>CreateSmtpCredential</td>
<td>CREDENTIAL_ADD</td>
</tr>
<tr>
<td>ListSmtpCredentials</td>
<td>CREDENTIAL_INSPECT</td>
</tr>
<tr>
<td>UpdateSmtpCredential</td>
<td>CREDENTIAL_UPDATE</td>
</tr>
<tr>
<td>DeleteSmtpCredential</td>
<td>CREDENTIAL_REMOVE</td>
</tr>
<tr>
<td>ListUserGroupMemberships</td>
<td>GROUP_INSPECT and USER_INSPECT</td>
</tr>
<tr>
<td>GetUserGroupMembership</td>
<td>USER_INSPECT and GROUP_INSPECT</td>
</tr>
<tr>
<td>AddUserToGroup</td>
<td>GROUP_UPDATE and USER_UPDATE</td>
</tr>
<tr>
<td>RemoveUserFromGroup</td>
<td>GROUP_UPDATE and USER_UPDATE</td>
</tr>
<tr>
<td>ListGroups</td>
<td>GROUP_INSPECT</td>
</tr>
<tr>
<td>GetGroup</td>
<td>GROUP_INSPECT</td>
</tr>
<tr>
<td>UpdateGroup</td>
<td>GROUP_UPDATE</td>
</tr>
<tr>
<td>CreateGroup</td>
<td>GROUP_CREATE</td>
</tr>
<tr>
<td>DeleteGroup</td>
<td>GROUP_DELETE</td>
</tr>
<tr>
<td>ListDynamicGroups</td>
<td>DYNAMIC_GROUP_INSPECT</td>
</tr>
<tr>
<td>GetDynamicGroup</td>
<td>DYNAMIC_GROUP_INSPECT</td>
</tr>
<tr>
<td>UpdateDynamicGroup</td>
<td>DYNAMIC_GROUP_UPDATE</td>
</tr>
<tr>
<td>CreateDynamicGroup</td>
<td>DYNAMIC_GROUP_CREATE</td>
</tr>
<tr>
<td>DeleteDynamicGroup</td>
<td>DYNAMIC_GROUP_DELETE</td>
</tr>
<tr>
<td>GetNetworkSource</td>
<td>NETWORK_SOURCE_INSPECT</td>
</tr>
<tr>
<td>ListNetworkSources</td>
<td>NETWORK_SOURCE_INSPECT</td>
</tr>
<tr>
<td>CreateNetworkSource</td>
<td>NETWORK_SOURCE_CREATE</td>
</tr>
<tr>
<td>UpdateNetworkSource</td>
<td>NETWORK_SOURCE_UPDATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>DeleteNetworkSource</td>
<td>NETWORK_SOURCE_DELETE</td>
</tr>
<tr>
<td>ListPolicies</td>
<td>POLICY_READ</td>
</tr>
<tr>
<td>GetPolicy</td>
<td>POLICY_READ</td>
</tr>
<tr>
<td>UpdatePolicy</td>
<td>POLICY_UPDATE</td>
</tr>
<tr>
<td>CreatePolicy</td>
<td>POLICY_CREATE</td>
</tr>
<tr>
<td>DeletePolicy</td>
<td>POLICY_DELETE</td>
</tr>
<tr>
<td>ListIdentityProviders</td>
<td>IDENTITY_PROVIDER_INSPECT</td>
</tr>
<tr>
<td>GetIdentityProvider</td>
<td>IDENTITY_PROVIDER_INSPECT</td>
</tr>
<tr>
<td>UpdateIdentityProvider</td>
<td>IDENTITY_PROVIDER_UPDATE</td>
</tr>
<tr>
<td>CreateIdentityProvider</td>
<td>IDENTITY_PROVIDER_CREATE</td>
</tr>
<tr>
<td>DeleteIdentityProvider</td>
<td>IDENTITY_PROVIDER_DELETE</td>
</tr>
<tr>
<td>ListIdpGroupMappings</td>
<td>IDENTITY_PROVIDER_INSPECT and GROUP_INSPECT</td>
</tr>
<tr>
<td>GetIdpGroupMapping</td>
<td>IDENTITY_PROVIDER_INSPECT and GROUP_INSPECT</td>
</tr>
<tr>
<td>AddIdpGroupMapping</td>
<td>IDENTITY_PROVIDER_UPDATE and GROUP_UPDATE</td>
</tr>
<tr>
<td>DeleteIdpGroupMapping</td>
<td>IDENTITY_PROVIDER_UPDATE and GROUP_UPDATE</td>
</tr>
<tr>
<td>ListTagNamespaces</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>ListTaggingWorkRequest</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>ListTaggingWorkRequestErrors</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>ListTaggingWorkRequestLogs</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>GetTaggingWorkRequest</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>GetTagName</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>CreateTagName</td>
<td>TAG_NAMESPACE_CREATE</td>
</tr>
<tr>
<td>UpdateTagName</td>
<td>TAG_NAMESPACE_UPDATE</td>
</tr>
<tr>
<td>ChangeTagNameNamespaceCompartment</td>
<td>TAG_NAMESPACE_MOVE</td>
</tr>
<tr>
<td>CascadeDeleteTagNameNamespace</td>
<td>TAG_NAMESPACE_DELETE</td>
</tr>
<tr>
<td>DeleteTagName</td>
<td>TAG_NAMESPACE_DELETE</td>
</tr>
<tr>
<td>ListTags</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>BulkEditTags</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>ListCostTrackingTags</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>GetTag</td>
<td>TAG_NAMESPACE_INSPECT</td>
</tr>
<tr>
<td>CreateTag</td>
<td>TAG_NAMESPACE_USE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>UpdateTag</td>
<td>TAG_NAMESPACE_USE</td>
</tr>
<tr>
<td>DeleteTag</td>
<td>TAG_NAMESPACE_DELETE</td>
</tr>
<tr>
<td>BulkDeleteTags</td>
<td>TAG_NAMESPACE_DELETE</td>
</tr>
<tr>
<td>ListTagDefaults</td>
<td>TAG_DEFAULT_INSPECT</td>
</tr>
<tr>
<td>GetTagDefault</td>
<td>TAG_DEFAULT_INSPECT</td>
</tr>
<tr>
<td>CreateTagDefault</td>
<td>TAG_DEFAULT_INSPECT</td>
</tr>
<tr>
<td>UpdateTagDefault</td>
<td>TAG_DEFAULT_MANAGE</td>
</tr>
<tr>
<td>DeleteTagDefault</td>
<td>TAG_DEFAULT_MANAGE</td>
</tr>
</tbody>
</table>

Details for Load Balancing

This topic covers details for writing policies to control access to the Load Balancing service.

Resource-Types

load-balancers

Supported Variables

Only the general variables are supported (see General Variables for All Requests on page 2169).

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for load-balancers includes the same permissions and API operations as the inspect verb, plus the LOAD_BALANCER_READ permission and a number of API operations (e.g., GetLoadBalancer, ListWorkRequests, etc.). The use verb covers still another permission and set of API operations compared to read. And manage covers two more permissions and operations compared to use.

load-balancers

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOAD_BALANCER_INSPECT</td>
<td>ListLoadBalancers</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListShapes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListPolicies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListProtocols</td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>LOAD_BALANCER_READ</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetLoadBalancer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequests</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListBackendSets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetBackendSet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListBackends</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetBackend</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetHealthChecker</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListCertificates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>READ +</td>
<td>LOAD_BALANCER_UPDATE</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateLoadBalancer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOAD_BALANCER_MOVE</td>
<td>ChangeLoadBalancerCompartment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateBackendSet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateBackendSet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteBackendSet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateBackend</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateBackend</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteBackend</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateHealthChecker</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateCertificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteCertificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateListener</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateListener</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteListener</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>LOAD_BALANCER_CREATE</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateLoadBalancer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOAD_BALANCER_DELETE</td>
<td>DeleteLoadBalancer</td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

**Tip:**

If a group uses the Console to manage load balancers, permissions to use the associated networking resources are required. See the load balancing policy examples for further guidance.

For information about permissions, see [Permissions](#) on page 2162.
<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListLoadBalancers</td>
<td>LOAD_BALANCER_INSPECT and</td>
</tr>
<tr>
<td>GetLoadBalancer</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>ChangeLoadBalancerCompartment</td>
<td>LOAD_BALANCER_MOVE</td>
</tr>
<tr>
<td>UpdateLoadBalancer</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>CreateLoadBalancer</td>
<td>LOAD_BALANCER_CREATE</td>
</tr>
<tr>
<td>DeleteLoadBalancer</td>
<td>LOAD_BALANCER_DELETE</td>
</tr>
<tr>
<td>ListShapes</td>
<td>LOAD_BALANCER_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>ListBackendSets</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>GetBackendSet</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>UpdateBackendSet</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>CreateBackendSet</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>DeleteBackendSet</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>ListBackends</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>GetBackend</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>UpdateBackend</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>CreateBackend</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>DeleteBackend</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>GetHealthChecker</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>UpdateHealthChecker</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>ListCertificates</td>
<td>LOAD_BALANCER_READ</td>
</tr>
<tr>
<td>CreateCertificate</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>DeleteCertificate</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>UpdateListener</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>CreateListener</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>DeleteListener</td>
<td>LOAD_BALANCER_UPDATE</td>
</tr>
<tr>
<td>ListPolicies</td>
<td>LOAD_BALANCER_INSPECT</td>
</tr>
<tr>
<td>ListProtocols</td>
<td>LOAD_BALANCER_INSPECT</td>
</tr>
</tbody>
</table>

**Details for Logging**

This topic covers details for writing policies to control access to Logging.

**Resource-Types**

**Aggregate Resource-Type**
- logging-family
Individual Resource-Ttypes

- log-objects
- log-groups
- log-content

Comments

A policy that uses `<verb> logs` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations for a detailed breakout of the API operations covered by each verb, for each individual resource-type included in logs.

Supported Variables

Logging supports all the general variables (see General Variables for All Requests on page 2169), plus additional ones listed here:

<table>
<thead>
<tr>
<th>Operations for This Resource-Type...</th>
<th>Can Use These Variables...</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-groups</td>
<td>target.loggroup.id</td>
<td>Entity (OCID)</td>
<td></td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the log-groups resource-type includes the same permissions and API operations as the inspect verb, plus the LOG_GROUPS_READ permission and the corresponding API operations GetLog and GetLogGroup.

log-objects

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSPECT</td>
<td>LOG_OBJECT_INSPECT</td>
<td>ListLogs</td>
<td>none</td>
</tr>
<tr>
<td>READ</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_OBJECT_READ</td>
<td>GetLog</td>
<td></td>
</tr>
<tr>
<td>USE</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_OBJECT_UPDATE</td>
<td>UpdateLog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_OBJECT_WRITE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MANAGE</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_OBJECT_CREATE</td>
<td>CreateLog</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_OBJECT_DELETE</td>
<td>DeleteLog</td>
<td></td>
</tr>
</tbody>
</table>

log-groups

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSPECT</td>
<td>LOG_GROUP_INSPECT</td>
<td>ListLogGroups</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListLogs</td>
<td></td>
</tr>
</tbody>
</table>
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ</td>
<td><code>INSPECT +</code></td>
<td><code>INSPECT +</code></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><code>LOG_GROUP_READ</code></td>
<td><code>GetLogGroup</code></td>
<td><code>GetLog</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ListSearchLogs</code></td>
<td></td>
</tr>
<tr>
<td>USE</td>
<td><code>READ +</code></td>
<td><code>READ +</code></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><code>LOG_GROUP_UPDATE</code></td>
<td><code>UpdateLogGroup</code></td>
<td><code>ChangeLogGroupCompartment</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>UpdateLog</code></td>
<td></td>
</tr>
<tr>
<td>MANAGE</td>
<td><code>USE +</code></td>
<td><code>USE +</code></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><code>LOG_GROUP_CREATE</code></td>
<td><code>CreateLogGroup</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>LOG_GROUP_DELETE</code></td>
<td><code>DeleteLogGroup</code></td>
<td><code>CreateLog</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>DeleteLog</code></td>
</tr>
</tbody>
</table>

### log-content

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSPECT</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>READ</td>
<td><code>INSPECT +</code></td>
<td><code>INSPECT +</code></td>
<td>none</td>
</tr>
<tr>
<td>USE</td>
<td><code>READ +</code></td>
<td><code>READ +</code></td>
<td>none</td>
</tr>
<tr>
<td>MANAGE</td>
<td><code>READ +</code></td>
<td><code>READ +</code></td>
<td>none</td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type. For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListSearchLogs</td>
<td>LOG_CONTENT_READ</td>
</tr>
<tr>
<td>ListLogs</td>
<td>LOG_GROUP_INSPECT</td>
</tr>
<tr>
<td>GetLog</td>
<td>LOG_GROUP_READ</td>
</tr>
<tr>
<td>UpdateLog</td>
<td>LOG_GROUP_UPDATE</td>
</tr>
<tr>
<td>CreateLog</td>
<td>LOG_GROUP_CREATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>DeleteLog</td>
<td>LOG_GROUP_DELETE</td>
</tr>
<tr>
<td>ListLogGroups</td>
<td>LOG_GROUP_INSPECT</td>
</tr>
<tr>
<td>GetLogGroup</td>
<td>LOG_GROUP_READ</td>
</tr>
<tr>
<td>UpdateLogGroup</td>
<td>LOG_GROUP_UPDATE</td>
</tr>
<tr>
<td>CreateLogGroup</td>
<td>LOG_GROUP_CREATE</td>
</tr>
<tr>
<td>DeleteLogGroup</td>
<td>LOG_GROUP_DELETE</td>
</tr>
<tr>
<td>ChangeLogGroupCompartment</td>
<td>LOG_GROUP_UPDATE</td>
</tr>
</tbody>
</table>

**Details for Logging Analytics**

This topic covers details for writing policies to control access to the Logging Analytics service.

**Resource-Types**

**Individual Resource-Types**

loganalytics-config-work-request
loganalytics-entity
loganalytics-entity-type
loganalytics-field
loganalytics-label
loganalytics-lifecycle
loganalytics-log-group
loganalytics-lookup
loganalytics-object-collection-rule
loganalytics-ondemand-upload
loganalytics-parser
loganalytics-query
loganalytics-queryjob-work-request
loganalytics-scheduled-task
loganalytics-source
loganalytics-storage
loganalytics-storage-work-request

**Aggregate Resource-Types**

The loganalytics-features-family aggregate resource-type covers these individual resource-types (resource kinds that are not modeled as resources; that is, resource kinds that do not belong to a compartment):

loganalytics-entity-type
loganalytics-field
loganalytics-label
loganalytics-lifecycle
loganalytics-lookup
loganalytics-ondemand-upload
loganalytics-parser
loganalytics-query
loganalytics-source
loganalytics-storage
loganalytics-storage-work-request

The loganalytics-resources-family aggregate resource-type covers these individual resource-types (resource kinds that are modeled as resources; that is, resource kinds that belong to a compartment):

loganalytics-config-work-request
loganalytics-entity
loganalytics-log-group
loganalytics-object-collection-rule
loganalytics-queryjob-work-request
loganalytics-scheduled-task
loganalytics-storage-work-request

Comments

A policy that uses <verb> loganalytics-features-family or <verb> loganalytics-resources-family is equivalent to writing one with a separate <verb> <individual resource-type> statement for each of the individual resource-types in the family.

See the table in Permissions Required for Each API Operation on page 2308 for details of the API operations covered by each verb, for each individual resource-type.

Supported Variables

Only the general variables are supported (see General Variables for All Requests on page 2169).

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

<table>
<thead>
<tr>
<th>loganalytics-config-work-request</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verbs</strong></td>
</tr>
<tr>
<td>inspect</td>
</tr>
<tr>
<td>read</td>
</tr>
<tr>
<td>use</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Verbs</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>manage</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**loganalytics-entity**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_ENTITY_INSPECT</td>
<td>ListLogAnalyticsEntitiesSummary</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListEntityAssociations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListLogAnalyticsEntities</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>LOG_ANALYTICS_ENTITY_READ</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>AddEntityAssociation</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_CREATE</td>
<td>CreateLogAnalyticsEntityCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_DELETE</td>
<td>DeleteLogAnalyticsEntity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_MOVE</td>
<td>UpdateLogAnalyticsEntity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_UPDATE</td>
<td>UpdateLogAnalyticsEntity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RemoveEntityAssociations</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**loganalytics-entity-type**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_READ</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>CreateLogAnalyticsEntityType</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_TYPE_CREATE</td>
<td>CreateLogAnalyticsEntityType</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_TYPE_DELETE</td>
<td>DeleteLogAnalyticsEntityType</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ENTITY_TYPE_UPDATE</td>
<td>UpdateLogAnalyticsEntityType</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### loganalytics-field

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_FIELD_INSPECT  &lt;br&gt; ListFieldsSummary &lt;br&gt; ListFields</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +  &lt;br&gt; LOG_ANALYTICS_FIELD_READ</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ + &lt;br&gt; LOG_ANALYTICS_FIELD_CREATE &lt;br&gt; LOG_ANALYTICS_FIELD_DELETE &lt;br&gt; LOG_ANALYTICS_FIELD_UPDATE</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +  &lt;br&gt; no extra</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

### loganalytics-label

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_LABEL_INSPECT  &lt;br&gt; ListLabelPriorities &lt;br&gt; ListLabels</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +  &lt;br&gt; BatchGetBasicInfo &lt;br&gt; ListLabelSourceDetails</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ + &lt;br&gt; LOG_ANALYTICS_LABEL_CREATE &lt;br&gt; LOG_ANALYTICS_LABEL_DELETE &lt;br&gt; LOG_ANALYTICS_LABEL_UPDATE</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +  &lt;br&gt; no extra</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

### loganalytics-lifecycle

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_LIFECYCLE_INSPECT  &lt;br&gt; ListNamespaces</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +  &lt;br&gt; GetNamespace</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>OffboardNamespace</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LIFECYCLE_HOMEPAGE_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LIFECYCLE_OFFBOARD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LIFECYCLE_ONBOARD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### loganalytics-log-group

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_LOG_GROUP_INSPECT</td>
<td>ListLogAnalyticsLogGroups</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetLogAnalyticsLogGroup</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>LOG_ANALYTICS_LOG_GROUP_READ</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>ChangeLogAnalyticsLogGroupCompartmennt</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOG_GROUP_CREATE</td>
<td>CreateLogAnalyticsLogGroup</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOG_GROUP_UPDATE</td>
<td>UpdateLogAnalyticsLogGroup</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOG_GROUP_UPLOAD_LOGS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DeleteLogAnalyticsLogGroup</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOG_GROUP_DELETE_LOGS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### loganalytics-lookup

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_LOOKUP_INSPECT</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>LOG_ANALYTICS_LOOKUP_READ</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>RegisterLookups</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOOKUP_CREATE</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOOKUP_DELETE</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_LOOKUP_UPDATE</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### loganalytics-object-collection-rule

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inspect</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetLogAnalyticsObjectCollectionRulesObjectCollectionRules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>use</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ +</td>
<td></td>
<td>ChangeLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td><strong>manage</strong></td>
<td>USE +</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ChangeLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MoveLogAnalyticsObjectCollectionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>use</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>manage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### loganalytics-ondemand-upload

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inspect</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetUpload</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ONDEMANDUPLOAD_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>use</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ +</td>
<td></td>
<td>ValidateFile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ONDEMANDUPLOAD_CREATING</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DeleteUploadWarning</td>
<td>DeleteUpload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(also needs manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>loganalytics-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>log-group, read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>loganalytics-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>query, and read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>compartments)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteUploadFile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(also needs manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>loganalytics-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>log-group, read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>loganalytics-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>query, and read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>compartments)</td>
<td></td>
</tr>
</tbody>
</table>

**loganalytics-parser**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSPECT</td>
<td>ListParserSummary</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListParserMetaPlugins</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListParsers</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>READ +</td>
<td>ExtractStructuredLogFieldPaths</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtractStructuredLogHeaderPaths</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetParser</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListParserFunctions</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TestParser</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>DeleteParser</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_PARSER_CREATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_PARSER_UPDATE</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>no extra</td>
<td></td>
</tr>
</tbody>
</table>

**loganalytics-query**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>INSPECT</td>
<td>LOG_ANALYTICS_QUERY_INSPECT</td>
<td>Filter, ParseQuery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(both also need read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>loganalytics-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>lifecycle)</td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>none</td>
<td>Export (also needs read loganalytics-lifecycle, read loganalytics-log-group, and read compartments)</td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_QUERY_VIEW</td>
<td></td>
<td>GetQueryResult (also needs read loganalytics-lifecycle and read loganalytics-queryjob-work-request)</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
<td>Suggest (also needs read loganalytics-lifecycle and read compartments)</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
<td>Query (also needs read loganalytics-lifecycle, read loganalytics-log-group, read loganalytics-queryjob-work-request, and read compartments)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>

**loganalytics-queryjob-work-request**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_INSPECT</td>
<td></td>
<td>ListQueryWorkRequests (also needs read loganalytics-lifecycle)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>none</td>
<td>GetQueryResult (also needs read loganalytics-lifecycle and read loganalytics-query) GetQueryWorkRequest, PutQueryWorkRequestBackground (both also need read loganalytics-lifecycle) Query (also needs read loganalytics-lifecycle, read loganalytics-log-group, read loganalytics-query, and read compartments) CancelQueryWorkRequest (also needs read loganalytics-lifecycle)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>none</td>
<td>Clean (also needs read loganalytics-lifecycle)</td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>no extra</td>
</tr>
</tbody>
</table>

**loganalytics-scheduled-task**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_INSPECT none LOG_ANALYTICS_PURGETASK_INSPECT LOG_ANALYTICS_SAVEDSEARCHTASK_INSPECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>Clean none</td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_READ LOG_ANALYTICS_PURGETASK_READ LOG_ANALYTICS_SAVEDSEARCHTASK_READ</td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>ChangeScheduledTaskCompartment for taskType ACCELERATION, ACCELERATION_MAINTENANCE, or SAVED_SEARCH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_CREATE</td>
<td>CreateScheduledTask for taskType ACCELERATION, ACCELERATION_MAINTENANCE, or SAVED_SEARCH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_DELETE</td>
<td>DeleteScheduledTask for taskType ACCELERATION, ACCELERATION_MAINTENANCE, or SAVED_SEARCH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_MOVE</td>
<td>UpdateScheduledTask for taskType ACCELERATION, ACCELERATION_MAINTENANCE, or SAVED_SEARCH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>manage</td>
<td>ChangeScheduledTaskCompartment for taskType PURGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USE +</td>
<td>CreateScheduledTask for taskType PURGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_PURGETASK_CREATE</td>
<td>DeleteScheduledTask for taskType PURGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_PURGETASK_DELETE</td>
<td>UpdateScheduledTask for taskType PURGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_PURGETASK_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG_ANALYTICS_PURGETASK_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>loganalytics-source</td>
<td>inspect</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetAssociationSummary</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListAssociatedEntities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListEntitySourceAssociations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListMetaSourceTypes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListSourceLabelOperators</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListSourceMetaFunctions</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListSources</td>
<td></td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetColumnNames</td>
<td>ExportCustomContent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also needs read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-field,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>read loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>label, and read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>parser)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ValidateSource</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ValidateSource</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ValidateSource</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ExtendedFieldDetails</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>DeleteAssociations</td>
<td>ImportCustomContent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also needs use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-field,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>use loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>label, and use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>parser)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| loganalytics-storage

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>LOG_ANALYTICS_STORAGE_INSPECT</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetStorage</td>
<td>GetStorageWorkRequest,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ListStorageWorkRequestErrors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-storage-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>work-request)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ListStorageWorkRequests</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also need inspect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-storage-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>work-request)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>RecallArchivedData,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ReleaseRecalledData</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>loganalytics-storage-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>work-request)</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 2307
## IAM

### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>DisableArchiving</td>
<td>PurgeStorageData</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_STORAGE_ARCHIVE_DISABLE</td>
<td>(also needs manage loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_STORAGE_ARCHIVE_ENABLE</td>
<td>storage-work-request)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_STORAGE_PURGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_STORAGE_UPDATE</td>
<td></td>
</tr>
</tbody>
</table>

### loganalytics-storage-work-request

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>LOG_ANALYTICS_STORAGE_WORK_REQUEST_INSPECT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG_ANALYTICS_STORAGE_WORK_REQUEST_READ</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>none</td>
<td>GetStorageWorkRequest,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ListStorageWorkRequestErrors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need read loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>storage)</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>none</td>
<td>PurgeStorageData</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(also needs manage loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>storage-work-request)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RecallArchivedData,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ReleaseRecalledData</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(both also need use loganalytics-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>storage)</td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in alphabetical order.

For information about permissions, see [Permissions](#) on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddEntityAssociation</td>
<td>LOG_ANALYTICS_ENTITY_UPDATE</td>
</tr>
<tr>
<td>BatchGetBasicInfo</td>
<td>LOG_ANALYTICS_LABEL_READ</td>
</tr>
<tr>
<td>CancelQueryWorkRequest</td>
<td>LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_DELETE and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>ChangeLogAnalyticsEntityCompartment</td>
<td>LOG_ANALYTICS_ENTITY_MOVE</td>
</tr>
<tr>
<td>ChangeLogAnalyticsLogGroupCompartment</td>
<td>LOG_ANALYTICS_LOG_GROUP_UPDATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>ChangeLogAnalyticsObjectCollectionRuleCompartment</td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_MOVE on both source (current) and target (new) compartments.</td>
</tr>
<tr>
<td>ChangeScheduledTaskCompartment</td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_MOVE or LOG_ANALYTICS_ACCELERATIONTASK_MOVE or LOG_ANALYTICS_PURGETASK_MOVE</td>
</tr>
<tr>
<td>Clean</td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_READ</td>
</tr>
<tr>
<td>CreateLogAnalyticsEntity</td>
<td>LOG_ANALYTICS_ENTITY_CREATE</td>
</tr>
<tr>
<td>CreateLogAnalyticsEntityType</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_CREATE</td>
</tr>
<tr>
<td>CreateLogAnalyticsLogGroup</td>
<td>LOG_ANALYTICS_LOG_GROUP_CREATE</td>
</tr>
<tr>
<td>CreateLogAnalyticsObjectCollectionRule</td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_CREATE and LOG_ANALYTICS_SOURCE_READ and LOG_ANALYTICS_LOG_GROUP_UPLOAD_LOGS and LOG_ANALYTICS_ENTITY_UPLOAD_LOGS</td>
</tr>
<tr>
<td>CreateScheduledTask</td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_CREATE or LOG_ANALYTICS_ACCELERATIONTASK_CREATE or LOG_ANALYTICS_PURGETASK_CREATE</td>
</tr>
<tr>
<td>DeleteAssociations</td>
<td>LOG_ANALYTICS_SOURCE_ENTITY_DISASSOC</td>
</tr>
<tr>
<td>DeleteField</td>
<td>LOG_ANALYTICS_FIELD_DELETE</td>
</tr>
<tr>
<td>DeleteLabel</td>
<td>LOG_ANALYTICS_LABEL_DELETE</td>
</tr>
<tr>
<td>DeleteLogAnalyticsEntity</td>
<td>LOG_ANALYTICS_ENTITY_DELETE</td>
</tr>
<tr>
<td>DeleteLogAnalyticsEntityType</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_DELETE</td>
</tr>
<tr>
<td>DeleteLogAnalyticsLogGroup</td>
<td>LOG_ANALYTICS_LOG_GROUP_DELETE_LOGS</td>
</tr>
<tr>
<td>DeleteLogAnalyticsObjectCollectionRule</td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_DELETE</td>
</tr>
<tr>
<td>DeleteParser</td>
<td>LOG_ANALYTICS_PARSER_DELETE</td>
</tr>
<tr>
<td>DeleteScheduledTask</td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_DELETE or LOG_ANALYTICS_ACCELERATIONTASK_DELETE or LOG_ANALYTICS_PURGETASK_DELETE</td>
</tr>
<tr>
<td>DeleteSource</td>
<td>LOG_ANALYTICS_SOURCE_DELETE</td>
</tr>
<tr>
<td>DeleteUpload</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_DELETE and LOG_ANALYTICS_LOG_GROUP_DELETE_LOGS and LOG_ANALYTICS_QUERY_VIEW and Compartment Permissions (COMPARTMENT_READ)</td>
</tr>
<tr>
<td>DeleteUploadFile</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_DELETE and LOG_ANALYTICS_LOG_GROUP_DELETE_LOGS and LOG_ANALYTICS_QUERY_VIEW and Compartment Permissions (COMPARTMENT_READ)</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DeleteUploadWarning</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_DELETE</td>
</tr>
<tr>
<td>DisableArchiving</td>
<td>LOG_ANALYTICS_STORAGE_ARCHIVE_DISABLE</td>
</tr>
<tr>
<td>EnableArchiving</td>
<td>LOG_ANALYTICS_STORAGE_ARCHIVE_ENABLE</td>
</tr>
<tr>
<td>EstimatePurgeDataSize</td>
<td>LOG_ANALYTICS_STORAGE_UPDATE</td>
</tr>
<tr>
<td>Export</td>
<td>LOG_ANALYTICS_QUERY_VIEW and READ_COMPARTMENTS and LOGANALYTICS_LOG_GROUP_READ_LOGS and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>ExportCustomContent</td>
<td>LOG_ANALYTICS_SOURCE_READ or LOG_ANALYTICS_PARSER_READ or LOG_ANALYTICS_FIELD_READ or LOG_ANALYTICS_LABEL_READ or LOG_ANALYTICS_METRIC_READ</td>
</tr>
<tr>
<td>ExtractStructuredLogFieldPaths</td>
<td>LOG_ANALYTICS_PARSER_READ</td>
</tr>
<tr>
<td>ExtractStructuredLogHeaderPaths</td>
<td>LOG_ANALYTICS_PARSER_READ</td>
</tr>
<tr>
<td>Filter</td>
<td>LOG_ANALYTICS_QUERY_INSPECT and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>GetAssociationSummary</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>GetColumnNames</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>GetConfigWorkRequest</td>
<td>LOG_ANALYTICS_CONFIG_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>GetField</td>
<td>LOG_ANALYTICS_FIELD_READ</td>
</tr>
<tr>
<td>GetFieldsSummary</td>
<td>LOG_ANALYTICS_FIELD_INSPECT</td>
</tr>
<tr>
<td>GetLabel</td>
<td>LOG_ANALYTICS_LABEL_READ</td>
</tr>
<tr>
<td>GetLabelSummary</td>
<td>LOG_ANALYTICS_LABEL_INSPECT</td>
</tr>
<tr>
<td>GetLogAnalyticsEntitiesSummary</td>
<td>LOG_ANALYTICS_ENTITY_INSPECT</td>
</tr>
<tr>
<td>GetLogAnalyticsEntity</td>
<td>LOG_ANALYTICS_ENTITY_READ</td>
</tr>
<tr>
<td>GetLogAnalyticsEntityType</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_READ</td>
</tr>
<tr>
<td>GetLogAnalyticsLogGroup</td>
<td>LOG_ANALYTICS_LOG_GROUP_READ</td>
</tr>
<tr>
<td>GetLogAnalyticsLogGroupsSummary</td>
<td>LOG_ANALYTICS_LOG_GROUP_INSPECT</td>
</tr>
<tr>
<td>GetLogAnalyticsObjectCollectionRule</td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_READ and LOG_ANALYTICS_LOG_GROUP_INSPECT and LOG_ANALYTICS_SOURCE_INSPECT and LOG_ANALYTICS_ENTITY_INSPECT</td>
</tr>
<tr>
<td>GetNamespace</td>
<td>LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>GetParser</td>
<td>LOG_ANALYTICS_PARSER_READ</td>
</tr>
<tr>
<td>GetParserSummary</td>
<td>LOG_ANALYTICS_PARSER_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GetQueryResult</td>
<td>LOG_ANALYTICS_QUERY_VIEW and LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_READ and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>GetQueryWorkRequest</td>
<td>LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_READ and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>GetScheduledTask</td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_READ or LOG_ANALYTICS_ACCELERATIONTASK_READ or LOG_ANALYTICS_PURGETASK_READ</td>
</tr>
<tr>
<td>GetSource</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>GetSourceSummary</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>GetStorage</td>
<td>LOG_ANALYTICS_STORAGE_READ</td>
</tr>
<tr>
<td>GetStorageUsage</td>
<td>LOG_ANALYTICS_STORAGE_READ</td>
</tr>
<tr>
<td>GetStorageWorkRequest</td>
<td>LOG_ANALYTICS_STORAGE_WORK_REQUEST_READ and LOG_ANALYTICS_STORAGE_READ</td>
</tr>
<tr>
<td>GetUpload</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_READ</td>
</tr>
<tr>
<td>ImportCustomContent</td>
<td>LOG_ANALYTICS_SOURCE_CREATE or LOG_ANALYTICS_PARSER_CREATE or LOG_ANALYTICS_FIELD_CREATE or LOG_ANALYTICS_LABEL_CREATE or LOG_ANALYTICS_METRIC_CREATE or LOG_ANALYTICS_SOURCE_UPDATE or LOG_ANALYTICS_PARSER_UPDATE or LOG_ANALYTICS_FIELD_UPDATE or LOG_ANALYTICS_LABEL_UPDATE or LOG_ANALYTICS_METRIC_UPDATE</td>
</tr>
<tr>
<td>ListAssociatedEntities</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>ListConfigWorkRequests</td>
<td>LOG_ANALYTICS_CONFIG_WORK_REQUEST_INSPECT</td>
</tr>
<tr>
<td>ListEntityAssociations</td>
<td>LOG_ANALYTICS_ENTITY_INSPECT</td>
</tr>
<tr>
<td>ListEntitySourceAssociations</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>ListFields</td>
<td>LOG_ANALYTICS_FIELD_INSPECT</td>
</tr>
<tr>
<td>ListLabelPriorities</td>
<td>LOG_ANALYTICS_LABEL_INSPECT</td>
</tr>
<tr>
<td>ListLabels</td>
<td>LOG_ANALYTICS_LABEL_INSPECT</td>
</tr>
<tr>
<td>ListLabelSourceDetails</td>
<td>LOG_ANALYTICS_LABEL_READ</td>
</tr>
<tr>
<td>ListLogAnalyticsEntities</td>
<td>LOG_ANALYTICS_ENTITY_INSPECT</td>
</tr>
<tr>
<td>ListLogAnalyticsEntityType</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_INSPECT</td>
</tr>
<tr>
<td>ListLogAnalyticsLogGroups</td>
<td>LOG_ANALYTICS_LOG_GROUP_INSPECT</td>
</tr>
<tr>
<td>ListLogAnalyticsObjectCollectionRules</td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_INSPECT</td>
</tr>
<tr>
<td>ListMetaSourceType</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ListNamespaces</td>
<td>LOG_ANALYTICS_LIFECYCLE_INSPECT</td>
</tr>
<tr>
<td>ListParserFunctions</td>
<td>LOG_ANALYTICS_PARSER_READ</td>
</tr>
<tr>
<td>ListParserMetaPlugins</td>
<td>LOG_ANALYTICS_PARSER_INSPECT</td>
</tr>
<tr>
<td>ListParsers</td>
<td>LOG_ANALYTICS_PARSER_INSPECT</td>
</tr>
<tr>
<td>ListQueryWorkRequests</td>
<td>LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_INSPECT and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>ListScheduledTasks</td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_INSPECT or LOG_ANALYTICS_ACCELERATIONTASK_INSPECT or LOG_ANALYTICS_PURGETASK_INSPECT</td>
</tr>
<tr>
<td>ListSourceAssociations</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>ListSourceExtendedFieldDefinitions</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>ListSourceLabelOperators</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>ListSourceMetaFunctions</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>ListSourcePatterns</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>ListSources</td>
<td>LOG_ANALYTICS_SOURCE_INSPECT</td>
</tr>
<tr>
<td>ListStorageWorkRequestErrors</td>
<td>LOG_ANALYTICS_STORAGE_WORK_REQUEST_READ and LOG_ANALYTICS_STORAGE_READ</td>
</tr>
<tr>
<td>ListStorageWorkRequests</td>
<td>LOG_ANALYTICS_STORAGE_WORK_REQUEST_INSPECT and LOG_ANALYTICS_STORAGE_READ</td>
</tr>
<tr>
<td>ListSupportedCharEncodings</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_INSPECT</td>
</tr>
<tr>
<td>ListSupportedTimezones</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_INSPECT</td>
</tr>
<tr>
<td>ListUploadFiles</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_READ and LOG_ANALYTICS_LOG_GROUP_READ</td>
</tr>
<tr>
<td>ListUploads</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_INSPECT</td>
</tr>
<tr>
<td>ListUploadWarnings</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_READ</td>
</tr>
<tr>
<td>OffboardNamespace</td>
<td>LOG_ANALYTICS_LIFECYCLE_OFFBOARD</td>
</tr>
<tr>
<td>OnboardNamespace</td>
<td>LOG_ANALYTICS_LIFECYCLE_ONBOARD</td>
</tr>
<tr>
<td>ParseQuery</td>
<td>LOG_ANALYTICS_QUERY_INSPECT and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>PurgeStorageData</td>
<td>LOG_ANALYTICS_STORAGE_PURGE and LOG_ANALYTICS_STORAGE_WORK_REQUEST_CREATE</td>
</tr>
<tr>
<td>PutQueryWorkRequestBackground</td>
<td>LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_READ and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Query</td>
<td>LOG_ANALYTICS_QUERY_VIEW and READ_COMPARTMENTS and LOGANALYTICS_LOG_GROUP_READ_LOGS and LOG_ANALYTICS_LIFECYCLE_READ and LOG_ANALYTICS_QUERYJOB_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>RecallArchivedData</td>
<td>LOG_ANALYTICS_STORAGE_ARCHIVE_RECALL and LOG_ANALYTICS_STORAGE_WORK_REQUEST_CREATE</td>
</tr>
<tr>
<td>RegisterLookup</td>
<td>LOG_ANALYTICS_LOOKUP_CREATE</td>
</tr>
<tr>
<td>ReleaseRecalledData</td>
<td>LOG_ANALYTICS_STORAGE_ARCHIVE_RELEASE and LOG_ANALYTICS_STORAGE_WORK_REQUEST_CREATE</td>
</tr>
<tr>
<td>RemoveEntityAssociations</td>
<td>LOG_ANALYTICS_ENTITY_UPDATE</td>
</tr>
<tr>
<td>Run</td>
<td>LOG_ANALYTICS_ACCELERATIONTASK_READ</td>
</tr>
<tr>
<td>Suggest</td>
<td>LOG_ANALYTICS_QUERY_VIEW and READ_COMPARTMENTS and LOG_ANALYTICS_LIFECYCLE_READ</td>
</tr>
<tr>
<td>TestParser</td>
<td>LOG_ANALYTICS_PARSER_READ</td>
</tr>
<tr>
<td>UpdateLogAnalyticsEntity</td>
<td>LOG_ANALYTICS_ENTITY_UPDATE</td>
</tr>
<tr>
<td>UpdateLogAnalyticsEntityType</td>
<td>LOG_ANALYTICS_ENTITY_TYPE_UPDATE</td>
</tr>
<tr>
<td>UpdateLogAnalyticsLogGroup</td>
<td>LOG_ANALYTICS_LOG_GROUP_UPDATE</td>
</tr>
<tr>
<td>UpdateLogAnalyticsObjectCollectionRule</td>
<td>LOG_ANALYTICS_OBJECT_COLLECTION_RULE_UPDATE and LOG_ANALYTICS_SOURCE_READ and LOG_ANALYTICS_LOG_GROUP_UPLOAD_LOGS and LOG_ANALYTICS_ENTITY_UPLOAD_LOGS</td>
</tr>
<tr>
<td>UpdateScheduledTask</td>
<td>LOG_ANALYTICS_SAVEDSEARCHTASK_UPDATE or LOG_ANALYTICS_ACCELERATIONTASK_UPDATE or LOG_ANALYTICS_PURGETASK_UPDATE</td>
</tr>
<tr>
<td>UpdateStorage</td>
<td>LOG_ANALYTICS_STORAGE_UPDATE</td>
</tr>
<tr>
<td>UploadLogFile</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_CREATE and LOG_ANALYTICS_LOG_GROUP_UPLOAD_LOGS and LOG_ANALYTICS_SOURCE_READ and LOG_ANALYTICS_ENTITY_UPLOAD_LOGS</td>
</tr>
<tr>
<td>UpsertAssociations</td>
<td>LOG_ANALYTICS_SOURCE_ENTITY_ASSOC</td>
</tr>
<tr>
<td>UpsertField</td>
<td>LOG_ANALYTICS_FIELD_CREATE or LOG_ANALYTICS_FIELD_UPDATE</td>
</tr>
<tr>
<td>UpsertLabel</td>
<td>LOG_ANALYTICS_LABEL_CREATE or LOG_ANALYTICS_LABEL_UPDATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UpsertParser</td>
<td>LOG_ANALYTICS_PARSER_CREATE or LOG_ANALYTICS_PARSER_UPDATE</td>
</tr>
<tr>
<td>UpsertSource</td>
<td>LOG_ANALYTICS_SOURCE_CREATE or LOG_ANALYTICS_SOURCE_UPDATE</td>
</tr>
<tr>
<td>ValidateAssociationParameters</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>ValidateFile</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_CREATE</td>
</tr>
<tr>
<td>ValidateSource</td>
<td>LOG_ANALYTICS_SOURCE_CREATE or LOG_ANALYTICS_SOURCE_UPDATE</td>
</tr>
<tr>
<td>ValidateSourceExtendedFieldDetails</td>
<td>LOG_ANALYTICS_SOURCE_READ</td>
</tr>
<tr>
<td>ValidateSourceMapping</td>
<td>LOG_ANALYTICS_ONDEMAND_UPLOAD_CREATE</td>
</tr>
</tbody>
</table>

**Details for Management Agent**

This topic covers details for writing policies to control access to the Management Agent service.

**Resource-Types**

management-agents

management-agent-install-keys

**Supported Variables**

Only the general variables are supported (see General Variables for All Requests on page 2169).

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

**management-agents**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>MGMT_AGENT_INSPECT</td>
<td>ListManagementAgentPlugin</td>
<td>ListManagementAgents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestErrors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestLogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequests</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>MGMT_AGENT_READ</td>
<td>GetManagementAgent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>MGMT_AGENT_UPDATE</td>
<td>UpdateManagementAgent</td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE + MGMT_AGENT_CREATE</td>
<td>DeleteManagementAgent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeployPlugins</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteWorkRequest</td>
<td></td>
</tr>
</tbody>
</table>

management-agent-install-keys

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>MGMT_AGENT_INSTALL_KEY_INSPECT</td>
<td>GetManagementAgentInstallKey</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + MGMT_AGENT_INSTALL_KEY_READ</td>
<td>GetManagementAgentInstallKeyContent</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ + MGMT_AGENT_INSTALL_KEY_UPDATE</td>
<td>GetManagementAgentInstallKey</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE + MGMT_AGENT_INSTALL_KEY_CREATE</td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>

Permissions Required for Each API Operation

The following table lists the API operations in alphabetical order.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateManagementAgentInstallKey</td>
<td>MGMT_AGENT_INSTALL_KEY_CREATE</td>
</tr>
<tr>
<td>DeleteManagementAgent</td>
<td>MGMT_AGENT_DELETE</td>
</tr>
<tr>
<td>DeleteManagementAgentInstallKey</td>
<td>MGMT_AGENT_INSTALL_KEY_DELETE</td>
</tr>
<tr>
<td>DeleteWorkRequest</td>
<td>MGMT_AGENT_DELETE</td>
</tr>
<tr>
<td>DeployPlugins</td>
<td>MGMT_AGENT_DEPLOY_PLUGIN_CREATE</td>
</tr>
<tr>
<td>GetManagementAgent</td>
<td>MGMT_AGENT_READ</td>
</tr>
<tr>
<td>GetManagementAgentInstallKey</td>
<td>MGMT_AGENT_INSTALL_KEY_READ</td>
</tr>
<tr>
<td>GetManagementAgentInstallKeyContent</td>
<td>MGMT_AGENT_INSTALL_KEY_READ</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>MGMT_AGENT_READ</td>
</tr>
<tr>
<td>ListManagementAgentInstallKeys</td>
<td>MGMT_AGENT_INSTALL_KEY_INSPECT</td>
</tr>
<tr>
<td>ListManagementAgentPlugins</td>
<td>MGMT_AGENT_INSPECT</td>
</tr>
<tr>
<td>ListManagementAgents</td>
<td>MGMT_AGENT_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>MGMT_AGENT_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>MGMT_AGENT_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>MGMT_AGENT_INSPECT</td>
</tr>
<tr>
<td>UpdateManagementAgent</td>
<td>MGMT_AGENT_UPDATE</td>
</tr>
<tr>
<td>UpdateManagementAgentInstallKey</td>
<td>MGMT_AGENT_INSTALL_KEY_UPDATE</td>
</tr>
</tbody>
</table>

For more details and examples, see Set Up Oracle Cloud Infrastructure for Management Agents.

Details for Management Dashboard

This topic covers details for writing policies to control access to Management Dashboard.

Resource-Types

Individual Resource-Types

- management-dashboard
- management-saved-search

Aggregate Resource-Type

- management-dashboard-family

Comments

A policy that uses `<verb>` management-dashboard-family is equivalent to writing one with a separate `<verb>` `<individual resource-type>` statement for each of the individual resource-types. The resource-type management-dashboard allows a user group to work with dashboards while the resource-type management-saved-search allows a user group to work with saved searches (widgets) that are displayed in dashboards.

See the table in Details for Verb + Resource-Type Combinations on page 2316 for details of the API operations covered by each verb, for each individual resource-type included in management-dashboard-family.

Supported Variables

Only the general variables are supported (see General Variables for All Requests on page 2169).

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

management-dashboard

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>MANAGEMENT_DASHBOARD_INSPECT</td>
<td>ListManagementDashboards</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>MANAGEMENT_DASHBOARD_READ +</td>
<td>ExportDashboard</td>
<td>none</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 2316
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateManagementDashboard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_DASHBOARD_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeManagementDashboardsCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_DASHBOARD_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_DASHBOARD_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_DASHBOARD_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**management-saved-search**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>MANAGEMENT_SAVED_SEARCH_INSPECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ListManagementSavedSearches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>no extra none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_SAVED_SEARCH_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateManagementSavedSearch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_SAVED_SEARCH_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeManagementSavedSearchesCompart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_SAVED_SEARCH_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_SAVED_SEARCH_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MANAGEMENT_SAVED_SEARCH_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in alphabetical order.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChangeManagementDashboardsCompartment</td>
<td>MANAGEMENT_DASHBOARD_MOVE</td>
</tr>
<tr>
<td>ChangeManagementSavedSearchesCompartment</td>
<td>MANAGEMENT_SAVED_SEARCH_MOVE</td>
</tr>
<tr>
<td>CreateManagementDashboard</td>
<td>MANAGEMENT_DASHBOARD_CREATE</td>
</tr>
<tr>
<td>CreateManagementSavedSearch</td>
<td>MANAGEMENT_SAVED_SEARCH_CREATE</td>
</tr>
<tr>
<td>DeleteManagementDashboard</td>
<td>MANAGEMENT_DASHBOARD_DELETE</td>
</tr>
<tr>
<td>DeleteManagementSavedSearch</td>
<td>MANAGEMENT_SAVED_SEARCH_DELETE</td>
</tr>
<tr>
<td>ExportDashboard</td>
<td>MANAGEMENT_DASHBOARD_READ</td>
</tr>
<tr>
<td>GetManagementDashboard</td>
<td>MANAGEMENT_DASHBOARD_INSPECT</td>
</tr>
<tr>
<td>GetManagementSavedSearch</td>
<td>MANAGEMENT_SAVED_SEARCH_INSPECT</td>
</tr>
<tr>
<td>ImportDashboard</td>
<td>MANAGEMENT_DASHBOARD_CREATE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>ListManagementDashboards</td>
<td>MANAGEMENT_DASHBOARD_INSPECT</td>
</tr>
<tr>
<td>ListManagementSavedSearches</td>
<td>MANAGEMENT_SAVED_SEARCH_INSPECT</td>
</tr>
<tr>
<td>UpdateManagementDashboard</td>
<td>MANAGEMENT_DASHBOARD_UPDATE</td>
</tr>
<tr>
<td>UpdateManagementSavedSearch</td>
<td>MANAGEMENT_SAVED_SEARCH_UPDATE</td>
</tr>
</tbody>
</table>

**Example Policies**

This section provides example policies for use with Management Dashboard.

**Dashboard Policies**

Here are examples of policy statements that authorize access to dashboards (management-dashboard resource-type):

- To allow a user group to list the dashboards in a compartment, use the inspect verb:

  ```
  Allow group dashboard-users to inspect management-dashboard in compartment myCompartment1
  ```

- To allow a user group to list dashboards and obtain details regarding the dashboards in a compartment, use the read verb:

  ```
  Allow group dashboard-users to read management-dashboard in compartment myCompartment1
  ```

- To allow a group of administrators to list dashboards, obtain details regarding dashboards, and update the dashboards in a compartment, use the use verb:

  ```
  Allow group dashboard-admins to use management-dashboard in compartment myCompartment1
  ```

- To allow a group of administrators to list dashboards, obtain details regarding dashboards, update dashboards, and manage (create, move, and delete) the dashboards in a compartment, use the manage verb:

  ```
  Allow group dashboard-admins to manage management-dashboard in compartment myCompartment1
  ```

**Saved Search Policies**

Here are examples of policy statements that authorize access to saved searches (management-saved-search resource-type):

- To allow a user group to list the saved searches in a compartment, use the inspect verb:

  ```
  Allow group saved-search-users to inspect management-saved-search in compartment myCompartment1
  ```

- To allow a user group to list saved searches and obtain details regarding the saved searches in a compartment, use the read verb:

  ```
  Allow group saved-search-users to read management-saved-search in compartment myCompartment1
  ```
- To allow a group of administrators to list saved searches, obtain details regarding saved searches, update the saved searches in a compartment, use the use verb:

```
Allow group saved-search-admins to use management-saved-search in compartment myCompartment1
```

- To allow a group of administrators to list saved searches, obtain details regarding saved searches, update saved searches, and manage (create, move, and delete) the saved searches in a compartment, use the manage verb:

```
Allow group saved-search-admins to manage management-saved-search in compartment myCompartment1
```

**Aggregate Policies**

Here's an example of a policy that simultaneously authorizes access to both dashboards and saved searches by using the aggregate `management-dashboard-family` resource-type. In this example, the inspect verb is used to allow a user group to list both the dashboards and saved searches in a compartment:

```
Allow group dashboard-family-admins to inspect management-dashboard-family in compartment myCompartment1
```

Similarly, the other Oracle Cloud Infrastructure verbs can be used to allow user groups to perform the corresponding tasks for dashboards and saved searches in one policy.

**Details for the Marketplace Service**

This topic covers details for writing policies to control access to the Marketplace service.

**Individual Resource-Type**

`marketplace-listings`

**Supported Variables**

Marketplace supports all the general variables, plus the ones listed here. Specifically, you can use the variables listed here when writing policies that grant read, use, and manage verbs. You cannot use them with the inspect verb. For more information about general variables supported by Oracle Cloud Infrastructure services, see General Variables for All Requests on page 2169.

<table>
<thead>
<tr>
<th>Resource-Type</th>
<th>Variable</th>
<th>Variable Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>marketplace-listings</td>
<td>listing.id</td>
<td>String</td>
<td>Use this variable to control whether to return a specific listing (based on the given listing ID) in response to a request.</td>
</tr>
<tr>
<td>marketplace-listings</td>
<td>listing.publisher.id</td>
<td>String</td>
<td>Use this variable to control whether to return only listings from a specific publisher (based on the given publisher ID) in response to a request.</td>
</tr>
</tbody>
</table>

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.
For example, the `use` verb for the `marketplace-listings` resource-type includes the same permissions and API operations as the `read` verb, plus the `MARKETPLACE_LISTING_LAUNCH` permission and an additional API operation, `LaunchListing`. However, the `manage` verb covers no extra permissions or API operations compared to `use`.

### `marketplace-listings`

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td><code>MARKETPLACE_LISTING_INSPECT</code></td>
<td>ListListings</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td><code>INSPECT + MARKETPLACE_LISTING_READ</code></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td><code>READ + MARKETPLACE_LISTING_LAUNCH</code></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see [Permissions](#) on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListListings</td>
<td><code>MARKETPLACE_LISTING_INSPECT</code></td>
</tr>
<tr>
<td>GetListing</td>
<td><code>MARKETPLACE_LISTING_READ</code></td>
</tr>
<tr>
<td>LaunchListing</td>
<td><code>MARKETPLACE_LISTING_LAUNCH</code></td>
</tr>
</tbody>
</table>

**Details for Monitoring**

This topic covers details for writing policies to control access to the Monitoring service.

**Resource-Types**

- alarms
- metrics

**Supported Variables**

Monitoring supports all the general variables (see [General Variables for All Requests](#) on page 2169), plus the one listed here:
Operations for This Resource-Type...

<table>
<thead>
<tr>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.metrics.namespace</td>
<td>Use this variable to control access to specific resource types. Surround the namespace value with single quotes. For example, to control access to metrics for Compute instances, use the following phrase: where target.metrics.namespace='oci_computeagent'. For an example policy, see Restrict user access to a specific metric namespace on page 2156. For valid namespace values, see Supported Services on page 2669.</td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

**alarms**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ALARM_INSPECT</td>
<td>ListAlarms ListAlarmsStatus</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetAlarmHistory</td>
<td>GetAlarm (also need METRIC_READ for the metric compartment and metric namespace)</td>
</tr>
<tr>
<td></td>
<td>ALARM_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeAlarmCompartment CreateAlarm (also need METRIC_READ for the metric compartment and metric namespace)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALARM_CREATE</td>
<td>DeleteAlarm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALARM_UPDATE</td>
<td>RemoveAlarmSuppression</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALARM_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALARM_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### metrics

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>METRIC_INSPECT</td>
<td>ListMetrics</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + METRIC_READ</td>
<td>SummarizeMetricsData</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ + METRIC_WRITE</td>
<td>PostMetricData</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE + METRIC_WRITE</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListMetrics</td>
<td>METRIC_INSPECT or METRIC_READ</td>
</tr>
<tr>
<td>SummarizeMetricsData</td>
<td>METRIC_READ</td>
</tr>
<tr>
<td>PostMetricData</td>
<td>METRIC_WRITE</td>
</tr>
<tr>
<td>ListAlarms</td>
<td>ALARM_INSPECT</td>
</tr>
<tr>
<td>ListAlarmsStatus</td>
<td>ALARM_INSPECT</td>
</tr>
<tr>
<td>GetAlarm</td>
<td>ALARM_READ and METRIC_READ</td>
</tr>
<tr>
<td>GetAlarmHistory</td>
<td>ALARM_READ</td>
</tr>
<tr>
<td>CreateAlarm</td>
<td>ALARM_CREATE and METRIC_READ</td>
</tr>
<tr>
<td>ChangeAlarmCompartment</td>
<td>ALARM_MOVE</td>
</tr>
<tr>
<td>UpdateAlarm</td>
<td>ALARM_UPDATE and METRIC_READ</td>
</tr>
<tr>
<td>RemoveAlarmSuppression</td>
<td>ALARM_UPDATE</td>
</tr>
<tr>
<td>DeleteAlarm</td>
<td>ALARM_DELETE</td>
</tr>
</tbody>
</table>

### Details for the Notifications Service

This topic covers details for writing policies to control access to the Notifications service.

**Aggregate Resource-Type**

ons-family

**Individual Resource-Types**

ons-topics

ons-subscriptions
### Supported Variables

Only the general variables are supported (see [General Variables for All Requests](#) on page 2169).

### Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

#### ons-topics

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ONS_TOPIC_INSPECT</td>
<td>ListTopics</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSPECT +</td>
<td>GetTopic</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>READ +</td>
<td>CreateSubscription</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_PUBLISH</td>
<td>UpdateSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_SUBSCRIBE</td>
<td>DeleteSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ResendSubscriptionConfirmation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PublishMessage</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateTopic</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_CREATE</td>
<td>ChangeTopicCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_MOVE</td>
<td>UpdateTopic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_UPDATE</td>
<td>DeleteTopic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### ons-subscriptions

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ONS_SUBSCRIPTION_INSPECT</td>
<td>ListSubscriptions</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>INSPECT +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>READ +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeSubscriptionCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ONS_SUBSCRIPTION_MOVE</td>
<td>CreateSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ONS_TOPIC_SUBSCRIBE</td>
<td>UpdateSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetSubscription</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ResendSubscriptionConfirmation</td>
<td></td>
</tr>
</tbody>
</table>
Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListTopics</td>
<td>ONS_TOPIC_INSPECT</td>
</tr>
<tr>
<td>GetTopic</td>
<td>ONS_TOPIC_READ</td>
</tr>
<tr>
<td>CreateTopic</td>
<td>ONS_TOPIC_CREATE</td>
</tr>
<tr>
<td>ChangeTopicCompartment</td>
<td>ONS_TOPIC_MOVE</td>
</tr>
<tr>
<td>UpdateTopic</td>
<td>ONS_TOPIC_UPDATE</td>
</tr>
<tr>
<td>DeleteTopic</td>
<td>ONS_TOPIC_DELETE</td>
</tr>
<tr>
<td>ListSubscriptions</td>
<td>ONS_SUBSCRIPTION_INSPECT</td>
</tr>
<tr>
<td>CreateSubscription</td>
<td>ONS_TOPIC_SUBSCRIBE</td>
</tr>
<tr>
<td>ChangeSubscriptionCompartment</td>
<td>ONS_SUBSCRIPTION_MOVE</td>
</tr>
<tr>
<td>UpdateSubscription</td>
<td>ONS_TOPIC_SUBSCRIBE</td>
</tr>
<tr>
<td>DeleteSubscription</td>
<td>ONS_TOPIC_SUBSCRIBE</td>
</tr>
<tr>
<td>GetSubscription</td>
<td>ONS_TOPIC_SUBSCRIBE</td>
</tr>
<tr>
<td>GetConfirmSubscription</td>
<td>(no permissions required; available to anyone)</td>
</tr>
<tr>
<td>ResendSubscriptionConfirmation</td>
<td>ONS_TOPIC_SUBSCRIBE</td>
</tr>
<tr>
<td>GetUnsubscription</td>
<td>(no permissions required; available to anyone)</td>
</tr>
<tr>
<td>PublishMessage</td>
<td>ONS_TOPIC_PUBLISH</td>
</tr>
</tbody>
</table>

Details for Object Storage, Archive Storage, and Data Transfer

This topic covers details for writing policies to control access to Archive Storage, Object Storage, and Data Transfer.

Tip:

The object lifecycle policies feature requires that you grant permissions to the Object Storage service to archive and delete objects on your behalf. See Using Object Lifecycle Policies for more information.

Resource-Types

Individual Resource-Types

objectstorage-namespaces
buckets
objects

Aggregate Resource-Type

object-family

A policy that uses <verb> object-family is equivalent to writing one with a separate <verb> <individual resource-type> statement for each of the individual resource-types.
See the table in Details for Verb + Resource-Type Combinations on page 2325 for details of the API operations covered by each verb, for each individual resource-type included in object-family.

**Additional Individual Resource-Type for Data Transfer**

**data-transfer-jobs**

**Supported Variables**

Object Storage supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here:

<table>
<thead>
<tr>
<th>Operations for This Resource-Type...</th>
<th>Can Use This Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>buckets and objects</td>
<td>target.bucket.name</td>
<td>String</td>
<td>Use this variable to control access to a specific bucket. For an example policy, see Let users write objects to Object Storage buckets on page 2149. <strong>Important:</strong> Condition matching is case insensitive. If you have a bucket named &quot;BucketA&quot; and a bucket named &quot;bucketA&quot;, the condition where target.bucket.name=&quot;BucketA&quot; applies to both. To avoid potential issues with resource names in policy, give your resources distinct names.</td>
</tr>
</tbody>
</table>

**Note:**
The request.ipv4.ipaddress and the request.vcn.id variables are deprecated. Instead of using these variables, create a network source to specify either an IP address range or a specific VCN ID. You can then use the network source in your policy to restrict access to only requests coming from the allowed networks. For more information, see Managing Network Sources on page 2427.

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

**For object-family Resource Types**

<table>
<thead>
<tr>
<th>objectstorage-namespaces</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>None</td>
<td>GetNamespace</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>OBJECTSTORAGE_NAMESPACE_READ</td>
<td>GetNamespace</td>
<td>none</td>
</tr>
<tr>
<td>None</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>OBJECTSTORAGE_NAMESPACE_UPDATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### buckets

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>BUCKET_INSPECT</td>
<td>HeadBucket</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListBuckets</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>BUCKET_READ</td>
<td>GetBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListMultipartUploads</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetObjectLifecyclePolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetRetentionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListRetentionRules</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetReplicationPolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListReplicationPolicies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListReplicationSources</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>PutObjectLifecyclePolicy</td>
</tr>
<tr>
<td></td>
<td>BUCKET_UPDATE</td>
<td>UpdateBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteObjectLifecyclePolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReencryptBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>USE +</td>
<td>USE +</td>
<td>CreateReplicationPolicy, DeleteReplicationPolicy, MakeBucketWritable</td>
</tr>
<tr>
<td></td>
<td>BUCKET_CREATE</td>
<td>CreateBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BUCKET_DELETE</td>
<td>DeleteBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAR_MANAGE</td>
<td>CreatePar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RETENTION_RULE_MANAGE</td>
<td>Par</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RETENTION_RULE_LOCK (if using optional rule locking)</td>
<td>ListPar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeletePar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateRetentionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateRetentionRule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteRetentionRule</td>
<td></td>
</tr>
</tbody>
</table>
### objects

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>OBJECT_INSPECT</td>
<td>HeadObject</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListObjects</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListMultipartUploadParts</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>OBJECT_READ</td>
<td>GetObject</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>READ +</td>
</tr>
<tr>
<td></td>
<td>OBJECT_OVERWRITE</td>
<td>ReencryptObject</td>
<td>PutObject (USE allows PutObject to overwrite existing objects, but creating a new object also requires OBJECT_CREATE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateMultipartUpload, UploadPart, CommitMultipartUpload (these operations also need manage objects)</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>PutObjectLifecyclePolicy (also needs manage objects)</td>
</tr>
<tr>
<td></td>
<td>OBJECT_CREATE</td>
<td>CreateObject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OBJECT_DELETE</td>
<td>RenameObject</td>
<td>CreateReplicationPolicy. DeleteReplicationPolicy. MakeBucketWritable (these operations also need manage buckets)</td>
</tr>
<tr>
<td></td>
<td>OBJECT_VERSION_DELETE</td>
<td>RestoreObject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OBJECT_RESTORE</td>
<td>DeleteObject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OBJECT_UPDATE_TIER</td>
<td>DeleteObjectVersion</td>
<td>UpdateObjectStorageTier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CreateMultipartUpload</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UploadPart</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CommitMultipartUpload</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AbortMultipartUpload</td>
</tr>
</tbody>
</table>

### data-transfer-jobs

Policies for data transfer jobs also require either manage objects or manage objects and manage buckets. See Creating the Required IAM Users, Groups, and Policies on page 1023 for details.

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>TRANSFER_JOB_INSPECT</td>
<td>no customer-facing API</td>
<td>no customer-facing API</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>no customer-facing API</td>
</tr>
<tr>
<td></td>
<td>TRANSFER_JOB_READ</td>
<td>no customer-facing API</td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>----------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>READ +</td>
</tr>
<tr>
<td></td>
<td>TRANSFER_JOB_UPDATE</td>
<td>no customer-facing API</td>
<td>no customer-facing API</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>TRANSFER_JOB_CREATE</td>
<td>no customer-facing API</td>
<td>no customer-facing API</td>
</tr>
<tr>
<td></td>
<td>TRANSFER_JOB_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetNamespace</td>
<td>API requires no permissions and returns the caller's namespace. Use the API to validate your credentials.</td>
</tr>
<tr>
<td></td>
<td>OBJECTSTORAGE_NAMESPACE_READ permission is required if you include the optional compartmentId parameter.</td>
</tr>
<tr>
<td></td>
<td>Use the compartmentId parameter to determine the namespace for a third-party tenancy.</td>
</tr>
<tr>
<td>GetNamespaceMetadata</td>
<td>OBJECTSTORAGE_NAMESPACE_READ</td>
</tr>
<tr>
<td>UpdateNamespaceMetadata</td>
<td>OBJECTSTORAGE_NAMESPACE_UPDATE</td>
</tr>
<tr>
<td>CreateBucket</td>
<td>BUCKET_CREATE</td>
</tr>
<tr>
<td>UpdateBucket</td>
<td>BUCKET_UPDATE</td>
</tr>
<tr>
<td>GetBucket</td>
<td>BUCKET_READ</td>
</tr>
<tr>
<td>HeadBucket</td>
<td>BUCKET_INSPECT</td>
</tr>
<tr>
<td>ListBuckets</td>
<td>BUCKET_INSPECT</td>
</tr>
<tr>
<td>DeleteBucket</td>
<td>BUCKET_DELETE</td>
</tr>
<tr>
<td>ReencryptBucket</td>
<td>BUCKET_UPDATE</td>
</tr>
<tr>
<td>PutObject</td>
<td>The permission required depends on whether or not the object already exists in the bucket:</td>
</tr>
<tr>
<td></td>
<td>• OBJECT_CREATE is required when an object with that name does not already exist in the bucket.</td>
</tr>
<tr>
<td></td>
<td>• OBJECT_OVERWRITE is required when an object with that name already exists in the bucket.</td>
</tr>
<tr>
<td>RenameObject</td>
<td>OBJECT_CREATE and OBJECT_OVERWRITE</td>
</tr>
<tr>
<td>GetObject</td>
<td>OBJECT_READ</td>
</tr>
<tr>
<td>HeadObject</td>
<td>OBJECT_READ or OBJECT_INSPECT</td>
</tr>
<tr>
<td>DeleteObject</td>
<td>OBJECT_DELETE</td>
</tr>
<tr>
<td>DeleteObjectVersion</td>
<td>OBJECT_VERSION_DELETE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>ListObjects</td>
<td>OBJECT_INSPECT</td>
</tr>
<tr>
<td>ReencryptObject</td>
<td>OBJECT_READ &amp; OBJECT_OVERWRITE</td>
</tr>
<tr>
<td>RestoreObjects</td>
<td>OBJECT_RESTORE</td>
</tr>
<tr>
<td>UpdateObjectStorageTier</td>
<td>OBJECT_UPDATE_TIER</td>
</tr>
<tr>
<td>CreateMultipartUpload</td>
<td>OBJECT_CREATE and OBJECT_OVERWRITE</td>
</tr>
<tr>
<td>UploadPart</td>
<td>OBJECT_CREATE and OBJECT_OVERWRITE</td>
</tr>
<tr>
<td>CommitMultipartUpload</td>
<td>OBJECT_CREATE and OBJECT_OVERWRITE</td>
</tr>
<tr>
<td>ListMultipartUploadParts</td>
<td>OBJECT_INSPECT</td>
</tr>
<tr>
<td>ListMultipartUploads</td>
<td>BUCKET_READ</td>
</tr>
<tr>
<td>AbortMultipartUpload</td>
<td>OBJECT_DELETE</td>
</tr>
<tr>
<td>CreatePar</td>
<td>PAR_MANAGE</td>
</tr>
<tr>
<td>GetPar</td>
<td>PAR_MANAGE</td>
</tr>
<tr>
<td>ListPars</td>
<td>PAR_MANAGE</td>
</tr>
<tr>
<td>DeletePar</td>
<td>PAR_MANAGE</td>
</tr>
<tr>
<td>PutObjectLifecyclePolicy</td>
<td>BUCKET_UPDATE, OBJECT_CREATE, and OBJECT_DELETE</td>
</tr>
<tr>
<td>GetObjectLifecyclePolicy</td>
<td>BUCKET_READ</td>
</tr>
<tr>
<td>DeleteObjectLifecyclePolicy</td>
<td>BUCKET_UPDATE</td>
</tr>
<tr>
<td>CreateRetentionRule</td>
<td>BUCKET_UPDATE &amp; RETENTION_RULE_MANAGE (&amp; RETENTION_RULE_LOCK)</td>
</tr>
<tr>
<td>GetRetentionRule</td>
<td>BUCKET_READ</td>
</tr>
<tr>
<td>ListRetentionRule</td>
<td>BUCKET_READ</td>
</tr>
<tr>
<td>UpdateRetentionRule</td>
<td>BUCKET_UPDATE &amp; RETENTION_RULE_MANAGE (&amp; RETENTION_RULE_LOCK)</td>
</tr>
<tr>
<td>DeleteRetentionRule</td>
<td>BUCKET_UPDATE &amp; RETENTION_RULE_MANAGE</td>
</tr>
<tr>
<td>CreateCopyRequest</td>
<td>OBJECT_READ, OBJECT_CREATE, OBJECT_OVERWRITE, and OBJECT_INSPECT</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>OBJECT_READ</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>OBJECT_INSPECT</td>
</tr>
<tr>
<td>CancelWorkRequest</td>
<td>OBJECT_DELETE</td>
</tr>
<tr>
<td>CreateReplicationPolicy</td>
<td>OBJECT_READ, OBJECT_CREATE, OBJECT_OVERWRITE, OBJECT_INSPECT, OBJECT_DELETE, OBJECT_RESTORE, BUCKET_READ, and BUCKET_UPDATE</td>
</tr>
<tr>
<td>GetReplicationPolicy</td>
<td>BUCKET_READ</td>
</tr>
</tbody>
</table>
## Details for Operations Insights

This topic covers details for writing policies to control access to the Operations Insights service.

### Resource-Types

**Individual Resource-Types**

.opsi-database-insights

**Aggregate Resource-Types**

.opsi-family

### Comments

See the table in Permissions Required for Each API Operation on page 2331 for details of the API operations covered by each verb, for each individual resource-type.

### Supported Variables

Only the general variables are supported (see General Variables for All Requests on page 2169).

### Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

**opsi-database-insights**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>OPSI_DATABASE_INSIGHT_INSPECT</td>
<td>listDatabaseInsights</td>
<td>none</td>
</tr>
</tbody>
</table>

<p>|</p>
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>ListSqlPlans</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_PLANS_READ</td>
<td>SummarizeSqlPlanInsights</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_SEARCH_READ</td>
<td>SummarizeSqlSearch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_TEXT_READ</td>
<td>SummarizeSqlTexts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_RESPONSE_TIME_DISTRIBUTIONS_READ</td>
<td>SummarizeSqlResponseTimeDistributions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_STATISTICS_READ</td>
<td>SummarizeSqlStatistics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_STATISTICS_TIME_SERIES_READ</td>
<td>SummarizeSqlStatisticsTimeSeries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_TEXTS_READ</td>
<td>SummarizeSqlTexts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_BUCKET_INGEST</td>
<td>IngestSqlBucket</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_PLAN_LINES_INGEST</td>
<td>IngestSqlPlanLines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_TEXT_INGEST</td>
<td>IngestSqlText</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>IngestSqlBucket</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_BUCKET_INGEST</td>
<td>IngestSqlBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_PLAN_LINES_INGEST</td>
<td>IngestSqlPlanLines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OPSI_DATABASE_INSIGHT_SQL_TEXT_INGEST</td>
<td>IngestSqlText</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in alphabetical order.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IngestSqlBucket</td>
<td>OPSI_DATABASE_INSIGHT_SQL_BUCKET_INGEST</td>
</tr>
<tr>
<td>IngestSqlPlanLines</td>
<td>OPSI_DATABASE_INSIGHT_SQL_PLAN_LINES_INGEST</td>
</tr>
<tr>
<td>IngestSqlText</td>
<td>OPSI_DATABASE_INSIGHT_SQL_TEXT_INGEST</td>
</tr>
<tr>
<td>ListDatabaseInsights</td>
<td>OPSI_DATABASE_INSIGHT_INSPECT</td>
</tr>
<tr>
<td>ListSqlPlans</td>
<td>OPSI_DATABASE_INSIGHT_SQL_PLAN_READ</td>
</tr>
<tr>
<td>ListSqlSearches</td>
<td>OPSI_DATABASE_INSIGHT_SQL_SEARCH_READ</td>
</tr>
<tr>
<td>ListSqlTexts</td>
<td>OPSI_DATABASE_INSIGHT_SQL_TEXTS_READ</td>
</tr>
<tr>
<td>SummarizeDatabaseInsightResourceCapacityTrend</td>
<td>OPSI_DATABASE_INSIGHT_RESOURCE_CAPACITY_TREND_READ</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>SummarizeDatabaseInsightResourceForecastTrend</td>
<td>OPSI_DATABASE_INSIGHT_RESOURCE_FORECAST_TREND_READ</td>
</tr>
<tr>
<td>SummarizeDatabaseInsightResourceStatistics</td>
<td>OPSI_DATABASE_INSIGHT_RESOURCE_STATISTICS_READ</td>
</tr>
<tr>
<td>SummarizeDatabaseInsightResourceUsage</td>
<td>OPSI_DATABASE_INSIGHT_RESOURCE_USAGE_READ</td>
</tr>
<tr>
<td>SummarizeDatabaseInsightResourceUsageTrend</td>
<td>OPSI_DATABASE_INSIGHT_RESOURCE_USAGE_TREND_READ</td>
</tr>
<tr>
<td>SummarizeDatabaseInsightResourceUtilizationInsight</td>
<td>OPSI_DATABASE_INSIGHT_RESOURCE_UTILIZATION_INSIGHT</td>
</tr>
<tr>
<td>SummarizeSqlInsights</td>
<td>OPSI_DATABASE_INSIGHT_SQL_INSIGHTS_READ</td>
</tr>
<tr>
<td>SummarizeSqlPlanInsights</td>
<td>OPSI_DATABASE_INSIGHT_SQL_PLAN_INSIGHTS_READ</td>
</tr>
<tr>
<td>SummarizeSqlResponseTimeDistributions</td>
<td>OPSI_DATABASE_INSIGHT_SQL_RESPONSE_TIME_DISTRIBUTIONS_READ</td>
</tr>
<tr>
<td>SummarizeSqlStatistics</td>
<td>OPSI_DATABASE_INSIGHT_SQL_STATISTICS_READ</td>
</tr>
<tr>
<td>SummarizeSqlStatisticsTimeSeries</td>
<td>OPSI_DATABASE_INSIGHT_SQL_STATISTICS_TIME_SERIES_READ</td>
</tr>
<tr>
<td>SummarizeSqlStatisticsTimeSeriesByPlan</td>
<td>OPSI_DATABASE_INSIGHT_SQL_STATISTICS_TIME_SERIES_BY_PLAN_READ</td>
</tr>
</tbody>
</table>

Details for Oracle Cloud VMware Solution

This topic covers details for writing policies to control access to Oracle Cloud VMware Solution resources.

**Resource-Types**

sddcs

**Supported Variables**

Only the general variables are supported (see General Variables for All Requests on page 2169).

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for sddcs includes the same permissions and API operations as the inspect verb, plus the SDDC_READ permission and a number of API operations (e.g., GetSddc, ListWorkRequests, etc.). The use verb covers two more permissions and set of API operations compared to read. And manage covers five more permissions and operations compared to use.

**sddcs**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SDDC_INSPECT</td>
<td>ListSddcs</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequests</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>SDDC_READ</td>
<td>GetSddc</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>SDDC_UPDATE</td>
<td>UpdateSddc</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDDC_UPDATE_ESXI_HOST</td>
<td>UpdateEsxiHost</td>
<td></td>
</tr>
</tbody>
</table>
## IAM

### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>CreateSddc (also need manage instances, manage vcns, use subnets, use vnic, use vlans, use private-ips, inspect security-lists, use network-security-groups)</td>
</tr>
<tr>
<td></td>
<td>SDDC_CREATE</td>
<td></td>
<td>DeleteSddc, CreateEsxiHost, DeleteEsxiHost (also need manage instances, manage vcns, use subnets, use vnic, use vlans, use private-ips)</td>
</tr>
<tr>
<td></td>
<td>SDDC_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDDC_ADD_ESXI_HOST</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDDC_DELETE_ESXI_HOST</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDDC_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListSddcs</td>
<td>SDDC_INSPECT</td>
</tr>
<tr>
<td>GetSddc</td>
<td>SDDC_READ</td>
</tr>
<tr>
<td>CreateSddc</td>
<td>SDDC_CREATE &amp; INSTANCE_CREATE &amp; INSTANCE_ATTACH_SECONDARY_VNIC &amp; VCN_READ &amp; VCN_ATTACH &amp; SUBNET_READ &amp; SUBNET_ATTACH &amp; VNIC_READ &amp; VNIC_CREATE &amp; VLAN_READ &amp; VLAN_ATTACH &amp; PRIVATE_IP_CREATE &amp; PRIVATE_IP_ASSIGN &amp; SECURITY_LIST_READ &amp; NETWORK_SECURITY_GROUP_LIST_SECURITY_RULES</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>SDDC_INSPECT</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>SDDC_READ</td>
</tr>
<tr>
<td>ChangeSddcCompartment</td>
<td>SDDC_MOVE</td>
</tr>
<tr>
<td>UpdateSddc</td>
<td>SDDC_UPDATE</td>
</tr>
<tr>
<td>DeleteSddc</td>
<td>SDDC_DELETE &amp; INSTANCE_DELETE &amp; INSTANCE_DETACH_SECONDARY_VNIC &amp; VCN_DETACH &amp; SUBNET_DETACH &amp; VLAN_DETACH &amp; VNIC_READ &amp; VNIC_DELETE &amp; PRIVATE_IP_DELETE &amp; PRIVATE_IP_UNASSIGN</td>
</tr>
<tr>
<td>ListEsxiHosts</td>
<td>SDDC_INSPECT</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CreateEsxiHost</td>
<td>SDDC_ADD_ESXI_HOST &amp; INSTANCE_CREATE &amp; INSTANCE_ATTACH_SECONDARY_VNIC &amp; VCN_READ &amp; VCN_ATTACH &amp; SUBNET_READ &amp; SUBNET_ATTACH &amp; VLAN_READ &amp; VLAN_ATTACH &amp; VNIC_READ &amp; VNIC_CREATE &amp; PRIVATE_IP_CREATE &amp; PRIVATE_IP_ASSIGN</td>
</tr>
<tr>
<td>UpdateEsxiHost</td>
<td>SDDC_UPDATE_ESXI_HOST</td>
</tr>
<tr>
<td>DeleteEsxiHost</td>
<td>SDDC_DELETE_ESXI_HOST &amp; INSTANCE_DELETE &amp; INSTANCE_DETACH_SECONDARY_VNIC &amp; VCN_DETACH &amp; SUBNET_DETACH &amp; VLAN_DETACH &amp; VNIC_DELETE &amp; PRIVATE_IP_DELETE &amp; PRIVATE_IP_UNASSIGN</td>
</tr>
</tbody>
</table>

Details for the Quotas Service

This topic covers details for writing policies to control access to the Quotas service.

**Supported Variables**

The Quotas service supports all the general variables (see General Variables for All Requests on page 2169) plus the following:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.quota.id</td>
<td>Entity</td>
<td>Request/OCID</td>
</tr>
<tr>
<td>target.quota.name</td>
<td>String</td>
<td>Request/Stored</td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>QUOTA_INSPECT</td>
<td>listQuotas</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>QUOTA_READ</td>
<td>getQuota</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>createQuota</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>QUOTA_CREATE</td>
<td>deleteQuota</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QUOTA_DELETE</td>
<td>updateQuota</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QUOTA_UPDATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Permissions Required for Each API Operation

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>listQuotas</td>
<td>QUOTA_INSPECT</td>
</tr>
<tr>
<td>createQuota</td>
<td>QUOTA_CREATE</td>
</tr>
<tr>
<td>getQuota</td>
<td>QUOTA_READ</td>
</tr>
<tr>
<td>deleteQuota</td>
<td>QUOTA_DELETE</td>
</tr>
<tr>
<td>updateQuota</td>
<td>QUOTA_UPDATE</td>
</tr>
</tbody>
</table>

Details for Registry
This topic covers details for writing policies to control access to the Registry.

Resource-Types
- repos

Supported Variables
Oracle Cloud Infrastructure Registry supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

The repos resource-type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.repo.name</td>
<td>String</td>
<td>Use this variable to control access to specific repositories. For an example policy, see Policies to Control Repository Access on page 3527.</td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations
The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the repos resource-type includes the same permissions and API operations as the inspect verb, plus the REPOSITORY_READ permission and a number of API operations (e.g., GetContainerRepository, etc.). The use verb covers still another permission and API operation compared to read. Lastly, manage covers more permissions and operations compared to use.

repos
### Permissions Required for Each API Operation

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListContainerRepositories</td>
<td>REPOSITORY_INSPECT</td>
</tr>
<tr>
<td>CreateContainerRepository</td>
<td>REPOSITORY_CREATE</td>
</tr>
<tr>
<td>GetContainerRepository</td>
<td>REPOSITORY_READ</td>
</tr>
<tr>
<td>UpdateContainerRepository</td>
<td>REPOSITORY_MANAGE</td>
</tr>
<tr>
<td>DeleteContainerRepository</td>
<td>REPOSITORY_DELETE</td>
</tr>
<tr>
<td>ChangeContainerRepositoryCompartment</td>
<td>REPOSITORY_MANAGE</td>
</tr>
<tr>
<td>ListContainerImages</td>
<td>REPOSITORY_INSPECT</td>
</tr>
<tr>
<td>GetContainerImage</td>
<td>REPOSITORY_READ</td>
</tr>
<tr>
<td>DeleteContainerImage</td>
<td>REPOSITORY_UPDATE</td>
</tr>
<tr>
<td>RestoreContainerImage</td>
<td>REPOSITORY_UPDATE</td>
</tr>
<tr>
<td>RemoveContainerVersion</td>
<td>REPOSITORY_UPDATE</td>
</tr>
<tr>
<td>GetContainerConfiguration</td>
<td>REPOSITORY_INSPECT</td>
</tr>
<tr>
<td>UpdateContainerConfiguration</td>
<td>REPOSITORY_MANAGE</td>
</tr>
</tbody>
</table>

### Details for Resource Manager

This topic covers details for writing policies to control access to the Resource Manager service.
Aggregate Resource-Type

orm-family

Individual Resource-Types

orm-config-source-providers
orm-jobs
orm-stacks
orm-template
orm-work-requests

Supported Variables

Resource Manager supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

The orm-jobs resource type can use the following variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.job.operation</td>
<td>String</td>
<td>Use this variable to control access for running specified job types. For example, to limit access to PLAN and APPLY jobs, use the following phrase: where any {target.job.operation = 'PLAN', target.job.operation = 'APPLY'}</td>
</tr>
<tr>
<td>target.stack.id</td>
<td>String</td>
<td>Use this variable to limit access to specified stacks. For example, use the following phrase: where any {target.stack.id = ocid1.ormstack.uniqueid1, target.stack.id = ocid1.ormstack.uniqueid2}</td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

orm-config-source-providers

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>ORM_CONFIG_SOURCE_PROVIDERInspectable</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------</td>
<td>---------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetConfigurationSourceProvider</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_CONFIG_SOURCE_PROVIDER_READ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateConfigurationSourceProvider</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_CONFIG_SOURCE_PROVIDER_CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_CONFIG_SOURCE_PROVIDER_UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_CONFIG_SOURCE_PROVIDER_MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_CONFIG_SOURCE_PROVIDER_DELETE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**orm-jobs**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ORM_JOB_INSPECT</td>
<td>ListJobs</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetJob</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ORM_JOB_READ</td>
<td>GetJobTfState</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetJobTfConfig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetJobTfExecutionPlan</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetJobLogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetJobLogsContent</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>no extra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>UpdateJob</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_JOB_MANAGE</td>
<td>CancelJob</td>
<td></td>
</tr>
</tbody>
</table>

**orm-stacks**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ORM_STACK_INSPECT</td>
<td>ListResourceDiscoveryServices</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListStacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListTerraformVersions</td>
<td></td>
</tr>
</tbody>
</table>
### IAM

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetStack</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ORM_STACK_READ</td>
<td>GetStackTfConfig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetStackTfState</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListStackResourceDriftDetails</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>CreateJob (also need manage orm-jobs)</td>
</tr>
<tr>
<td></td>
<td>ORM_STACK_USE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateStack (unless using configuration source providers)</td>
<td>CreateStack: When creating stacks that use configuration source providers (configSourceType value GIT_CONFIG_SOURCE), also need read orm-config-source-providers</td>
</tr>
<tr>
<td></td>
<td>ORM_STACK_CREATE</td>
<td>UpdateStack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_STACK_UPDATE</td>
<td>ChangeStackCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_STACK_MOVE</td>
<td>DeleteStack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_STACK_DELETE</td>
<td>DetectStateDrift</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListTerraformVersions</td>
<td></td>
</tr>
</tbody>
</table>

**orm-template**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ORM_TEMPLATE_INSPECT</td>
<td>ListTemplates</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetTemplate</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ORM_TEMPLATE_READ</td>
<td>GetTemplateLogo</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetTemplateTfConfig</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>UpdateTemplate</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ORM_TEMPLATE_UPDATE</td>
<td>ChangeTemplateCompartment</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>CreateTemplate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_TEMPLATE_CREATE</td>
<td>DeleteTemplate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_TEMPLATE_DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ORM_TEMPLATE_MOVE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**orm-work-requests**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>ORM_WORK_REQUEST_INSPECT</td>
<td>ListWorkRequests</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>ListWorkRequestErrors</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ORM_WORK_REQUEST_READ</td>
<td>ListWorkRequestLogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWorkRequest</td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>use</td>
<td>READ + no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE + no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in alphabetical order.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CancelJob</td>
<td>ORM_JOB_MANAGE</td>
</tr>
<tr>
<td>ChangeConfigurationSourceProviderCompartment</td>
<td>ORM_CONFIG_SOURCE_PROVIDER_MOVE</td>
</tr>
<tr>
<td>ChangeStackCompartment</td>
<td>ORM_STACK_MOVE</td>
</tr>
<tr>
<td>ChangeTemplateCompartment</td>
<td>ORM_TEMPLATE_MOVE</td>
</tr>
<tr>
<td>CreateConfigurationSourceProvider</td>
<td>ORM_CONFIG_SOURCE_PROVIDER_CREATE</td>
</tr>
<tr>
<td>CreateJob</td>
<td>ORM_JOB_MANAGE and ORM_STACK_USE</td>
</tr>
<tr>
<td>CreateStack</td>
<td>ORM_STACK_CREATE if not using configuration source providers. If using configuration source providers (configSourceType value GIT_CONFIG_SOURCE), also need read orm-config-source-providers</td>
</tr>
<tr>
<td>DeleteConfigurationSourceProvider</td>
<td>ORM_CONFIG_SOURCE_PROVIDER_DELETE</td>
</tr>
<tr>
<td>DeleteStack</td>
<td>ORM_STACK_DELETE</td>
</tr>
<tr>
<td>DeleteTemplate</td>
<td>ORM_TEMPLATE_DELETE</td>
</tr>
<tr>
<td>DetectStateDrift</td>
<td>ORM_STACK_UPDATE</td>
</tr>
<tr>
<td>GetConfigurationSourceProvider</td>
<td>ORM_CONFIG_SOURCE_PROVIDER_READ</td>
</tr>
<tr>
<td>GetJob</td>
<td>ORM_JOB_READ</td>
</tr>
<tr>
<td>GetJobLogs</td>
<td>ORM_JOB_READ</td>
</tr>
<tr>
<td>GetJobLogsContent</td>
<td>ORM_JOB_READ</td>
</tr>
<tr>
<td>GetJobTfConfig</td>
<td>ORM_JOB_READ</td>
</tr>
<tr>
<td>GetJobTfExecutionPlan</td>
<td>ORM_JOB_READ</td>
</tr>
<tr>
<td>GetJobTfState</td>
<td>ORM_JOB_READ</td>
</tr>
<tr>
<td>GetStack</td>
<td>ORM_STACK_READ</td>
</tr>
<tr>
<td>GetStackTfConfig</td>
<td>ORM_STACK_READ</td>
</tr>
<tr>
<td>GetStackTfState</td>
<td>ORM_STACK_READ</td>
</tr>
</tbody>
</table>
### API Operation

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetTemplate</td>
<td>ORM_TEMPLATE_READ</td>
</tr>
<tr>
<td>GetTemplateLogo</td>
<td>ORM_TEMPLATE_READ</td>
</tr>
<tr>
<td>GetTemplateTfConfig</td>
<td>ORM_TEMPLATE_READ</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>ORM_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>ListConfigurationSourceProviders</td>
<td>ORM_CONFIG_SOURCE_PROVIDER_INSPECT</td>
</tr>
<tr>
<td>ListJobs</td>
<td>ORM_JOB_INSPECT</td>
</tr>
<tr>
<td>ListResourceDiscoveryServices</td>
<td>ORM_STACK_INSPECT</td>
</tr>
<tr>
<td>ListStackResourceDriftDetails</td>
<td>ORM_STACK_READ</td>
</tr>
<tr>
<td>ListStacks</td>
<td>ORM_STACK_INSPECT</td>
</tr>
<tr>
<td>ListTemplateCategories</td>
<td>None</td>
</tr>
<tr>
<td>ListTemplates</td>
<td>ORM_TEMPLATE_INSPECT</td>
</tr>
<tr>
<td>ListTerraformVersions</td>
<td>ORM_STACK_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>ORM_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>ORM_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>ORM_WORK_REQUEST_INSPECT</td>
</tr>
<tr>
<td>UpdateConfigurationSourceProvider</td>
<td>ORM_CONFIG_SOURCE_PROVIDER_UPDATE</td>
</tr>
<tr>
<td>UpdateJob</td>
<td>ORM_JOB_MANAGE</td>
</tr>
<tr>
<td>UpdateStack</td>
<td>ORM_STACK_UPDATE</td>
</tr>
<tr>
<td>UpdateTemplate</td>
<td>ORM_TEMPLATE_UPDATE</td>
</tr>
</tbody>
</table>

### Details for Search

The Search service does not require permissions for its API operations. You do not need to write policies specifically to control access to Search. However, what you can see in search or query results depends on the permissions you have. If a policy exists to give you access to the `inspect` verb for a particular resource type, you have access to the permissions needed to view that resource type and its associated metadata in search results. If a service does not recognize the `inspect` verb or if the resource type's `inspect` verb does not fully cover list operations, permissions to view the service's supported resource types are granted by the `read` verb instead.

For more information about permissions, see the Permissions section of Advanced Policy Features.

### Permissions Required to View Each Resource Type

The following table lists the resource types grouped by service, which are listed in alphabetical order. The Search API operations that can access the metadata for these resource types with these permissions are `GetResourceType`, `ListResourceTypes`, and `SearchResources`.

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Required to View in Search Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Volume</td>
<td>volumes</td>
<td>VOLUME_INSPECT</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volume-backups</td>
<td>VOLUME_BACKUP_INSPECT</td>
</tr>
<tr>
<td>Compute</td>
<td>console-histories</td>
<td>CONSOLE_HISTORY_INSPECT</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Permissions Required to View in Search Results</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Compute</td>
<td>instance-images</td>
<td>INSTANCE_IMAGE_READ</td>
</tr>
<tr>
<td>Compute</td>
<td>instances</td>
<td>INSTANCE_READ</td>
</tr>
<tr>
<td>Database</td>
<td>databases</td>
<td>DATABASE_INSPECT</td>
</tr>
<tr>
<td>Database</td>
<td>db-homes</td>
<td>DB_HOME_INSPECT (if you want to filter results using db-homes attributes)</td>
</tr>
<tr>
<td>Database</td>
<td>db-systems</td>
<td>DB_SYSTEM_INSPECT</td>
</tr>
<tr>
<td>IAM</td>
<td>compartments</td>
<td>COMPARTMENT_INSPECT</td>
</tr>
<tr>
<td>IAM</td>
<td>groups</td>
<td>GROUP_INSPECT</td>
</tr>
<tr>
<td>IAM</td>
<td>identity-providers</td>
<td>IDENTITY_PROVIDER_INSPECT</td>
</tr>
<tr>
<td>IAM</td>
<td>users</td>
<td>USER_INSPECT</td>
</tr>
<tr>
<td>Networking</td>
<td>route-tables</td>
<td>ROUTE_TABLE_READ</td>
</tr>
<tr>
<td>Networking</td>
<td>security-lists</td>
<td>SECURITY_LIST_READ</td>
</tr>
<tr>
<td>Networking</td>
<td>subnets</td>
<td>SUBNET_READ</td>
</tr>
<tr>
<td>Networking</td>
<td>vcns</td>
<td>VCN_READ</td>
</tr>
<tr>
<td>Object Storage</td>
<td>buckets</td>
<td>BUCKET_INSPECT</td>
</tr>
</tbody>
</table>

Details for Service Connector Hub

This topic covers details for writing policies to control access to the Service Connector Hub service.

**Individual Resource-Types**

`serviceconnectors`

**Supported Variables**

Service Connector Hub supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

The `serviceconnectors` resource type can use the following variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>target.serviceconnector.id</code></td>
<td>OCID</td>
<td>Use this variable to control access for service connectors.</td>
</tr>
</tbody>
</table>

Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.
### serviceconnectors

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SERVICE_CONNECTOR_INSPECT</td>
<td>ListWorkRequest</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListServiceConnectors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestErrors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequestLogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWorkRequests</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>GetServiceConnector</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>ActivateServiceConnector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateServiceConnector</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>ChangeServiceConnector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateServiceConnector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteServiceConnector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SERVICE_CONNECTOR_CREATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SERVICE_CONNECTOR_DELETE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SERVICE_CONNECTOR_MOVE</td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

The following table lists API operations in alphabetical order.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActivateServiceConnector</td>
<td>SERVICE_CONNECTOR_UPDATE</td>
</tr>
<tr>
<td>ChangeServiceConnectorCompartment</td>
<td>SERVICE_CONNECTOR_MOVE</td>
</tr>
<tr>
<td>CreateServiceConnector</td>
<td>SERVICE_CONNECTOR_CREATE</td>
</tr>
<tr>
<td>DeactivateServiceConnector</td>
<td>SERVICE_CONNECTOR_UPDATE</td>
</tr>
<tr>
<td>DeleteServiceConnector</td>
<td>SERVICE_CONNECTOR_DELETE</td>
</tr>
<tr>
<td>GetServiceConnector</td>
<td>SERVICE_CONNECTOR_READ</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>SERVICE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>ListServiceConnectors</td>
<td>SERVICE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>SERVICE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>SERVICE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>SERVICE_CONNECTOR_INSPECT</td>
</tr>
<tr>
<td>UpdateServiceConnector</td>
<td>SERVICE_CONNECTOR_UPDATE</td>
</tr>
</tbody>
</table>

### Details for the Streaming Service

This topic covers details for writing policies to control access to the Streaming service.
**Resource-Types**

- streams
- stream-pull
- stream-push
- connect-harnesses
- stream-pools

**Supported Variables**

The Streaming service supports all the general variables (see General Variables for All Requests on page 2169) plus the following:

The **streams** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.stream.id</td>
<td>Entity (OCID)</td>
<td>Request</td>
</tr>
</tbody>
</table>

The **connect-harnesses** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.connectharness.id</td>
<td>Entity (OCID)</td>
<td>Request</td>
</tr>
</tbody>
</table>

The **stream-pools** resource type can use the following variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.streampool.id</td>
<td>Entity (OCID)</td>
<td>Request</td>
</tr>
</tbody>
</table>

**Details for Verb + Resource-Type Combinations**

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

**streams**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>STREAM_INSPECT</td>
<td>ListStreams</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + STREAM_READ</td>
<td>GetStream</td>
<td>none</td>
</tr>
</tbody>
</table>
### IAM

**Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
---|---|---|---
**use** | READ + | UpdateStream | none
STREAM_UPDATE | MoveStream
STREAM_MOVE | PutMessages
STREAM_PRODUCE | GetMessages
STREAM_CONSUME | CreateCursor
CreateGroupCursor
GetGroup
UpdateGroup
ConsumerHeartbeat
ConsumerCommit
**manage** | USE + | CreateStream | none
STREAM_CREATE | DeleteStream
STREAM_DELETE | none

#### stream-pull

**Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
---|---|---|---
inspect | none | none | none
read | none | none | none
use | STREAM_CONSUME | GetMessages | none
CreateCursor
CreateGroupCursor
GetGroup
UpdateGroup
ConsumerHeartbeat
ConsumerCommit
**manage** | no extra | no extra | none

#### stream-push

**Verbs** | **Permissions** | **APIs Fully Covered** | **APIs Partially Covered**
---|---|---|---
inspect | none | none | none
read | none | none | none
use | STREAM_PRODUCE | PutMessages | none
**manage** | no extra | no extra | none
### stream-pools

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>STREAM_POOL_INSPECT</td>
<td>ListStreamPools</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + STREAM_POOL_READ</td>
<td>GetStreamPools</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ + STREAM_POOL_UPDATE</td>
<td>UpdateStreamPool</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>STREEm_POOL_Move</td>
<td>MoveStreamPool</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>USE+ STREAM_POOL_CREATE</td>
<td>CreateStreamPool</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>DELETE STREAM_POOL_DELETE</td>
<td>DeleteStreamPool</td>
<td>none</td>
</tr>
</tbody>
</table>

### connect-harnesses

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>CONNECT_HARNESS_INSPECT</td>
<td>GetConnectHarness</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + CONNECT_HARNESS_READ</td>
<td>GetConnectHarness</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ + CONNECT_HARNESS_UPDATE</td>
<td>UpdateConnectHarness</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>CONNECT_HARNESS_MOVE</td>
<td>MoveConnectHarness</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>CONNECT_HARNESS_USE</td>
<td>CreateConnectHarness</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>CONNECT_HARNESS_CREATE</td>
<td>DeleteConnectHarness</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>CONNECT_HARNESS_DELETE</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

### Permissions Required for Each API Operation

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListStreams</td>
<td>STREAM_INSPECT</td>
</tr>
<tr>
<td>CreateStream</td>
<td>STREAM_CREATE</td>
</tr>
<tr>
<td>GetStream</td>
<td>STREAM_READ</td>
</tr>
<tr>
<td>DeleteStream</td>
<td>STREAM_DELETE</td>
</tr>
<tr>
<td>GetMessages</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>PutMessages</td>
<td>STREAM_PRODUCE</td>
</tr>
<tr>
<td>UpdateStream</td>
<td>STREAM_UPDATE</td>
</tr>
<tr>
<td>CreateCursor</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>CreateGroupCursor</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>GetGroup</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>UpdateGroup</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>ConsumerHeartbeat</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>ConsumerCommit</td>
<td>STREAM_CONSUME</td>
</tr>
<tr>
<td>ListStreamPools</td>
<td>STREAM_POOL_INSPECT</td>
</tr>
<tr>
<td>CreateStreamPool</td>
<td>STREAM_POOL_CREATE</td>
</tr>
<tr>
<td>GetStreamPool</td>
<td>STREAM_POOL_READ</td>
</tr>
<tr>
<td>DeleteStreamPool</td>
<td>STREAM_POOL_DELETE</td>
</tr>
<tr>
<td>MoveStreamPool</td>
<td>STREAM_POOL_MOVE</td>
</tr>
<tr>
<td>UpdateStreamPool</td>
<td>STREAM_POOL_UPDATE</td>
</tr>
<tr>
<td>ListConnectHarnesses</td>
<td>CONNECT_HARNESS_INSPECT</td>
</tr>
<tr>
<td>CreateConnectHarness</td>
<td>CONNECT_HARNESS_CREATE</td>
</tr>
<tr>
<td>GetConnectHarness</td>
<td>CONNECT_HARNESS_READ</td>
</tr>
<tr>
<td>DeleteConnectHarness</td>
<td>CONNECT_HARNESS_DELETE</td>
</tr>
<tr>
<td>MoveConnectHarness</td>
<td>CONNECT_HARNESS_MOVE</td>
</tr>
<tr>
<td>UpdateConnectHarness</td>
<td>CONNECT_HARNESS_UPDATE</td>
</tr>
</tbody>
</table>

**Details for the Vault Service**

This topic covers details for writing policies to control access to the Vault service.

**Individual Resource-Types**

- vaults
- keys
- key-delegate
- secrets
- secret-versions
- secret-bundles

**Aggregate Resource-Type**

- secret-family

A policy that uses `<verb> secret-family` is equivalent to writing one with a separate `<verb>` `<individual resource-type>` statement for each of the individual secret resource-types. (Secret resource-types include only secrets, secret-versions, and secret-bundles.)

See the table in **Details for Verb + Resource-Type Combinations** on page 2348 for details of the API operations covered by each verb, for each individual resource-type included in `secret-family`.

**Supported Variables**

Vault supports all the general variables, plus the ones listed here. For more information about general variables supported by Oracle Cloud Infrastructure services, see **General Variables for All Requests** on page 2169.
### Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>request.includePlainTextKey</td>
<td>String</td>
<td>Use this variable to control whether to return the plaintext key, in addition to the encrypted key, in response to a request to generate a data encryption key.</td>
</tr>
<tr>
<td>request.kms-key.id</td>
<td>String</td>
<td>Use this variable to control whether block volumes or buckets can be created without a Vault master encryption key.</td>
</tr>
<tr>
<td>target.boot-volume.kms-key.id</td>
<td>String</td>
<td>Use this variable to control whether Compute instances can be launched with boot volumes that were created without a Vault master encryption key.</td>
</tr>
<tr>
<td>target.key.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific keys by OCID.</td>
</tr>
<tr>
<td>target.vault.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific vaults by OCID.</td>
</tr>
<tr>
<td>target.secret.name</td>
<td>String</td>
<td>Use this variable to control access to specific secrets, secret versions, and secret bundles by name.</td>
</tr>
<tr>
<td>target.secret.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific secrets, secret versions, and secret bundles by OCID.</td>
</tr>
</tbody>
</table>

### Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from inspect > read > use > manage. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the use verb for the keys resource-type includes the same permissions and API operations as the read verb, plus the KEY_ENCRYPT and KEY_DECRYPT permissions and a number of API operations (Encrypt, Decrypt, and GenerateDataEncryptionKey). The manage verb allows even more permissions and API operations when compared to the use verb.

#### vaults

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>VAULT_INSPECT</td>
<td>ListVaults</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>VAULT_READ</td>
<td>GetVault</td>
<td></td>
</tr>
</tbody>
</table>
### Verbs

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>no extra</td>
<td>CreateKey (also needs manage keys)</td>
</tr>
<tr>
<td></td>
<td>VAULT_CREATE_KEY</td>
<td></td>
<td>ImportKey (also needs manage keys)</td>
</tr>
<tr>
<td></td>
<td>VAULT_IMPORT_KEY</td>
<td></td>
<td>CreateSecret (also needs manage secrets)</td>
</tr>
<tr>
<td></td>
<td>VAULT_CREATE_SECRET</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>VAULT_CREATE</td>
<td>CreateVault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAULT_UPDATE</td>
<td>UpdateVault</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAULT_DELETE</td>
<td>ScheduleVaultDeletion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAULT_MOVE</td>
<td>CancelVaultDeletion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAULT_BACKUP</td>
<td>ChangeVaultCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAULT_RESTORE</td>
<td>BackupVault</td>
<td>RestoreVaultFromFile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RestoreVaultFromObjectStore</td>
</tr>
</tbody>
</table>

### keys

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>KEY_INSPECT</td>
<td>ListKeys</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListKeyVersions</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPeCT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>KEY_READ</td>
<td>GetKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetKeyVersion</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>KEY_ENCRYPT</td>
<td>Encrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_DECRYPT</td>
<td>GenerateDataEncryptionKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_EXPORT</td>
<td>Decrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_SIGN</td>
<td>ExportKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_VERIFY</td>
<td>Sign</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify</td>
<td></td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>CreateKey (also needs use vaults)</td>
</tr>
<tr>
<td></td>
<td>KEY_CREATE</td>
<td>UpdateKey</td>
<td>ImportKey (also needs use vaults)</td>
</tr>
<tr>
<td></td>
<td>KEY_UPDATE</td>
<td>DisableKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_ROTATE</td>
<td>EnableKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_DELETE</td>
<td>CreateKeyVersion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_MOVE</td>
<td>ScheduleKeyDeletion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_IMPORT</td>
<td>CancelKeyDeletion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_BACKUP</td>
<td>ChangeKeyCompartment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KEY_RESTORE</td>
<td>ImportKeyVersion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BackupKey</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RestoreKeyFromFile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RestoreKeyFromObjectStore</td>
<td></td>
</tr>
</tbody>
</table>

**key-delegate**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>KEY_ASSOCIATE</td>
<td>Encrypt</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>KEY_DISASSOCIATE</td>
<td>GenerateDataEncryptionKey</td>
<td>Decrypt</td>
</tr>
</tbody>
</table>

**secrets**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SECRET_INSPECT</td>
<td>ListSecrets</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>SECRET_READ</td>
<td>GetSecret</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECRET_UPDATE</td>
<td>UpdateSecret</td>
<td>ChangeSecretCompartment (also needs manage secrets)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ScheduleSecretVersionDeletion (also needs manage secret-versions)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CancelSecretVersionDeletion (also needs manage secret-versions)</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>USE +</td>
</tr>
<tr>
<td></td>
<td>SECRET_CREATE</td>
<td>ScheduleSecretDeletion</td>
<td>CreateSecret</td>
</tr>
<tr>
<td></td>
<td>SECRET_DELETE</td>
<td>CancelSecretDeletion</td>
<td>ChangeSecretCompartment</td>
</tr>
<tr>
<td></td>
<td>SECRET_MOVE</td>
<td></td>
<td>(also needs use secrets)</td>
</tr>
</tbody>
</table>

**secret-versions**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>ListSecretVersions</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>SECRET_VERSION_READ</td>
<td>GetKeyVersion</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>READ +</td>
<td>no extra</td>
<td>ScheduleSecretVersionDeletion</td>
</tr>
<tr>
<td></td>
<td>SECRET_VERSION_DELETE</td>
<td></td>
<td>(also needs use secrets)</td>
</tr>
</tbody>
</table>

**secret-bundles**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td></td>
<td>ListSecretBundles</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>SECRET_BUNDLE_READ</td>
<td>GetSecretBundle</td>
<td></td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see `Permissions` on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListVaults</td>
<td>VAULT_INSPECT</td>
</tr>
<tr>
<td>GetVault</td>
<td>VAULT_READ</td>
</tr>
<tr>
<td>CreateVault</td>
<td>VAULT_CREATE</td>
</tr>
<tr>
<td>UpdateVault</td>
<td>VAULT_UPDATE</td>
</tr>
<tr>
<td>ScheduleVaultDeletion</td>
<td>VAULT_DELETE</td>
</tr>
<tr>
<td>CancelVaultDeletion</td>
<td>VAULT_DELETE</td>
</tr>
<tr>
<td>ChangeVaultCompartment</td>
<td>VAULT_MOVE</td>
</tr>
<tr>
<td>BackupVault</td>
<td>VAULT_BACKUP</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>RestoreVaultFromFile</td>
<td>VAULT_RESTORE</td>
</tr>
<tr>
<td>RestoreVaultFromObjectStore</td>
<td>VAULT_RESTORE</td>
</tr>
<tr>
<td>ListKeys</td>
<td>KEY_INSPECT</td>
</tr>
<tr>
<td>ListKeyVersions</td>
<td>KEY_INSPECT</td>
</tr>
<tr>
<td>GetKey</td>
<td>KEY_READ</td>
</tr>
<tr>
<td>CreateKey</td>
<td>KEY_CREATE and VAULT_CREATE_KEY</td>
</tr>
<tr>
<td>EnableKey</td>
<td>KEY_UPDATE</td>
</tr>
<tr>
<td>DisableKey</td>
<td>KEY_UPDATE</td>
</tr>
<tr>
<td>UpdateKey</td>
<td>KEY_UPDATE</td>
</tr>
<tr>
<td>ScheduleKeyDeletion</td>
<td>KEY_DELETE</td>
</tr>
<tr>
<td>CancelKeyDeletion</td>
<td>KEY_DELETE</td>
</tr>
<tr>
<td>ChangeKeyCompartment</td>
<td>KEY_MOVE</td>
</tr>
<tr>
<td>BackupKey</td>
<td>KEY_BACKUP</td>
</tr>
<tr>
<td>RestoreKeyFromFile</td>
<td>KEY_RESTORE</td>
</tr>
<tr>
<td>RestoreKeyFromObjectStore</td>
<td>KEY_RESTORE</td>
</tr>
<tr>
<td>GetKeyVersion</td>
<td>KEY_READ</td>
</tr>
<tr>
<td>CreateKeyVersion</td>
<td>KEY_ROTATE</td>
</tr>
<tr>
<td>ImportKey</td>
<td>KEY_IMPORT and VAULT_IMPORT_KEY</td>
</tr>
<tr>
<td>ImportKeyVersion</td>
<td>KEY_IMPORT</td>
</tr>
<tr>
<td>ExportKey</td>
<td>KEY_EXPORT</td>
</tr>
<tr>
<td>GenerateDataEncryptionKey</td>
<td>KEY_ENCRYPT</td>
</tr>
<tr>
<td>Encrypt</td>
<td>KEY_ENCRYPT</td>
</tr>
<tr>
<td>Decrypt</td>
<td>KEY_DECRYPT</td>
</tr>
<tr>
<td>Sign</td>
<td>KEY_SIGN</td>
</tr>
<tr>
<td>Verify</td>
<td>KEY_VERIFY</td>
</tr>
<tr>
<td>CreateSecret</td>
<td>SECRET_CREATE and VAULT_CREATE_SECRET</td>
</tr>
<tr>
<td>UpdateSecret</td>
<td>SECRET_UPDATE</td>
</tr>
<tr>
<td>ListSecrets</td>
<td>SECRET_INSPECT</td>
</tr>
<tr>
<td>GetSecret</td>
<td>SECRET_READ</td>
</tr>
<tr>
<td>ScheduleSecretDeletion</td>
<td>SECRET_DELETE</td>
</tr>
<tr>
<td>ChangeSecretCompartment</td>
<td>SECRET_MOVE and SECRET_UPDATE</td>
</tr>
<tr>
<td>ListSecretVersions</td>
<td>SECRET_VERSION_INSPECT</td>
</tr>
<tr>
<td>GetSecretVersion</td>
<td>SECRET_VERSION_READ</td>
</tr>
<tr>
<td>ScheduleSecretVersionDeletion</td>
<td>SECRET_VERSION_DELETE and SECRET_UPDATE</td>
</tr>
</tbody>
</table>
### API Operation

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CancelSecretVersionDeletion</td>
<td>SECRET_VERSION_DELETE and SECRET_UPDATE</td>
</tr>
<tr>
<td>ListSecretBundles</td>
<td>SECRET_BUNDLE_INSPECT</td>
</tr>
<tr>
<td>GetSecretBundle</td>
<td>SECRET_BUNDLE_READ</td>
</tr>
</tbody>
</table>

### Details for the WAF Service

This topic covers details for writing policies to control access to the WAAS service.

#### Aggregate Resource-Type

waas-family

#### Individual Resource-Types

- waas-policy
- waas-certificate
- waas-work-request
- waas-metering
- waas-custom-protection-rule
- waas-address-list
- http-redirects

#### Comments

A policy that uses `<verb> waas` is equivalent to writing one with a separate `<verb> <individual resource-type>` statement for each of the individual resource-types.

See the table in Details for Verb + Resource-Type Combinations on page 2354 for details of the API operations covered by each verb, for each individual resource-type included in `waas`.

#### Supported Variables

The WAF Service supports all the general variables (see General Variables for All Requests on page 2169), plus the ones listed here.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.waas-policy.id</td>
<td>Entity (OCID)</td>
<td>Use this variable to control access to specific WAAS policies by OCID.</td>
</tr>
<tr>
<td>target.waf-rule-key</td>
<td>String</td>
<td>Use this variable to control access to specific WAF rules by name.</td>
</tr>
<tr>
<td>target.waas-work-request.id</td>
<td>Entity (OCID)</td>
<td>The OCID of WAAS work requests.</td>
</tr>
<tr>
<td>target.waas-policy-certificate.id</td>
<td>Entity (OCID)</td>
<td>The OCID of SSL certificates configured in a WAAS policy.</td>
</tr>
<tr>
<td>target.certificate.destination-compartment.id</td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
<tr>
<td>target.certificate.source-compartment.id</td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
</tbody>
</table>
### Details for Verb + Resource-Type Combinations

The following tables show the permissions and API operations covered by each verb. The level of access is cumulative as you go from `inspect` > `read` > `use` > `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the `use` and `manage` verbs for the `waas-policy` resource-type cover no extra permissions or API operations compared to the `read` verb.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Variable Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>target.waas-policy.destination-compartment.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
<tr>
<td><code>target.waas-policy.source-compartment.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
<tr>
<td><code>target.waas-custom-protection-rule.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of a custom protection rule.</td>
</tr>
<tr>
<td><code>target.waas-custom-protection-rule.destination-compartment.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
<tr>
<td><code>target.waas-address-list.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of an address list.</td>
</tr>
<tr>
<td><code>target.waas-address-list.source-compartment.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
<tr>
<td><code>target.waas-address-list.destination-compartment.id</code></td>
<td>Entity (OCID)</td>
<td>The OCID of a compartment.</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>inspect</td>
<td>WAAS_POLICY_INSPECT</td>
<td>ListWaasPolicies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWaasOriginRequestCidrs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListReports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWafReports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ListWafRules</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + WAAS_POLICY_READ</td>
<td>GetWaasPolicy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafTraffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafBlocked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafRequests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafSettings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetAccessRules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetCaptcha</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetDeviceFingerprintChallenge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetHumanInteractionChallenge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetJSChallenge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetIpRateLimiting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetGoodBots</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafWhitelists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafRecommendations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetWafRule</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetThreatFeeds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetAlerts</td>
</tr>
</tbody>
</table>

**waas-policy**
<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>use</td>
<td>READ +</td>
<td>READ +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>WAAS_POLICY_UPDATE</td>
<td>UpdateWaasPolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateWafSettings</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateAccessRules</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateCaptchas</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateDeviceFingerprintChallenge</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateHumanInteractionChallenge</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateJSChallenge</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateIpRateLimiting</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateGoodBots</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateWafWhitelists</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AcceptWafRecommendations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateWafRuleActions</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UpdateThreatFeedAction</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>WAAS_POLICY_CREATE</td>
<td>CreateWaasPolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAAS_POLICY_DELETE</td>
<td>DeleteWaasPolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAAS_POLICY_MOVE</td>
<td>ChangeWaasPolicyCompartment</td>
<td></td>
</tr>
</tbody>
</table>

**waas-certificate**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>WAAS_CERTIFICATE_INSPECT</td>
<td>ListCertificates</td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>INSPECT +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GetCertificate</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td>no extra</td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>USE +</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>WAAS_CERTIFICATE_CREATE</td>
<td>CreateCertificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAAS_CERTIFICATE_DELETE</td>
<td>DeleteCertificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAAS_CERTIFICATE_MOVE</td>
<td>ChangeCertificateCompartment</td>
<td></td>
</tr>
</tbody>
</table>

**waas-work-request**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>WAAS_WORK_REQUEST_INSPECT</td>
<td>ListWorkRequests</td>
<td>none</td>
</tr>
<tr>
<td>Verbs</td>
<td>Permissions</td>
<td>APIs Fully Covered</td>
<td>APIs Partially Covered</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td>WAAS_WORK_REQUEST_READ</td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>no extra</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td>WAAS_WORK_REQUEST_DELETE</td>
<td>none</td>
</tr>
</tbody>
</table>

### waas-metering

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>WAAS_METERING_READ</td>
<td>GetWafReport</td>
<td>none</td>
</tr>
</tbody>
</table>

### waas-custom-protection-rule

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>

### waas-address-list

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>WAAS_ADDRESS_LIST_INSPECT</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>read</td>
<td>INSPECT +</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>use</td>
<td>READ +</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>manage</td>
<td>USE +</td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>
**http-redirects**

<table>
<thead>
<tr>
<th>Verbs</th>
<th>Permissions</th>
<th>APIs Fully Covered</th>
<th>APIs Partially Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>HTTPREDIRECT_INSPECT ListHttpRedirects</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>INSPECT + HTTPREDIRECT_READ GetHttpRedirect</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>use</td>
<td>READ + HTTPREDIRECT_UPDATE UpdateHttpRedirect</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>manage</td>
<td>USE + HTTPREDIRECT_CREATE CreateHttpRedirect HTTPREDIRECT_DELETE DeleteHttpRedirect HTTPREDIRECT_MOVE ChangeHttpRedirectCompartment</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**Permissions Required for Each API Operation**

The following table lists the API operations in a logical order, grouped by resource type.

For information about permissions, see Permissions on page 2162.

<table>
<thead>
<tr>
<th>API Operation</th>
<th>Permissions Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateWaasPolicy</td>
<td>WAAS_POLICY_CREATE</td>
</tr>
<tr>
<td>ListWaasPolicies</td>
<td>WAAS_POLICY_INSPECT</td>
</tr>
<tr>
<td>GetWaasPolicy</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateWaasPolicy</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>DeleteWaasPolicy</td>
<td>WAAS_POLICY_DELETE</td>
</tr>
<tr>
<td>ChangeWaasPolicyCompartment</td>
<td>WAAS_POLICY_MOVE</td>
</tr>
<tr>
<td>ListReports</td>
<td>WAAS_POLICY_INSPECT</td>
</tr>
<tr>
<td>ListWafReports</td>
<td>WAAS_POLICY_INSPECT</td>
</tr>
<tr>
<td>GetWafTraffic</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>GetWafBlocked</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>GetWafRequests</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>GetWafSettings</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateWafSettings</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetAccessRules</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateAccessRules</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetCaptchas</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateCaptchas</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetDeviceFingerprintChallenge</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>UpdateDeviceFingerprintChallenge</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetHumanInteractionChallenge</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateHumanInteractionChallenge</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetJsChallenge</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateJsChallenge</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetIpRateLimiting</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateIpRateLimiting</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetGoodBots</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateGoodBots</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetWafWhitelists</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateWafWhitelists</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetWafRecommendations</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>AcceptWafRecommendions</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>ListWafRules</td>
<td>WAAS_POLICY_INSPECT</td>
</tr>
<tr>
<td>UpdateWafRuleActions</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetWafRule</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>GetThreatFeeds</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>UpdateThreatFeedAction</td>
<td>WAAS_POLICY_UPDATE</td>
</tr>
<tr>
<td>GetAlerts</td>
<td>WAAS_POLICY_READ</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>WAAS_WORK_REQUEST_INSPECT</td>
</tr>
<tr>
<td>ListWaasOriginRequestCidrs</td>
<td>WAAS_POLICY_INSPECT</td>
</tr>
<tr>
<td>GetWorkRequestDetails</td>
<td>WAAS_WORK_REQUEST_READ</td>
</tr>
<tr>
<td>DeleteWorkRequest</td>
<td>WAAS_WORK_REQUEST_DELETE</td>
</tr>
<tr>
<td>CreateCertificate</td>
<td>WAAS_CERTIFICATE_CREATE</td>
</tr>
<tr>
<td>ListCertificates</td>
<td>WAAS_CERTIFICATE_INSPECT</td>
</tr>
<tr>
<td>GetCertificate</td>
<td>WAAS_CERTIFICATE_READ</td>
</tr>
<tr>
<td>DeleteCertificate</td>
<td>WAAS_CERTIFICATE_DELETE</td>
</tr>
<tr>
<td>ChangeCertificateCompartment</td>
<td>WAAS_CERTIFICATE_MOVE</td>
</tr>
<tr>
<td>GetWafReport</td>
<td>WAAS_METERING_READ</td>
</tr>
<tr>
<td>CreateCustomProtectionRule</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_CREATE</td>
</tr>
<tr>
<td>ListCustomProtectionRules</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_CREATE</td>
</tr>
<tr>
<td>GetCustomProtectionRule</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_CREATE</td>
</tr>
<tr>
<td>UpdateCustomProtectionRule</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_UPDATE</td>
</tr>
<tr>
<td>DeleteCustomProtectionRule</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_DELETE</td>
</tr>
<tr>
<td>API Operation</td>
<td>Permissions Required to Use the Operation</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>ChangeCustomProtectionRuleCompartment</td>
<td>WAAS_CUSTOM_PROTECTION_RULE_MOVE</td>
</tr>
<tr>
<td>CreateAddressList</td>
<td>WAAS_ADDRESS_LIST_CREATE</td>
</tr>
<tr>
<td>GetAddressList</td>
<td>WAAS_ADDRESS_LIST_READ</td>
</tr>
<tr>
<td>ListAddressLists</td>
<td>WAAS_ADDRESS_LIST_INSPECT</td>
</tr>
<tr>
<td>ChangeAddressListCompartment</td>
<td>WAAS_ADDRESS_LIST_MOVE</td>
</tr>
<tr>
<td>UpdateAddressList</td>
<td>WAAS_ADDRESS_LIST_UPDATE</td>
</tr>
<tr>
<td>DeleteAddressList</td>
<td>WAAS_ADDRESS_LIST_DELETE</td>
</tr>
<tr>
<td>ListHttpRedirects</td>
<td>HTTPREDIRECT_INSPECT</td>
</tr>
<tr>
<td>GetHttpRedirect</td>
<td>HTTPREDIRECT_READ</td>
</tr>
<tr>
<td>CreateHttpRedirect</td>
<td>HTTPREDIRECT_CREATE</td>
</tr>
<tr>
<td>UpdateHttpRedirect</td>
<td>HTTPREDIRECT_UPDATE</td>
</tr>
<tr>
<td>DeleteHttpRedirect</td>
<td>HTTPREDIRECT_DELETE</td>
</tr>
<tr>
<td>ChangeHttpRedirectCompartment</td>
<td>HTTPREDIRECT_MOVE</td>
</tr>
</tbody>
</table>

### User Credentials

There are several types of credentials that you manage with Oracle Cloud Infrastructure Identity and Access Management (IAM):

- **Console password**: For signing in to the Console, the user interface for interacting with Oracle Cloud Infrastructure. Note that federated users can't have Console passwords because they sign in through their identity provider. See [Federating with Identity Providers](#) on page 2362.
- **API signing key (in PEM format)**: For sending API requests, which require authentication.
- **Auth token**: An Oracle-generated token that you can use to authenticate with third-party APIs. For example, use an auth token to authenticate with a Swift client when using Recovery Manager (RMAN) to back up an Oracle Database System (DB System) database to Object Storage.
- **Customer Secret Keys**: For using the Amazon S3 Compatibility API with Object Storage. See [Amazon S3 Compatibility API](#) on page 3493.
- **OAuth 2.0 Client Credentials**: For interacting with the APIs of those services that use OAuth 2.0 authorization. See [OAuth 2.0 Client Credentials](#) on page 2362.
- **SMTP Credentials**: For using the Email Delivery service.

#### Important:

API signing keys are different from the SSH keys you use to access a compute instance (see [Security Credentials](#) on page 179). For more information about API signing keys, see [Required Keys and OCIDs](#) on page 4179. For more information about instance SSH keys, see [Managing Key Pairs](#).

### User Password

The administrator who creates a new user in IAM also needs to generate a one-time Console password for the user (see [To create or reset another user's Console password](#) on page 2460). The administrator needs to securely deliver the password to the user by providing it verbally, printing it out, or sending it through a secure email service.
When the user signs in to the Console the first time, they'll be immediately prompted to change the password. If the user waits more than 7 days to initially sign in and change the password, it will expire and an administrator will need to create a new one-time password for the user.

Once the user successfully signs in to the Console, they can use Oracle Cloud Infrastructure resources according to permissions they've been granted through policies.

**Note:**
A user automatically has the ability to change their password in the Console. An administrator does not need to create a policy to give a user that ability.

### Changing a Password

If a user wants to change their own password *sometime after* they change their initial one-time password, they can do it in the Console. Remember that a user can automatically change *their own* password; an administrator does not need to create a policy to give the user that ability.

For more information, see To change your Console password on page 2459.

### If a User Needs Their Console Password Reset

If a user forgets their Console password and also has no access to the API, they can use the Console’s **Forgot Password** link to have a temporary password sent to them. This option is available if the user has an email address in their user profile.

If the user does not have an email address in their user profile, then they need to ask an administrator to reset their password for them. All administrators (and anyone else who has permission to the tenancy) can reset Console passwords. The process of resetting the password generates a new one-time password that the administrator needs to deliver to the user. The user will need to change their password the next time they sign in to the Console.

If you're an administrator who needs to reset a user's Console password, see To create or reset another user's Console password on page 2460.

### If a User Is Blocked from Signing In to the Console

If a user tries 10 times in a row to sign in to the Console unsuccessfully, they will be automatically blocked from further attempts. They'll need to contact an administrator to get unblocked (see To unblock a user on page 2460).

### API Signing Keys

A user who needs to make API requests must have an **RSA public key in PEM format (minimum 2048 bits)** added to their IAM user profile and sign the API requests with the corresponding private key (see Required Keys and OCIDs on page 4179).

**Important:**
A user automatically has the ability to generate and manage *their own* API keys in the Console or API. An administrator does not need to write a policy to give the user that ability. Remember that a user can't use the API to change or delete their own credentials until they themselves save a key in the Console, or an administrator adds a key for that user in the Console or the API.

If you have a non-human system that needs to make API requests, an administrator needs to create a user for that system and then add a public key to the IAM service for the system. There's no need to generate a Console password for the user.

For instructions on generating an API key, see To add an API signing key on page 2461.
OAuth 2.0 Client Credentials

**Note:**

OAuth 2.0 Client Credentials are not available in the United Kingdom Government Cloud (OC4).

OAuth 2.0 client credentials are required to interact programmatically with those services that use the OAuth 2.0 authorization protocol. The credentials enable you to obtain a secure token to access those service REST API endpoints. The allowed actions and endpoints granted by the token depend on the scopes (permissions) that you select when you generate the credentials. For more information, see Working with OAuth 2.0 Client Credentials on page 2457.

Auth Tokens

Auth tokens are authentication tokens generated by Oracle. You use auth tokens to authenticate with third-party APIs that do not support the Oracle Cloud Infrastructure signature-based authentication, for example, the Swift API. If your service requires an auth token, the service-specific documentation instructs you to generate one and how to use it.

Federating with Identity Providers

This topic describes identity federation concepts. Oracle Cloud Infrastructure supports federation with Oracle Identity Cloud Service, and Microsoft Active Directory (via Active Directory Federation Services (AD FS)), Microsoft Azure Active Directory, Okta, and other identity providers that supports the Security Assertion Markup Language (SAML) 2.0 protocol.

Overview

Enterprise companies commonly use an *identity provider (IdP)* to manage user login/passwords and to authenticate users for access to secure websites, services, and resources.

When someone in your company wants to use Oracle Cloud Infrastructure resources in the Console, they must sign in with a user login and password. Your administrators can federate with a supported IdP so that each employee can use an existing login and password and not have to create a new set to use Oracle Cloud Infrastructure resources.

To federate, an administrator goes through a short process to set up a relationship between the IdP and Oracle Cloud Infrastructure (commonly referred to as a *federation trust*). After an administrator sets up that relationship, any person in your company who goes to the Oracle Cloud Infrastructure Console is prompted with a "single sign-on" experience provided by the IdP. The user signs in with the login/password that they’ve already set up with the IdP. The IdP authenticates the user, and then that user can access Oracle Cloud Infrastructure.

When working with your IdP, your administrator defines groups and assigns each user to one or more groups according to the type of access the user needs. Oracle Cloud Infrastructure also uses the concept of groups (in conjunction with IAM policies) to define the type of access a user has. As part of setting up the relationship with the IdP, your administrator can map each IdP group to a similarly defined IAM group, so that your company can re-use the IdP group definitions when authorizing user access to Oracle Cloud Infrastructure resources. Here’s a screenshot from the mapping process:
For information about the number of federations and group mappings you can have, see Service Limits on page 215. There’s no limit on the number of federated users.

**Note:**

Any users who are in more than 50 IdP groups cannot be authenticated to use the Oracle Cloud Infrastructure Console.

**Automated User Provisioning and Synchronization with SCIM**

Tenancies federated with Oracle Identity Cloud Service or the third-party provider Okta, can also leverage SCIM (System for Cross-domain Identity Management) to enable provisioning of federated users in Oracle Cloud Infrastructure. Federated users that have been provisioned in Oracle Cloud Infrastructure through this process can have the additional user credentials such as API keys and auth tokens that are managed in the User Settings page. This enables federated users to use the SDK and CLI, and other features that require the additional user credentials. For more information, see User Provisioning for Federated Users on page 2404.

**General Concepts**

Here’s a list of the basic concepts you need to be familiar with.

**IDP**

IdP is short for identity provider, which is a service that provides identifying credentials and authentication for users.

Tenancies created after December 18, 2017 are automatically federated with Oracle Identity Cloud Service as the IdP. Oracle Cloud Infrastructure can be federated with any IdP that supports the Security Assertion Markup Language (SAML) 2.0 protocol.

**SERVICE PROVIDER (SP)**

A service (such as an application, website, and so on) that calls upon an IdP to authenticate users. In this case, Oracle Cloud Infrastructure is the SP.

**FEDERATION TRUST**

A relationship that an administrator configures between an IdP and SP. You can use the Oracle Cloud Infrastructure Console or API to set up that relationship. Then, the specific IdP is "federated" to that SP. In the Console and API, the process of federating is thought of as adding an identity provider to the tenancy.
SAML METADATA DOCUMENT

An IdP-provided XML-based document that provides the required information to an SP to federate with that IdP. Oracle Cloud Infrastructure supports the SAML 2.0 protocol, which is an XML-based standard for sharing required information between the IdP and SP. Depending on which IdP you are federating with, you must either provide the metadata URL (see below) to this document or upload the document to Oracle Cloud Infrastructure.

METADATA URL

An IdP-provided URL that enables an SP to get required information to federate with that IdP. Oracle Cloud Infrastructure supports the SAML 2.0 protocol, which is an XML-based standard for sharing required information between the IdP and SP. The metadata URL points to the SAML metadata document the SP needs.

FEDERATED USER

Someone who signs in to use the Oracle Cloud Infrastructure Console by way of a federated IdP.

LOCAL USER

A non-federated user. In other words, someone who signs in to use the Oracle Cloud Infrastructure Console with a login and password created in Oracle Cloud Infrastructure.

GROUP MAPPING

A mapping between an IdP group and an Oracle Cloud Infrastructure group, used for the purposes of user authorization.

SCIM

SCIM (System for Cross-domain Identity Management) is an IETF standard protocol that enables user provisioning across identity systems. Oracle Cloud Infrastructure hosts a SCIM endpoint for provisioning federated users into Oracle Cloud Infrastructure. Using a SCIM client to provision users in Oracle Cloud Infrastructure enables you to assign credentials to the users in Oracle Cloud Infrastructure.

PROVISIONED (OR SYNCHRONIZED) USER

A user provisioned by the identity provider's SCIM client in Oracle Cloud Infrastructure. These users can be listed in the Oracle Cloud Infrastructure Console and can have all the Oracle Cloud Infrastructure user credentials except for a Console password.

Encrypt Assertion

Some IdPs support the encryption of the SAML assertion. When enabled, the service provider expects the SAML assertion to be encrypted by the identity provider, using the service provider's encryption key. In this case, the service provider is Oracle Cloud Infrastructure authentication service. If you choose to enable this feature of your IdP, you must also enable the feature when you set up your Federation provider in the IAM service. Note that Microsoft AD FS enables the encryption of the SAML assertion by default. If your IdP is Microsoft AD FS, you must either enable this feature in IAM or disable it for Microsoft AD FS.

Experience for Federated Users

Federated users can use the Console to access Oracle Cloud Infrastructure (according to IAM policies for the groups the users are in).

They'll be prompted to enter their Oracle Cloud Infrastructure tenant (for example, ABCCorp).

They then see a page with two sets of sign-in instructions: one for federated users and one for non-federated (Oracle Cloud Infrastructure) users. See the following screenshot.
The tenant name is shown on the left. Directly below is the sign-in area for federated users. On the right is the sign-in area for non-federated users.

Federated users choose which identity provider to use for sign-in, and then they're redirected to that identity provider's sign-in experience for authentication. After entering their login and password, they are authenticated by the IdP and redirected back to the Oracle Cloud Infrastructure Console.

The federated users (without SCIM configuration) cannot access the "User Settings" page in the Console. This page is where a user can change or reset their Console password and manage other Oracle Cloud Infrastructure credentials such as API signing keys and auth tokens.

**Experience for Federated Users with SCIM Configuration**

If your IdP has also been configured with a SCIM client, a user signed in through their identity provider can access the User Settings page and have user capabilities such as API keys, auth tokens, and other user credentials. *(Note: This is currently available for Oracle Identity Cloud Service and Okta federations only.)*

**Required IAM Policy**

To add and manage identity providers in your tenancy, you must be authorized by an IAM policy. If you're in the Administrators group, then you have the required access.

Here's a more limited policy that restricts access to only the resources related to identity providers and group mappings:

```
Allow group IdPAdmins to manage identity-providers in tenancy
Allow group IdPAdmins to manage groups in tenancy
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.
Supported Identity Providers

**Important:**

Oracle Cloud Infrastructure tenancies created December 18, 2017 or later are automatically federated with Oracle Identity Cloud Service.

If your tenancy was created before December 18, 2017, and you want to set up a federation with Oracle Identity Cloud Service, see Federating with Oracle Identity Cloud Service on page 2366.

For instructions for federating with other identity providers, see the following:

Federating with Microsoft Active Directory on page 2385
Federating with Microsoft Azure Active Directory on page 2391
Cloud Infrastructure Okta Configuration for Federation and Provisioning (white paper)
Federating with SAML 2.0 Identity Providers on page 2401

**Federating with Oracle Identity Cloud Service**

This topic points to the appropriate topics for federating Oracle Cloud Infrastructure with Oracle Identity Cloud Service depending on when you activated your tenancy.

**Tenancies created December 21, 2018 and after**

These tenancies are automatically federated with Oracle Identity Cloud Service and configured to provision federated users in Oracle Cloud Infrastructure.

To manage your federated users and groups, see Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372.

For information about the federation, see Frequently Asked Questions for Oracle Identity Cloud Service Federated Users on page 2383.

**Tenancies created between December 18, 2017 and December 20, 2018**

These tenancies are automatically federated with Oracle Identity Cloud Service but are not configured to provision federated users in Oracle Cloud Infrastructure to allow these users to have additional credentials (API keys, auth tokens, etc.).

To enable this feature for users, you need to perform a one-time upgrade, see: User Provisioning for Federated Users on page 2404.

After you have performed this upgrade, see Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372 to manage your federated users and groups.

**Tenancies created before December 18, 2017**

These tenancies must be manually federated with Oracle Identity Cloud Service. See Federating with Oracle Identity Cloud Service on page 2366 described below.

**Manually Federating with Oracle Identity Cloud Service**

Your organization can have multiple Oracle Identity Cloud Service accounts (e.g., one for each division of the organization). You can federate multiple Identity Cloud Service accounts with Oracle Cloud Infrastructure, but each federation trust that you set up must be for a single Identity Cloud Service account.

**Note:**

Before following the steps in this topic, see Federating with Identity Providers on page 2362 to ensure that you understand general federation concepts.
Components of the Manual Federation to Understand

Web Application and Client Credentials

For each trust, you must set up a web application in Oracle Identity Cloud Service (also called a trusted application); instructions are in Instructions for Federating with Oracle Identity Cloud Service on page 2367. The resulting application has a set of client credentials (a client ID and client secret). When you federate your Identity Cloud Service account with Oracle Cloud Infrastructure, you must provide these credentials.

COMPUTEBAREMETAL application

A trusted application in Oracle Identity Cloud Service that contains the set of client credentials (a client ID and client secret) you'll need to provide when you federate your Identity Cloud Service account with Oracle Cloud Infrastructure.

Required URLs

The easiest way to federate with Oracle Identity Cloud Service is through the Oracle Cloud Infrastructure Console, although you could do it programmatically with the API. If you're using the Console, you're asked to provide a base URL instead of the metadata URL. The base URL is the left-most part of the URL in the browser window when you're signed in to the Identity Cloud Service console:

- **Base URL:** `<Identity Cloud Service account name>.identity.oraclecloud.com`

If you're using the API to federate, you need to provide the metadata URL, which is the base URL with /fed/v1/ metadata appended, like so:

- **Metadata URL:** `<Identity Cloud Service account name>.identity.oraclecloud.com/fed/v1/metadata`

The metadata URL links directly to the IdP-provided XML required to federate. If you're using the API, you need to provide both the metadata URL and the metadata itself when federating. For more information, see Managing Identity Providers in the API on page 2371.

OCI-V2-<tenancy_name> app

When you manually federate an Oracle Identity Cloud Service account with Oracle Cloud Infrastructure, a new SAML application called OCI-V2-<tenancy_name> is automatically created in that Oracle Identity Cloud Service account. If you later need to delete the Oracle Identity Cloud Service identity provider from your Oracle Cloud Infrastructure tenancy, make sure to also delete the OCI-V2-<tenancy_name> from Oracle Identity Cloud Service. If you don't, and you later try to federate the same Oracle Identity Cloud Service account again, you'll get a 409 error saying that an application with the same name already exists (that is, OCI-V2-<tenancy_name>).

Provisioned User

A provisioned user is provisioned by Oracle Identity Cloud Service in Oracle Cloud Infrastructure and is synched to a federated user that is managed in Oracle Identity Cloud Service. The provisioned user can have the special Oracle Cloud Infrastructure credentials like API keys and auth tokens to enable programmatic access. Provisioned users cannot have Console passwords.

Instructions for Federating with Oracle Identity Cloud Service

Following is the general process an administrator goes through to set up the identity provider, and below are instructions for each step. It's assumed that the administrator is an Oracle Cloud Infrastructure user with the required credentials and access.

1. Sign in to Oracle Identity Cloud Service. Perform one of the following, as appropriate:
   - **Option A:** Get the required information from the COMPUTEBAREMETAL application you'll need to perform the set up steps in Oracle Cloud Infrastructure.
   - **Option B:** If Oracle Identity Cloud Service does not include the COMPUTEBAREMETAL application, set up a trusted application.

2. In Oracle Cloud Infrastructure, set up the federation:
   - **a.** Set up Oracle Identity Cloud Service as an identity provider.
   - **b.** Map Oracle Identity Cloud Service groups to IAM groups.
3. In Oracle Cloud Infrastructure, set up the IAM policies for the IAM groups to define the access you want the members of the mapped groups to have.


   **Step 1: Get required information from Oracle Identity Cloud Service**

**Option A: Get information from the COMPUTEBAREMETAL application**

1. Go to the Oracle Identity Cloud Service console and sign in with admin privileges. Make sure you're viewing the Admin Console.
2. In the Identity Cloud Service console, click **Applications**. The list of trusted applications is displayed.
3. Click COMPUTEBAREMETAL. If your instance does not include the COMPUTEBAREMETAL application, perform **Step 1 Option B**, instead.
4. Click **Configuration**.
5. Expand **General Information**. The client ID is displayed. Click **Show Secret** to display the client secret.

   ![Oracle Identity Cloud Service Console](image)

6. Record the Client ID and Client Secret. They look similar to this:
   - Client ID: de06b81cb45a45a8acdcde923402a9389d8
   - Client Secret: 8a297afd-66df-49ee-c67d-39fcdf3d1c31

**Option B: Set up a trusted application and get required information from Oracle Identity Cloud Service**

Perform this step only if you were unable to complete Step 1 Option A.

**Summary**: For Oracle Identity Cloud Service, you need to create a confidential application (also referred to as a trusted application) with particular properties described in the following instructions. For the general Oracle Identity Cloud Service documentation, see Add a Confidential Application.

**Instructions for Oracle Identity Cloud Service**:

1. Go to the Oracle Identity Cloud Service console and sign in with privileges to create the application. Make sure you're viewing the Admin Console.
2. **Add a confidential (or trusted) application**, which enables secure, programmatic interaction between Oracle Cloud Infrastructure and Oracle Identity Cloud Service. Specify these items when setting up the application:

   a. On the first page:
      1. Enter an application a name (e.g., Oracle Cloud Infrastructure Federation).
      2. Leave other fields empty or unselected.
   b. On the next page:
      1. Select **Configure this application as a client now**.
      2. For the **Allowed Grant Types**, select the check box for **Client Credentials**.
      3. Leave other fields empty.
      4. At the bottom of the page:
         a. Select the check box for **Grant the client access to Identity Cloud Service Admin APIs**.
         b. Select **Identity Domain Administrator** from the list of roles.
   c. On the next page, leave any fields empty or unselected and continue until you click **Finish**.
   d. Copy and paste the displayed client credentials so you can later give them to Oracle Cloud Infrastructure when federating. You can view the application's client credentials any time in the Oracle Identity Cloud Service console. They look similar to this:
      - Client ID: de06b81cb45a45a8adcdce923402a9389d8
      - Client Secret: 8a297af6-6d6f-49ee-c67d-39fedf3d1c31

3. Record the **Oracle Identity Cloud Service base URL**, which you'll need when federating.

4. **Activate the application**.

**Step 2: Add Oracle Identity Cloud Service as an identity provider in Oracle Cloud Infrastructure**

1. Go to the **Console** and sign in with your Oracle Cloud Infrastructure login and password.
2. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
3. Click **Add identity provider**.
4. Enter the following:
   a. **Name**: A unique name for this federation trust. This is the name federated users see when choosing which identity provider to use when signing in to the Console (for example, **ABCCorp_IDCS** as shown in the screenshot in **Experience for Federated Users** on page 2364). The name must be unique across all identity providers you add to the tenancy. You cannot change this later.
   b. **Description**: A friendly description.
   c. **IDCS Base URL**: See **Required URLs** on page 2367.
   d. **Client ID**: From Step 1 Option A or Option B.
   e. **Client secret**: From Step 1 Option A or Option B.
   f. **Encrypt Assertion**: Selecting the check box lets the IAM service know to expect the encryption from the IdP. If you select this check box, you must also set up encryption of the assertion in IDCS. For more information, see **General Concepts** on page 2363. For information about setting this feature up in the IDCS, see **Managing Oracle Identity Cloud Service Applications**.
   g. **Force Authentication**: Selected by default. When selected, users are required to provide their credentials to the IdP (re-authenticate) even when they are already signed in to another session.
   h. **Authentication Context Class References**: This field is required for Government Cloud customers. When one or more values are specified, Oracle Cloud Infrastructure (the relying party) expects the identity provider to use one of the specified authentication mechanisms when authenticating the user. The returned SAML response from the IdP must contain an authentication statement with that authentication context class reference. If the SAML response authentication context does not match what is specified here, the Oracle Cloud Infrastructure auth service rejects the SAML response with a 400. Several common authentication context class references are listed in the menu. To use a different context class, select **Custom**, then manually enter the class reference.
   i. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information
about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Continue.

6. Set up the mappings between Oracle Identity Cloud Service groups and IAM groups in Oracle Cloud Infrastructure. A given Oracle Identity Cloud Service group can be mapped to zero, one, or multiple IAM groups, and vice versa. However, each individual mapping is between only a single Oracle Identity Cloud Service group and a single IAM group. Changes to group mappings take effect typically within seconds.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you don't want to set up the group mappings now, you can simply click Create and come back to add the mappings later.</td>
</tr>
</tbody>
</table>

To create a group mapping:

a. Select the Oracle Identity Cloud Service group from the list under Identity Provider Group.
b. Choose the IAM group you want to map this group to from the list under OCI Group.

c. Repeat the above sub-steps for each mapping you want to create, and then click Create.

After the Federation Set Up

The identity provider is now added to your tenancy and appears in the list on the Federation page. Click the identity provider to view its details and the group mappings you just set up.

Oracle assigns the identity provider and each group mapping a unique ID called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

In the future, come to the Federation page if you want to edit the group mappings or delete the identity provider from your tenancy.

Users that are members of the Oracle Identity Cloud Service groups mapped to the Oracle Cloud Infrastructure groups are now listed in the Console on the Users page. See Managing User Capabilities for Federated Users on page 2408 for more information on assigning these users additional credentials.

Step 3: Set up IAM policies for the groups

If you haven't already, set up IAM policies to control the access the federated users have to your organization's Oracle Cloud Infrastructure resources. For more information, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Step 4: Give your federated users the name of the tenant and URL to sign in

Give your federated users need the URL for the Oracle Cloud Infrastructure Console, https://cloud.oracle.com), and the name of your tenant. They'll be prompted to provide the tenant name when they sign in to the Console.

Managing Identity Providers in the Console

To add an Oracle Identity Cloud Service as an identity provider

See Instructions for Federating with Oracle Identity Cloud Service on page 2367.

To delete the identity provider

All the group mappings will also be deleted.
1. Delete the identity provider from your tenancy:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation. A list of the identity providers in your tenancy is displayed.
   b. Click the identity provider to view its details.
   c. Click Delete.
   d. Confirm when prompted.

2. Delete the OCI-V2-<tenancy_name> from your Oracle Identity Cloud Service account:
   a. Go to Oracle Identity Cloud Service and sign in to the federated account.
   b. Click Applications. The list of applications is displayed.
   c. Locate the OCI-V2-<tenancy_name> and click its name to view its details page.
   d. In the upper right of the page, click Deactivate. Confirm when prompted.
   e. Click Remove. Confirm when prompted.

To add group mappings for Oracle Identity Cloud Service

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation. A list of the identity providers in your tenancy is displayed.
2. Click the name you chose for your Oracle Identity Cloud Service federation to view its details.
3. Click Add Mappings.
   a. Select the Oracle Identity Cloud Service group from the list under Identity Provider Group.
   b. Choose the IAM group you want to map this group to from the list under OCI Group.
   c. To add more mappings, click +Another Mapping.
   d. When you are finished, click Add Mappings.

Your changes take effect typically within seconds in your home region. Wait several more minutes for changes to propagate to all regions.

Users that are members of the Oracle Identity Cloud Service groups mapped to the Oracle Cloud Infrastructure groups are now listed in the Console on the Users page. See Managing User Capabilities for Federated Users on page 2408 for more information on assigning these users additional credentials.

To update or delete a group mapping

You can't update a group mapping, but you can delete the mapping and add a new one.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
   A list of the identity providers in your tenancy is displayed.
2. Click the identity provider to view its details.
3. For the mapping you want to delete, select it, and then click Delete.
4. Confirm when prompted.
5. Add a new mapping, if wanted.

Your changes take effect typically within seconds in your home region. Wait several more minutes for changes to propagate to all regions.

If this action results in federated users no longer having membership in any group that is mapped to Oracle Cloud Infrastructure, the federated users' provisioned users' will also be removed from Oracle Cloud Infrastructure. Typically, this process takes several minutes.

Managing Identity Providers in the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations:

Identity providers:
IAM

- CreateIdentityProvider
- ListIdentityProviders
- GetIdentityProvider
- UpdateIdentityProvider
- DeleteIdentityProvider: Before you can use this operation, you must first use DeleteIdpGroupMapping to remove all the group mappings for the identity provider.

**Group mappings:**
- CreateIdpGroupMapping: Each group mapping is a separate entity with its own OCID.
- ListIdpGroupMappings
- GetIdpGroupMapping
- UpdateIdpGroupMapping
- DeleteIdpGroupMapping

**Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console**

This topic describes how to use the Oracle Cloud Infrastructure Console to manage your Oracle Identity Cloud Service users and groups. Before you get started, understand basic federation concepts. See Federating with Identity Providers on page 2362.

**Overview of Working with Oracle Identity Cloud Service Users and Groups in the Console**

The Oracle Cloud Infrastructure Console provides an integration with Oracle Identity Cloud Service (IDCS) that lets you perform many management tasks for your IDCS users and groups in the Console.

**User Management Tasks**

In the Console, you can do the following user management tasks:
- Add users
- Remove users
- Add users to groups
- Assign roles to users to access services and instances
- Reset user password

For information on more user management tasks, see Managing Oracle Identity Cloud Service Users in Administering Oracle Identity Cloud Service.

**Group Management Tasks**

In the Console, you can do the following group management tasks:
- Add groups
- Remove groups
- Add users to groups
- Map IDCS groups to IAM groups

For information on more group management tasks, see Managing Oracle Identity Cloud Service Groups in Administering Oracle Identity Cloud Service.

**Required Policies and Permissions**

To manage Oracle Identity Cloud Service users and groups in the Console, you'll need to be granted permissions in both the Oracle Cloud Infrastructure IAM service and in Oracle Identity Cloud Service.

Members of the OCI_Administrators group have the required permissions to create groups and policies in Oracle Cloud Infrastructure.

**Important:** To create users and groups in the Oracle Identity Cloud Service federation, you'll need the Identity Domain Administrator role, or be a member of a group that has been granted that role. For information on Oracle Identity Cloud Service roles, see Administering Oracle Identity Cloud Service.
To quickly create a user with the required permissions, see Add a User with Oracle Cloud Administrator Permissions on page 58.

**Navigating to Your Oracle Identity Cloud Service Users and Groups in the Console**

In the Console, you can add users and groups to Oracle Identity Cloud Service from the Identity Provider Details page.

To view your identity provider details:

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.

![Identity Provider Details](image)

From the Identity Provider Details page, click **Users** to display the users created in Oracle Identity Cloud Service. Click **Groups** to display the groups created in Oracle Identity Cloud Service.

**Working with Oracle Identity Cloud Service Groups**

The Console lets you perform the following tasks to manage groups in Oracle Identity Cloud Service:

- Add groups
- Delete groups
- Edit the name and description
- Add users to groups
- Remove users from groups
- Map groups to Oracle Cloud Infrastructure groups

Some tasks you can't perform in the Oracle Cloud Infrastructure Console. To add the predefined application roles for some Oracle Cloud products, you need to assign roles in the Identity Cloud Service console. For more information about using Oracle Identity Cloud Service, see Administering Oracle Identity Cloud Service.

For the members of a group in Oracle Identity Cloud Service to have permissions in Oracle Cloud Infrastructure, you must map the IDCS group to a group in IAM. Before you set up any new groups in IDCS, ensure that you understand how to assign permissions to groups in Oracle Cloud Infrastructure. See Overview of Oracle Cloud Infrastructure Identity and Access Management on page 2124.

**Working with Oracle Identity Cloud Service Users**

The Console lets you perform the following tasks to manage users in Oracle Identity Cloud Service:

- Add users
- Delete users
- Edit user details
- Add users to groups
- Add roles to users
- Remove users from groups
- Reset user passwords

**User Management Tasks You Can’t Perform in the Console**

The Oracle Cloud Console does not support management of the following Oracle Identity Cloud Service user features and tasks:

- Manage multi-factor authentication

For information about managing these tasks, see *Administering Oracle Identity Cloud Service*.

*Managing Oracle Identity Cloud Service Groups in the Console*

To create a group in Oracle Identity Cloud Service

This procedure creates a new group in Oracle Identity Cloud Service. Optionally, you can add users to the group at the time you create it. This group will not have any permissions in Oracle Cloud Infrastructure until you map it to an Oracle Cloud Infrastructure group.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**. A list of the federations in your tenancy is displayed.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named `OracleIdentityCloudService`. The identity provider details page is displayed.
3. Under **Resources**, click **Groups**.

The list of existing groups is displayed.

4. Click **Create IDCS Group**.

5. Enter the following:
   - **Name**: A unique name for the group. Avoid entering confidential information.
   - **Description**: A friendly description. You can change this later if you want to.
   - **Users**: Add Oracle Identity Cloud Service users to this group. You can add users when you create the group, or later. Select users from the list. To find a specific user, you can start typing the user name to filter the list as you type.

6. Click **Create**.

After you create a group in Oracle Identity Cloud Service, you'll want to give the group permissions to user services:

- To grant the group access to map it to an Oracle Cloud Infrastructure group as described in the next procedure.
- To add roles to this group, see *Managing Oracle Identity Cloud Service Roles for Groups* on page 2381.

To map an Oracle Identity Cloud Service group to an IAM group

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named `OracleIdentityCloudService`. The identity provider details page is displayed.
3. Click **Edit Mapping**.
4. In the **Edit Identity Provider** dialog, click **+ Add Mapping**.
5. Select the **Identity Provider Group** you want to map from the list. To find a specific group, you can start typing the group name to filter the list as you type.
6. Select the **OCI Group** you want to map this Identity Cloud Service group to. To find a specific group, you can start typing the group name to filter the list as you type.
7. To add more mappings, click **Add Mapping** and continue adding the mappings.
8. Select the group you want to map this group to from the list under **OCI Mapped User Group**.

Members of this group now have the permissions granted to the OCI Mapped User Group.

To add roles to a group
Oracle Cloud Infrastructure services use policies to control access to services. However, some Oracle Cloud services use roles to manage access. This procedure describes how to add roles to an IDCS group.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation. A list of the identity providers in your tenancy is displayed.
2. Click the Oracle Identity Cloud Service Console link.
   The Identity Cloud Service console is displayed.
3. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
   The list of applications is displayed. Notice that the service that the application corresponds to is displayed underneath the application name. For example, underneath the JAAS application entry, you'll see Oracle Java Cloud Service.
4. Click the name of the service that you are interested in.
   The Details page is displayed.
5. Click Application Roles.
   The roles are displayed.
6. Click the menu for the role you want to assign and select Assign Groups.
7. Select the group you want to assign to the role, and click OK.
8. Click the Applications breadcrumb to return to the list of applications.
9. Repeat steps 4 through 7 for each role you want to assign to this group.

To remove roles from a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation. A list of the identity providers in your tenancy is displayed.
2. Click the Oracle Identity Cloud Console link.
   The Identity Cloud Service console is displayed.
3. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Applications.
   The list of applications is displayed. Notice that the service that the application corresponds to is displayed underneath the application name. For example, underneath the JAAS application entry, you'll see Oracle Java Cloud Service.
4. Click the name of the service that you are interested in.
   The Details page is displayed.
5. Click Application Roles.
   The roles are displayed.
6. Click the menu for the role you want to remove from the group and select Revoke Groups.
7. Select the group you want to remove the role from, and click OK.
8. Click the Applications breadcrumb to return to the list of applications.
9. Repeat steps 4 through 7 for each role you want to remove from this group.

To edit details for an Oracle Identity Cloud Service group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
   The list of existing groups in the federation is displayed.
4. Find the group you want to edit and click its name.
   The Group Details page is displayed.
5. Click Edit.
6. You can update the **Group Name** or the **Description**: Avoid entering confidential information.

   **Caution:**
   
   Changing the group name will break mappings to Oracle Cloud Infrastructure (OCI) groups. If you change the group name, ensure that you delete any existing group mappings and add new mappings with the new name. See the previous task on editing mappings.

7. Click **Update** to save your changes.

To add users to a group

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.
3. Under **Resources**, click **Groups**.
   
   The list of existing groups is displayed.
4. Find the group you want to add a user to.
   
   The **User Group Details** page is displayed.
5. Click **Add IDCS User**.
6. Select the user you want to add to this group from the **Users** list.
7. Click **Add**.

To remove users from a group

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.
3. Under **Resources**, click **Groups**.
   
   The list of existing groups is displayed.
4. Find the group you want to remove the user from.
   
   The list of users is displayed in the **Group Details** page.
5. Find the user you want to remove, and then click the the Actions icon (three dots).
6. Click **Remove User**.
7. Confirm when prompted.

To delete a group

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.
3. Under **Resources**, click **Groups**.
   
   The list of existing groups is displayed.
4. Find the group you want to edit and click its name.
   
   The **Group Details** page is displayed.
5. Click **Delete**.
6. Confirm when prompted.

Create a policy to grant the group permissions on Oracle Cloud Infrastructure resources

The group you created in Oracle Identity Cloud Service gets permissions to access resources in Oracle Cloud Infrastructure through the policy you assign to the Oracle Cloud Infrastructure group. Before you complete this step, you need to decide what permissions you want to give your new group. For more information, see **Getting Started with Policies** on page 2135 and **Common Policies** on page 2142.

Prerequisite: The group and compartment that you're writing the policy for must already exist.
1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**. A list of the policies in the compartment you're viewing is displayed.

2. If you want to attach the policy to a compartment other than the one you're viewing, select the desired compartment from the list on the left. Where the policy is attached controls who can later modify or delete it (see **Policy Attachment** on page 2141).

3. Click **Create Policy**.

4. Enter the following:

   - **Name**: A unique name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
   - **Description**: A friendly description. You can change this later if you want to.
   - **Statement**: A policy statement. For the correct format to use, see **Policy Basics** on page 2137 and also **Policy Syntax** on page 2164. If you want to add more than one statement, click +.

For example:

To allow your group to manage all resources within a specified compartment enter a statement like the following:

```
Allow group <OCI_group_name> to manage all-resources in compartment <compartment_name>
```

For more policy examples, see **Common Policies** on page 2142.

- **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Create**.

**Managing Oracle Identity Cloud Service Users in the Console**

After you add a user in Oracle Identity Cloud Service, a user is also automatically provisioned in Oracle Cloud Infrastructure. This provisioned user can have the Oracle Cloud Infrastructure credentials, such as API keys and auth tokens. To understand this provisioning, see **User Provisioning for Federated Users** on page 2404.

To create a user

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.

2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.

3. Click **Create IDCS User**.

4. In the **Create IDCS User** dialog enter the following:

   - **User Name**: Enter a unique name or email address for the new user. The value will be the user's login to the Console and must be unique across all other users in your tenancy.
   - **Email**: Enter an email address for this user. The initial sign-in credentials will be sent to this email address.
   - **First Name**: Enter the user's first name.
   - **Last Name**: Enter the user's last name.
   - **Phone Number**: Optionally, enter a phone number.
   - **Groups**: Optionally, select groups to add this user to.

5. Click **Create User**.

**Important:**

For the user to have permissions in Oracle Cloud Infrastructure, you must assign the user to a group that is mapped to an Oracle Cloud Infrastructure group. Or, if you are also creating a new group, you can perform this mapping later. The user will not be able to sign in to the Console until the mapping is accomplished.
The user creation process generates an email that is sent to the address provided that you entered. The email includes the new user’s username and password to use with the Oracle Cloud Infrastructure Console.

To add API keys, auth tokens, customer secret keys, or SMTP credentials for this user, see Managing User Capabilities for Federated Users on page 2408.

To edit a user

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
   - The list of existing users is displayed.
4. Find the user you want to edit and click its name.
   - The User Details page is displayed.
5. Click Edit.
6. Update the fields.
7. Click Save when finished.

To reset a user’s password

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
   - The list of existing user groups in the federation is displayed.
4. Find the user you want to reset the password for and click the name.
   - The User Details page is displayed.
5. Click Reset Password.
   - The user's password is reset. This user can't access their account until they complete the password reset steps.
6. Click Email Password Instructions to send the password link and instructions to the user.
   - The password link is good for 24 hours. If the user does not reset their password in time, you can generate a new password link by clicking Reset Password for the user again.

To manage roles for services managed through IDCS

See see Managing Oracle Identity Cloud Service Roles for Users on page 2379.

To add API keys, auth tokens, or other Oracle Cloud Infrastructure credentials

1. View the user's details:
   - If you're adding credentials for yourself:
     Open the Profile menu (🔗) and click User Settings.
   - If you're an administrator adding credentials for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
     Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
     Find the user in the list and click the OCI Synched User link.
2. Add the credentials for the user.
   - For more details about these credentials, see Managing User Credentials on page 2456.

To delete a user

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.


   The list of existing user groups in the federation is displayed.

4. Find the user you want to delete and click the name.

   The User Details page is displayed.

5. Click Delete.

Managing Group Mappings

To add group mappings for Oracle Identity Cloud Service

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.

   A list of the identity providers in your tenancy is displayed.

2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.

3. Click Edit Provider Details.

4. Add at least one mapping:
   a. Click + Add Mapping.
   b. Select the Oracle Identity Cloud Service group from the list under Identity Provider Group.
   c. Choose the IAM group you want to map this group to from the list under OCI Group.
   d. Repeat the above sub-steps for each mapping you want to create, and then click Submit.

Your changes take effect typically within seconds in your home region. Wait several more minutes for changes to propagate to all regions.

Users that are members of the Oracle Identity Cloud Service groups mapped to the Oracle Cloud Infrastructure groups are now listed in the Console on the Users page. See Managing User Capabilities for Federated Users on page 2408 for more information on assigning these users additional credentials.

To update or delete a group mapping

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.

   A list of the identity providers in your tenancy is displayed.

2. Click the identity provider to view its details.

3. Click Edit Mapping.

4. Update the mappings (or click the X to delete a mapping), and then click Submit.

If this action results in federated users no longer having membership in any group that is mapped to Oracle Cloud Infrastructure, the federated users' provisioned users' will also be removed from Oracle Cloud Infrastructure. Typically, this process takes several minutes.

Managing Oracle Identity Cloud Service Roles for Users

This topic describes managing user roles for users created in Oracle Identity Cloud Service.

About User Roles in Oracle Identity Cloud Service

You can assign roles to a user to allow access to those Oracle Cloud services that have predefined roles defined in Oracle Identity Cloud Service. You can also grant access just to service instances.

Services managed through Identity Cloud Service can have two types of predefined roles:

- Service access roles - grant access to use the service.
- Instance access roles - grant access to specific instances of a service. These can only be granted after the instances are created

For information about more complex role management including assigning other administrative privileges, see Managing Oracle Identity Cloud Service Users.
**Available Roles for Each Service**

Service-specific roles vary from one Oracle Cloud service to another, but they typically include at least one administrator role. See About Service Administrator Roles for more information about administrator roles. See your service-specific documentation for a description of the predefined roles for that service.

**Required Permissions to Manage Roles**

Before you can manage roles using the Oracle Cloud Infrastructure Console, you must be allowed to access the Identity Provider Details page. To access this page, you must belong to a group that is allowed to inspect identity providers. If you are a Cloud Administrator or if you belong to the OCI_Administrators group, this permission is included. To give this permission to non-administrators, you'll need to write a policy like the following:

```
Allow group GroupA to inspect identity-providers in tenancy
```

where you replace GroupA with the name of the group you want to grant the permission to.

To manage the service roles for another user, you must be assigned the appropriate role in Oracle Identity Cloud Service. See Understanding Administrator Roles.

**Managing Roles User Roles in the Console**

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.

   By default, users belonging to all identity providers are displayed. To view only users that belong to your Identity Cloud Service federation, clear the check boxes for any other identity providers.

2. Click the name of the user you want to edit.

3. On the user details page, click Manage Roles. The Manage Roles page displays the list of services for which you have Administrator access. The service and instance roles that this user has already been granted are also displayed.

   Note that you won't see services that you don't have Administrator access for.

4. Find the service you want to edit this user's access to, click the Actions icon (three dots), and then click Manage service access or Manage instance access, as appropriate. The list of roles for the selected service is displayed.

5. Edit the user's access as follows:
   - Select each role you want to give to the user.
   - Click the x next to each role you want remove from the user. Note that you can't remove a role that has been granted through a group. These roles are read only.

   **Note:**

   If a user is assigned the Cloud Account Administrator role, then you can’t remove the individual entitlement roles for the user.

6. Click Apply Role Settings or Update Instance Settings, as appropriate.

7. If you are granting roles to a user, in the confirmation dialog, click Send Email to User to send an email to the user to notify them of this change.

8. Your email client launches with a default email message you can send to the user. You can send the email as shown, or make modifications before sending.

9. Return to the Console and click Close.

**Managing Instance Roles in the Console**

Some services allow you to grant access to instances of the service. After you (or someone in your organization) creates an instance, use this procedure to manage individual user access to the instance.

**Managing User Access to an Instance**
1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**.

   A list of the users in your tenancy is displayed.

   By default, users belonging to all identity providers are displayed. To view only users that belong to your Identity Cloud Service federation, clear the check boxes for any other identity providers.

2. Click the name of the user you want to edit.

3. On the user details page, click **Manage Roles**. The **Manage Roles** page displays the list of services for which you have Administrator access. The service and instance roles that this user has already been granted are also displayed.

   Note that you won't see services that you don't have Administrator access for.

4. Find the service with instances that you want to edit this user's access to, click the Actions icon (three dots), and then click **Manage instance access**. The list of instances for the selected service is displayed.

5. On the **Manage Access to Instances** page, find the name of the instance you want to edit this user's access to.

   To grant access to this instance:

   In the **Instance Role** column, select the role you want to grant to the user. You can select multiple roles from the list.

   To remove access to this instance:

   In the **Instance Role** column, click the x next to the role you want to remove from the user.

6. When you are finished editing roles, click **Update Instance Settings**.

7. On the **Manage Roles** page, click **Apply Role Settings**.

8. If you are granting roles to a user, in the confirmation dialog, click **Send Email to User** to send an email to the user to notify them of this change.

9. Your email client launches with a default email message you can send to the user. You can send the email as shown, or make modifications before sending.

10. Return to the Console and click **Close**.

### Managing Oracle Identity Cloud Service Roles for Groups

This topic describes managing roles for groups created in Oracle Identity Cloud Service.

**About Group Roles in Oracle Identity Cloud Service**

You can assign roles to groups to allow access to those Oracle Cloud services that have predefined roles defined in Oracle Identity Cloud Service. You can also grant access just to service instances.

Services managed through Identity Cloud Service can have two types of predefined roles:

- Service access roles - grant access to use the service.
- Instance access roles - grant access to specific instances of a service. These can only be granted after the instances are created.

For information about more complex role management, see **Manage Oracle Identity Cloud Service Groups**.

**Available Roles for Each Service**

Service-specific roles vary from one Oracle Cloud service to another, but they typically include at least one administrator role. See **About Service Administrator Roles** for more information about administrator roles. See your service-specific documentation for a description of the predefined roles for that service.

**Required Permissions to Manage Roles**

Before you can manage roles using the Oracle Cloud Infrastructure Console, you must be allowed to access the Identity Provider Details page. To access this page, you must belong to a group that is allowed to inspect identity providers. If you are a Cloud Administrator or if you belong to the OCI_Administrators group, this permission is included. To give this permission to non-administrators, you'll need to write a policy like the following:

```
Allow group GroupA to inspect identity-providers in tenancy
```
where you replace GroupA with the name of the group you want to grant the permission to.

To manage service roles, you must be assigned the Administrator role for that service.

**Managing Group Roles in the Console**

To add roles to a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
3. Click Groups.

   The list of groups is displayed.

4. Click the name of the group you want to add roles to.
5. On the group details page, click Manage Roles. The Manage Roles page displays the list of services for which you have Administrator access. The service and instance roles that this group has already been granted are also displayed.

   Note that you won't see services that you don't have Administrator access for.
6. Find the service you want to edit this group's access to, click the Actions icon (three dots), and then click Manage service access. The list of roles for the selected service is displayed.
7. Select each role that you want to assign to the group.
8. Click Save Role Selections.
9. To add more service roles to this group, repeat steps 6 - 8.
10. Click Apply Role Settings.
11. In the confirmation dialog, click Send Email to Group to send an email to each member of the group to notify them of this change.

   Your email client launches with a default email message to the affected users with information about the access changes. You can send the email as written, or make modifications before sending.
12. Return to the Console and click Close.

To revoke roles from a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService. The identity provider details page is displayed.
3. Click Groups.

   The list of groups is displayed.

4. Click the name of the group you want to remove roles from.
5. On the group details page, click Manage Roles. The Manage Roles page displays the list of services for which you have Administrator access. The service and instance roles that this group has already been granted are also displayed.

   Note that you won't see services that you don't have Administrator access for.
6. Find the service you want to edit this group's access to, click the Actions icon (three dots), and then click Manage service access or Manage instance access, as appropriate. The list of roles for the selected service is displayed.
7. Clear the check box for each role you want remove from the group.
8. Click Save Role Selections or Update Instance Settings, as appropriate.
9. To revoke more service or instance roles from this group, repeat steps 6 - 8.
10. Click Apply Role Settings.
11. A confirmation dialog displays the services that you modified access to in this session. Click Close.

**Managing Instance Roles in the Console**

Some services allow you to grant access to instances of the service. After you (or someone in your organization) creates an instance, use this procedure to manage group access to the instance.

**Managing Group Access to an Instance**
1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.

2. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named **OracleIdentityCloudService**. The identity provider details page is displayed.

3. Click **Groups**.

   The list of groups is displayed.

4. On the group details page, click **Manage Roles**. The **Manage Roles** page displays the list of services for which you have Administrator access. The service and instance roles that this group has already been granted are also displayed.

   Note that you won't see services that you don't have Administrator access for.

5. Find the service with instances that you want to edit this group's access to, click the Actions icon (three dots), and then click **Manage instance access**. The list of instances for the selected service is displayed.

6. On the **Manage Access to Instances** page, find the name of the instance you want to edit this group's access to.

   - To grant access to this instance: In the **Instance Role** column, select the role you want to grant to the group. You can select multiple roles from the list.
   - To remove access to this instance: In the **Instance Role** column, click the **x** next to the role you want to remove from the group.

7. When you are finished editing roles for this service, click **Update Instance Settings**.

8. To edit more instance roles for this group, repeat steps 6 - 7.

9. On the **Manage Roles** page, click **Apply Role Settings**.

10. If you added roles, in the confirmation dialog, click **Send Email to Group** to send an email to each member of the group to notify them of this change. Your email client launches with a default email message to the affected users with information about the access changes. You can send the email as written, or make modifications before sending. Return to the Console and click **Close**.

   If you revoked roles, a confirmation dialog displays the services that you modified access to in this session. Click **Close**.

**Frequently Asked Questions for Oracle Identity Cloud Service Federated Users**

When you sign up for Oracle Cloud Infrastructure, your account is automatically federated with Oracle Identity Cloud Service as your identity provider. This topic answers some frequently asked questions about the federation.

**What resources are created in Oracle Identity Cloud Service?**

**The following resources are created in Identity Cloud Service:**

- **Applications:**
  - **OCI-V2-<tenancy_name>**
    This SAML application that creates the federation with Oracle Cloud Infrastructure.
  - **COMPUTEAREMETA** application
    A supporting application for the federation.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not delete these applications.</td>
</tr>
</tbody>
</table>

- **Group:**
  - **OCI_Administrators group**
    This group is mapped to the Administrators group in Oracle Cloud Infrastructure. Members of this group have full administrator privileges in Oracle Cloud Infrastructure.

- **User:**
  - A default administrator user (e.g., user@example.com) who is a member of the OCI_Administrators group.
What resources are created in Oracle Cloud Infrastructure?

The following resources are created in Oracle Cloud Infrastructure:

- **Identity Provider**: OracleIdentityCloudService
- **Group Mappings**: The federation is created with one group mapping:
  - OCI_Administrators group (from Oracle Identity Cloud Service) is mapped to the Administrators group (in Oracle Cloud Infrastructure).
- **Users**:
  - The default administrator user created in Oracle Identity Cloud Service is provisioned in Oracle Cloud Infrastructure. This user can have the Oracle Cloud Infrastructure credentials, but not a Console password.
  - A default administrator local-user with the same user name (user@example.com) is also created in Oracle Cloud Infrastructure's IAM service. Customers who choose not to use the Oracle Identity Cloud Service federation can use this user to administer Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The default administrator created in Oracle Identity Cloud Service and the local default administrator created in Oracle Cloud Infrastructure exist independently in their respective identity systems. Ensure that you manage passwords for them separately.</td>
</tr>
</tbody>
</table>

Why is my account federated with Oracle Identity Cloud Service?

Oracle Identity Cloud Service is the identity provider for multiple Oracle services. Federating Oracle Cloud Infrastructure with Oracle Identity Cloud Service allows you to have a seamless connection between services, without having to create a separate username and password for each one.

How do I know if I am signed in through Oracle Identity Cloud Service?

Click the **Profile** menu to display your username. Users signed in through an identity provider will see their username prefaced with their identity provider name, for example:

oracleidentitycloudservice/user@example.com

How do I add a user to Oracle Identity Cloud Service (a federated user)?

See Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372.

Can I add a user just for Oracle Cloud Infrastructure?

Yes. If you don't want to manage the user in Oracle Identity Cloud Service, you can add a user directly to the Oracle Cloud Infrastructure IAM service. See Adding Users on page 57. Using this procedure, you can create users who can sign in directly to the Oracle Cloud Infrastructure Console. Users created with this procedure do not have access to any other Oracle services.

How do I manage groups?

In short, managing groups requires actions in both Oracle Identity Cloud Service and Oracle Cloud Infrastructure. Groups you create in Oracle Identity Cloud Service have no privileges in Oracle Cloud Infrastructure until you map them to a group in Oracle Cloud Infrastructure. You define the policies that permit access to Oracle Cloud Infrastructure resources in the IAM service in Oracle Cloud Infrastructure. For more information, see Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372.

How do I find the client ID and client secret?

To edit mappings of your user groups in Oracle Identity Cloud Service to user groups in Oracle Cloud Infrastructure, you'll need to supply the client ID and client secret. The client ID and client secret are stored in Oracle Identity Cloud Service. To get this information:

1. Sign in to the Oracle Identity Cloud Service console.
2. In the Identity Cloud Service console, click **Applications**. The list of trusted applications is displayed.
3. Click COMPUTEBAREMETAL.
4. Click **Configuration**.
5. Expand **General Information**. The client ID is displayed. Click **Show Secret** to display the client secret.

![Identity Cloud Service Console](image)

---

**If I delete the federation, can I later recreate it?**

Yes. To recreate the federation with Oracle Identity Cloud Service, follow the instructions in the topic Federating with Oracle Identity Cloud Service on page 2366.

### Federating with Microsoft Active Directory

This topic describes how to federate with Microsoft Active Directory using Microsoft Active Federation Services (AD FS).

**Note:**

Before following the steps in this topic, see Federating with Identity Providers on page 2362 to ensure that you understand general federation concepts.

### About Federating with Microsoft Active Directory

Your organization can have multiple Active Directory accounts (for example, one for each division of the organization). You can federate multiple Active Directory accounts with Oracle Cloud Infrastructure, but each federation trust that you set up must be for a single Active Directory account.

To federate with Active Directory, you set up a trust between Active Directory and Oracle Cloud Infrastructure. To set up this trust, you perform some steps in the Oracle Cloud Infrastructure Console and some steps in Active Directory Federation Services.

Following is the general process an administrator goes through to set up federation with Active Directory. Details for each step are given in the sections below.

1. Get required information from Active Directory Federation Services.
2. Federate Active Directory with Oracle Cloud Infrastructure:
   a. Add the identity provider (AD FS) to your tenancy and provide the required information.
   b. Map Active Directory groups to IAM groups.
3. In Active Directory Federation Services, add Oracle Cloud Infrastructure as a trusted, relying party.
4. In Active Directory Federation Services, add the claim rules required in the authentication response by Oracle Cloud Infrastructure.
5. Test your configuration by logging in to Oracle Cloud Infrastructure with your Active Directory credentials.

Federating with Active Directory

Prerequisites
You have installed and configured Microsoft Active Directory Federation Services for your organization.
You have set up groups in Active Directory to map to groups in Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consider naming Active Directory groups that you intend to map to Oracle Cloud Infrastructure groups with a common prefix, to make it easy to apply a filter rule. For example, OCI_Administrators, OCI_NetworkAdmins, OCI_InstanceLaunchers.</td>
</tr>
</tbody>
</table>

Step 1: Get required information from Active Directory Federation Services

Summary: Get the SAML metadata document and the names of the Active Directory groups that you want to map to Oracle Cloud Infrastructure Identity and Access Management groups.

1. Locate the SAML metadata document for your AD FS federation server. By default, it is at this URL: https://<yourservername>/FederationMetadata/2007-06/FederationMetadata.xml
   Download this document and make a note of where you save it. You will upload this document to the Console in the next step.
2. Note all the Active Directory groups that you want to map to Oracle Cloud Infrastructure IAM groups. You will need to enter these in the Console in the next step.

Step 2: Add Active Directory as an identity provider in Oracle Cloud Infrastructure

Summary: Add the identity provider to your tenancy. You can set up the group mappings at the same time, or set them up later.

1. Go to the Console and sign in with your Oracle Cloud Infrastructure login and password.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
3. Click Add identity provider.
4. Enter the following:
   a. **Display Name:** A unique name for this federation trust. This is the name federated users see when choosing which identity provider to use when signing in to the Console. The name must be unique across all identity providers you add to the tenancy. You cannot change this later.
   b. **Description:** A friendly description.
   c. **Type:** Select Microsoft Active Directory Federation Services (ADFS) or SAML 2.0 compliant identity provider.
   d. **XML:** Upload the FederationMetadata.xml file you downloaded from Azure AD.
   e. Click **Show Advanced Options**.
   f. **Encrypt Assertion:** Selecting the check box lets the IAM service know to expect the encryption from IdP. Do not select this check box unless you have enabled assertion encryption in Azure AD.

      To enable assertion encryption for this single sign-on application in Azure AD, set up the SAML Signing Certificate in Azure AD to sign the SAML response and assertion. For more information, see the Azure AD documentation.

   g. **Force Authentication:** Selected by default. When selected, users are required to provide their credentials to the IdP (re-authenticate) even when they are already signed in to another session.
   h. **Authentication Context Class References:** This field is required for Government Cloud customers. When one or more values are specified, Oracle Cloud Infrastructure (the relying party), expects the identity provider to use one of the specified authentication mechanisms when authenticating the user. The returned SAML response from the IdP must contain an authentication statement with that authentication context class reference. If the SAML response authentication context does not match what is specified here, the Oracle Cloud Infrastructure auth service rejects the SAML response with a 400. Several common authentication context class references are listed in the menu. To use a different context class, select **Custom**, then manually enter the class reference.
   i. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Continue**.

6. Set up the mappings between Active Directory groups and IAM groups in Oracle Cloud Infrastructure. A given Active Directory group can be mapped to zero, one, or multiple IAM groups, and vice versa. However, each individual mapping is between only a single Active Directory group and a single IAM group. Changes to group mappings take effect typically within seconds in your home region, but may take several minutes to propagate to all regions.

   **Note:**
   
   If you don't want to set up the group mappings now, you can simply click **Create** and come back to add the mappings later.

   To create a group mapping:
   a. Under **Identity Provider Group**, enter the Active Directory group name. You must enter the name exactly, including the correct case.

      Choose the IAM group you want to map this group to from the list under **OCI Group**.

      **Tip:**

      Requirements for IAM group name: No spaces. Allowed characters: letters, numerals, hyphens, periods, underscores, and plus signs (+). The name cannot be changed later.

   b. Repeat the above sub-steps for each mapping you want to create, and then click **Create**.

   The identity provider is now added to your tenancy and appears in the list on the **Federation** page. Click the identity provider to view its details and the group mappings you just set up.
Oracle assigns the identity provider and each group mapping a unique ID called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

In the future, come to the Federation page if you want to edit the group mappings or delete the identity provider from your tenancy.

**Step 3: Copy the URL for the Oracle Cloud Infrastructure Federation Metadata document**

**Summary:** The Federation page displays a link to the Oracle Cloud Infrastructure Federation Metadata document. Before you move on to configuring Active Directory Federation Services, you need to copy the URL.

1. On the Federation page, click **Download this document**.
2. Copy the URL. The URL looks similar to:

   https://auth.r2.oracleiaas.com/v1/saml/
   ocid1.tenancy.oc1..aaaaaaaaqdt2tvdmhsa3jmvc5dzulgs3pcv6imfwdgdy4aq/
   metadata.xml

**Step 4: In Active Directory Federation Services, add Oracle Cloud Infrastructure as a trusted relying party**

1. Go to the AD FS Management Console and sign in to the account you want to federate.
2. Add Oracle Cloud Infrastructure as a **trusted relying party**:
   a. From the AD FS Management Console, right-click AD FS and select **Add Relying Party Trust**.
   b. In the **Add Relying Party Trust Wizard**, click **Start**.
   c. Select **Import data about the relying party published online or on a local network**.
      Paste the Oracle Cloud Infrastructure Federation Metadata URL that you copied in Step 3. Click **Next**.
      AD FS will connect to the URL. If you get an error during the attempt to read the federation metadata, you can alternatively upload the Oracle Cloud Infrastructure Federation Metadata XML document.
      **To upload the federation metadata document**
      1. In a web browser, paste the Oracle Cloud Infrastructure Federation Metadata URL in the address bar.
      2. Save the XML document to a location that is accessible by your AD FS Management Console.
      3. In the **Select Data Source** step of the **Add Relying Party Trust Wizard**, select **Import data about the relying party from a file**.
         4. Click **Browse** and select the metadata.xml file that you saved.
         5. Click **Next**.
   d. Set the display name for the relying party (for example, Oracle Cloud Infrastructure) and then click **Next**.
   e. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time**.
   f. Choose the appropriate Issuance Authorization Rules to either permit or deny all users access to the relying party. Note that if you choose "Deny", then you must later add the authorization rules to enable access for the appropriate users.
      Click **Next**.
   g. Review the settings and click **Next**.
   h. Check **Open the Edit Claim Rules** dialog for this relying part trust when the wizard closes and then click **Close**.

**Step 5: Add the claim rules for the Oracle Cloud Infrastructure relying party**

**Summary:** Add the claim rules so that the elements that Oracle Cloud Infrastructure requires (Name ID and groups) are added to the SAML authentication response.

**Add the Name ID rule:**
1. In the **Add Transform Claim Rule Wizard**, select **Transform an Incoming Claim**, and click **Next**.
2. Enter the following:
   - **Claim rule name**: Enter a name for this rule, for example, nameid.
   - **Incoming claim type**: Select Windows account name.
   - **Outgoing claim type**: Select Name ID.
   - **Outgoing name ID format**: Select Persistent Identifier.
   - Select **Pass through all claim value**.
   - Click **Finish**.
3. The rule is displayed in the rules list. Click **Add Rule**.

### Add the groups rule:

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any users who are in more than 100 IdP groups cannot be authenticated to use the Oracle Cloud Infrastructure Console. To enable authentication, apply a filter to the groups rule, as described below.</td>
</tr>
</tbody>
</table>

**If your Active Directory users are in no more than 100 groups**

**Add the groups rule:**

1. Under Claim rule template, select **Send Claims Using a Custom Rule**. Click **Next**.
2. In the **Add Transform Claim Rule Wizard**, enter the following:
   a. **Claim rule name**: Enter groups.
   b. **Custom rule**: Enter the following custom rule:

   ```
c: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = ("https://auth.oraclecloud.com/saml/claims/groupName"), query = ";tokenGroups;{0}", param = c.Value);
   ```
   c. Click **Finish**.

**If your Active Directory users are in more than 100 groups**

**Add the groups rule with a filter:**

To limit the groups sent to Oracle Cloud Infrastructure, create two custom claim rules. The first one retrieves all groups the user belongs to directly and indirectly. The second rule applies a filter to limit the groups passed to the service provider to only those that match the filter criteria.

Add the first rule:

1. In the Edit Claim Rules dialog, click **Add Rule**.
2. Under Claim rule template, select **Send Claims Using a Custom Rule**. Click **Next**.
3. In the **Add Transform Claim Rule Wizard**, enter the following:
   a. **Claim rule name**: Enter a name, for example, groups.
   b. **Custom rule**: Enter the following custom rule:

   ```
c: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("https://auth.oraclecloud.com/saml/claims/groupName"), query = ";tokenGroups;{0}", param = c.Value);
   ```

   Note that in this custom rule you use `add` instead of `issue`. This command passes the results of the rule to the next rule, instead of sending the results to the service provider.
   c. Click **Finish**.
4. Now add the filter rule.
   a. In the Edit Claim Rules dialog, click Add Rule.
   b. Under Claim rule template, select Send Claims Using a Custom Rule. Click Next.
   c. In the Add Transform Claim Rule Wizard, enter the following:
      1. Claim rule name: Enter groups.
      2. Custom rule: Enter an appropriate filter rule. For example to send only groups that begin with the string "OCI", enter the following:
         ```
         c:[Type == "https://auth.oraclecloud.com/saml/claims/groupName", Value =~ "(?i)OCI"] => issue(claim = c);
         ```
         This rule filters the list from the first rule to only those groups that begin with the string OCI. The issue command, sends the results of the rule to the service provider.
         You can create filters with the appropriate criteria for your organization.
         For information on AD FS syntax for custom rules, see the Microsoft document: Understanding Claim Rule Language in AD FS 2.0 and Higher.
      3. Click Finish.

Step 6: Set up IAM policies for the groups
If you haven't already, set up IAM policies to control the access the federated users have to your organization's Oracle Cloud Infrastructure resources. For more information, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Step 7: Give your federated users the name of the tenant and URL to sign in
Give federated users the URL for the Oracle Cloud Infrastructure Console, https://cloud.oracle.com, and the name of your tenant. They'll be prompted to provide the tenant name when they sign in to the Console.

Managing Identity Providers in the Console
To add an identity provider
See About Federating with Microsoft Active Directory on page 2385.

To delete an identity provider
All the group mappings for the identity provider will also be deleted.

1. Delete the identity provider from your tenancy:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
      A list of the identity providers in your tenancy is displayed.
   b. Click the identity provider to view its details.
   c. Click Delete.
   d. Confirm when prompted.

To add group mappings for an identity provider
1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
   A list of the identity providers in your tenancy is displayed.
2. Click the identity provider to view its details.
3. Click **Add Mappings**.
   a. Under **Identity Provider Group**, enter the Active Directory group name. The name you enter here must match exactly the name in Active Directory.
   b. Choose the IAM group you want to map this group to from the list under **OCI Group**.
   c. To add more mappings, click **+ Another Mapping**.
   d. When you are finished, click **Add Mappings**.

Your changes take effect typically within seconds.

**To update a group mapping**

You can't update a group mapping, but you can delete the mapping and add a new one.

**To delete a group mapping**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
   
   A list of the identity providers in your tenancy is displayed.
2. Click the identity provider to view its details.
3. For the mapping you want to delete, select it, and then click **Delete**.
4. Confirm when prompted.

Your changes take effect typically within seconds.

**Managing Identity Providers in the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations:

**Identity providers:**

- CreateIdentityProvider
- ListIdentityProviders
- GetIdentityProvider
- UpdateIdentityProvider
- DeleteIdentityProvider: Before you can use this operation, you must first use DeleteIdpGroupMapping to remove all the group mappings for the identity provider.

**Group mappings:**

- CreateIdpGroupMapping: Each group mapping is a separate entity with its own OCID.
- ListIdpGroupMappings
- GetIdpGroupMapping
- UpdateIdpGroupMapping
- DeleteIdpGroupMapping

**Federating with Microsoft Azure Active Directory**

This topic describes how to federate with Microsoft Azure Active Directory (AD).

**Note:**

Before following the steps in this topic, see Federating with Identity Providers on page 2362 to ensure that you understand general federation concepts.

**About Federating with Azure AD**

To federate with Azure AD, you set up Oracle Cloud Infrastructure as a basic SAML single sign-on application in Azure AD. To set up this application, you perform some steps in the Oracle Cloud Infrastructure Console and some steps in Azure AD.
Following is the general process an administrator goes through to set up the federation. Details for each step are given in the next section.

1. In Oracle Cloud Infrastructure, download the federation metadata document.
2. In Azure AD, set up Oracle Cloud Infrastructure Console as an enterprise application.
3. In Azure AD, configure the Oracle Cloud Infrastructure enterprise application for single sign-on.
4. In Azure AD, set up the user attributes and claims.
5. In Azure AD, download the Azure AD SAML metadata document.
6. In Azure AD, assign user groups to the application.
7. In Oracle Cloud Infrastructure, set up Azure AD as an identity provider.
8. In Oracle Cloud Infrastructure, map your Azure AD groups to Oracle Cloud Infrastructure groups.
9. In Oracle Cloud Infrastructure, set up the IAM policies to govern access for your Azure AD groups.
10. Share the Oracle Cloud Infrastructure sign-in URL with your users.

**Steps to Federate with Azure AD**

**Prerequisites**

You have an Azure tenancy with groups and users set up in Azure AD.

**Step 1: In Oracle Cloud Infrastructure, download the federation metadata document**

**Summary:** The Oracle Cloud Infrastructure Console Federation page displays a link to the Oracle Cloud Infrastructure federation metadata document. Before you set up the application in Azure AD, you need to download the document.

1. Go to the **Federation** page: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
2. On the Federation page, click **Download this document**.

After you click the link, the metadata.xml document opens in your browser window. Use your browser's **Save page as** command to save the xml document locally where you can access it later.

**Step 2: In Azure AD, add Oracle Cloud Infrastructure as an enterprise application**

1. In the Azure portal, on the left navigation panel, select **Azure Active Directory**.
2. In the **Azure Active Directory** pane, select **Enterprise applications**. A sample of the applications in your Azure AD tenant is displayed.
3. At the top of the **All applications** pane, click **New application**.
4. In the **Add from gallery** region, enter **Oracle Cloud Infrastructure Console** in the search box.
5. Select the Oracle Cloud Infrastructure Console application from the results.
6. In the application-specific form, you can edit information about the application. For example, you can edit the name of the application.
7. When you are finished editing the properties, select **Create**.

The getting started page is displayed with the options for configuring the application for your organization.
Step 3: In Azure AD, configure Oracle Cloud Infrastructure as an enterprise application

1. Under the **Manage** section, select **Single sign-on**.

2. Select **SAML** to configure single sign-on. The **Set up Single Sign-On with SAML** page is displayed.

3. At the top of the page, click **Upload metadata file**.

4. Locate the federation metadata file (metadata.xml) you downloaded from Oracle Cloud Infrastructure in Step 1, and upload it here. After you upload the file, these **Basic SAML Configuration** fields are automatically populated:
   - Identifier (Entity ID)
   - Reply URL (Assertion Consumer Service URL)
5. In the **Basic SAML Configuration** section, click **Edit**. On the **Basic SAML Configuration** pane, enter the following required field:

   - **Sign on URL**: Enter the URL in the following format:
     
     ```
     https://console.<oci_home_region>.oraclecloud.com
     
     where `oci_home_region` is your tenancy's home region. For example, if you home region is Ashburn, enter:
     
     https://console.us-ashburn-1.oraclecloud.com
     
     [How do I find my tenancy home region?](page 136)
     ```

   ![Basic SAML Configuration Panel](image)

6. Click **Save**.

   **Step 4: Configure User Attributes & Claims**

   The Oracle Cloud Infrastructure Console enterprise application template is seeded with the required attributes, so you don't need to add any. However, you do need to make the following customizations:

   1. In the **User Attributes & Claims** section, click **Edit** in the upper-right corner. The **Manage claim** panel is displayed.
2. Next to the **Name identifier value** field, click **Edit**.
   - Under **Required claim**, select Unique User Identifier (Name ID).
   - Select **Email address** and change it to **Persistent**.
   - For **Source**, select Attribute.
   - For **Source attribute**, select user.userprincipalname.

3. Click **Add a group claim**.
4. In the Group Claims panel, configure the following:

- Select Security groups.
- **Source attribute**: Select Group ID.
- Under Advanced Options, select **Customize the name of the group claim**.
- In the Name field, enter: `groupName`.
  
  Ensure that you enter `groupName` with spelling and case exactly as given.

- In the Namespace field, enter: `https://auth.oraclecloud.com/saml/claims`

- Click Save.
Step 5: Download the SAML metadata document

1. In the SAML Signing Certificate section, click the download link next to Federation Metadata XML.

2. Download this document and make a note of where you save it. You will upload this document to the Console in the next step.

Step 6: Assign user groups to the application

To enable Azure AD users to sign in to Oracle Cloud Infrastructure, you need to assign the appropriate user groups to your new enterprise application.

1. On the left navigation pane, under Manage, select Users and Groups.
2. Click Add at the top of the Users and Groups list to open the Add Assignment pane.
3. Click the Users and groups selector.
4. Enter the name of the group you want to assign to the application into the Search by name or email address search box.
5. Hover over the group in the results list to display a check box. Select the check box to add the group to the Selected list.
6. When you are finished selecting groups, click Select to add them to the list of users and groups to be assigned to the application.
7. Click Assign to assign the application to the selected groups.

Step 7: Add Azure AD as an identity provider in Oracle Cloud Infrastructure

Summary: Add the identity provider to your tenancy. You can set up the group mappings at the same time, or set them up later.

1. Go to the Console and sign in with your Oracle Cloud Infrastructure username and password.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
3. Click Add identity provider.
4. Enter the following:
   a. **Display Name:** A unique name for this federation trust. This is the name federated users see when choosing which identity provider to use when signing in to the Console. The name must be unique across all identity providers you add to the tenancy. You cannot change this later.
   b. **Description:** A friendly description.
   c. **Type:** Select SAML 2.0 compliant identity provider.
   d. **XML:** Upload the FederationMetadata.xml file you downloaded from Azure AD.
   e. Click **Show Advanced Options**.
   f. **Encrypt Assertion:** Selecting the check box lets the IAM service know to expect the encryption from IdP. Do not select this check box unless you have enabled assertion encryption in Azure AD.
      To enable assertion encryption for this single sign-on application in Azure AD, set up the SAML Signing Certificate in Azure AD to sign the SAML response and assertion. For more information, see the Azure AD documentation.
   g. **Force Authentication:** Selected by default. When selected, users are required to provide their credentials to the IdP (re-authenticate) even when they are already signed in to another session.
   h. **Authentication Context Class References:** This field is required for Government Cloud customers. When one or more values are specified, Oracle Cloud Infrastructure (the relying party), expects the identity provider to use one of the specified authentication mechanisms when authenticating the user. The returned SAML response from the IdP must contain an authentication statement with that authentication context class reference. If the SAML response authentication context does not match what is specified here, the Oracle Cloud Infrastructure auth service rejects the SAML response with a 400. Several common authentication context class references are listed in the menu. To use a different context class, select **Custom**, then manually enter the class reference.
   i. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Continue**.

Note: If you don't want to set up the group mappings now, you can simply click **Create** and come back to add the mappings later.

**Step 8: Add group mappings**

Summary: Set up the mappings between Azure AD groups and IAM groups in Oracle Cloud Infrastructure. A given Azure AD group can be mapped to zero, one, or multiple IAM groups, and vice versa. However, each individual mapping is between only a single Azure AD group and a single IAM group. Changes to group mappings take effect typically within seconds in your home region, but may take several minutes to propagate to all regions. Note that the Azure AD groups that you choose to map must also be assigned to the enterprise application in Azure AD. See Step 6: Assign user groups to the application on page 2397.

Before you begin: Have your Azure AD groups page open. From the Azure Dashboard, under Manage, select Groups. From the list of groups, select the group you want to map to an Oracle Cloud Infrastructure group. In the group’s details page, click the Copy icon next to the Object ID for the group.

To create a group mapping:
1. For **Identity Provider Group**, enter (or paste) the Object ID of the Azure AD group. You must enter the Object ID exactly, including the correct case. An example Object ID looks like: `aa0e7d64-5b2c-623g-at32-65058526179c`

![Edit Identity Provider](image)

2. Choose the IAM group you want to map this group to from the list under **OCI Group**.
3. Repeat the preceding steps for each mapping you want to create, and then click **Create**.

**Tip:**

Requirements for IAM group name: No spaces. Allowed characters: letters, numerals, hyphens, periods, underscores, and plus signs (+). The name cannot be changed later.

The identity provider is now added to your tenancy and appears in the list on the **Federation** page. Click the identity provider to view its details and the group mappings you just set up.

Oracle assigns the identity provider and each group mapping a unique ID called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

In the future, come to the **Federation** page if you want to edit the group mappings or delete the identity provider from your tenancy.

**Step 9: Set up IAM policies for the groups**

If you haven't already, set up IAM policies to control the access the federated users have to your organization's Oracle Cloud Infrastructure resources. For more information, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Step 10: Give your federated users the name of the tenant and URL to sign in**

The federated users need the URL for the Oracle Cloud Infrastructure Console (for example, `https://cloud.oracle.com`) and the name of your tenant. They'll be prompted to provide the tenant name when they sign in to the Console.

**Managing Identity Providers in the Console**

*To add an identity provider*

See About Federating with Azure AD on page 2391.

*To delete an identity provider*

All the group mappings for the identity provider will also be deleted.
1. Delete the identity provider from your tenancy:
   a. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.

   A list of the identity providers in your tenancy is displayed.
   b. Click the identity provider to view its details.
   c. Click Delete.
   d. Confirm when prompted.

To add group mappings for an identity provider

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.

   A list of the identity providers in your tenancy is displayed.
2. Click the identity provider to view its details.
3. Click Add Mappings.
   a. Under Identity Provider Group, select Custom Group. Enter (or paste) the Object ID of the Azure AD group. You must enter the Object ID exactly, including the correct case. An example Object ID looks like: aa0e7d64-5b2c-623g-at32-65058526179c. Note that for groups to be able to sign in to Oracle Cloud Infrastructure, they must also be assigned to the enterprise application in Azure AD. See Step 6: Assign user groups to the application on page 2397.
   b. Choose the IAM group you want to map this group to from the list under OCI Group.
   c. To add more mappings, click +Another Mapping.
   d. When you are finished, click Add Mappings.

Your changes take effect typically within seconds.

To update a group mapping

You can't update a group mapping, but you can delete the mapping and add a new one.

To delete a group mapping

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.

   A list of the identity providers in your tenancy is displayed.
2. Click the identity provider to view its details.
3. For the mapping you want to delete, select it, and then click Delete.
4. Confirm when prompted.

Your changes take effect typically within seconds.

Managing Identity Providers in the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations:

Identity providers:
- CreateIdentityProvider
- ListIdentityProviders
- GetIdentityProvider
- UpdateIdentityProvider
- DeleteIdentityProvider: Before you can use this operation, you must first use DeleteIgpGroupMapping to remove all the group mappings for the identity provider.

Group mappings:
- CreateIgpGroupMapping: Each group mapping is a separate entity with its own OCID.
- ListIgpGroupMappings
- GetIgpGroupMapping
Federating with SAML 2.0 Identity Providers

This topic describes the general steps to federate Oracle Cloud Infrastructure with any identity provider that supports the Security Assertion Markup Language (SAML) 2.0 protocol. If you want specific instructions for Oracle Identity Cloud Service or Microsoft Active Directory, see Federating with Oracle Identity Cloud Service on page 2366 or Federating with Microsoft Active Directory on page 2385.

Tip:
Find detailed setup steps for more IdPs in the following white papers:

- Oracle Cloud Infrastructure Okta Configuration for Federation and Provisioning
- Federating Oracle Access Manager to Oracle Cloud Infrastructure

Instructions for Federating

Following is the general process an administrator goes through to set up the identity provider, and below are instructions for each step. It's assumed that the administrator is an Oracle Cloud Infrastructure user with the required credentials and access.

Note:
Before following the steps in this topic, see Federating with Identity Providers on page 2362 to ensure that you understand general federation concepts.

1. In the Oracle Cloud Infrastructure Console, get the federation metadata required to establish a trust relationship with the Identity Provider (IdP).
2. In the IdP, configure Oracle Cloud Infrastructure as an application (sometimes called a trusted relying party).
3. In the IdP, assign users and groups to your new Oracle Cloud Infrastructure application.
4. In the IdP, get the required information needed by Oracle Cloud Infrastructure.
5. In Oracle Cloud Infrastructure:
   a. Add the identity provider to your tenancy and provide information you got from the IdP.
   b. Map the IdP's groups to IAM groups.
6. In Oracle Cloud Infrastructure, make sure you have IAM policies set up for the groups so you can control users' access to Oracle Cloud Infrastructure resources.

Step 1: Get information from Oracle Cloud Infrastructure

Summary: Download the federation metadata document.

The federation metadata document is a standard SAML 2.0 document, which provides information about Oracle Cloud Infrastructure you'll need to provide to your IdP. Depending on your provider's setup requirements, you may need to upload the entire document, or you may be asked to provide only specific metadata values from the document.

1. Sign in to the Oracle Cloud Infrastructure Console as an administrator.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
3. Right-click the Download this document link and save the document.

Step 2: Set up Oracle Cloud Infrastructure as a trusted application

Consult your IdP documentation for how to set up a trusted application. Refer to the metadata document you downloaded for required parameters.

Step 3: Assign users and groups to the new application.
Follow your IdP's procedures for adding users and groups to the application you set up for Oracle Cloud Infrastructure.

Step 4: Download the IdP's metadata document.

Your IdP should provide a SAML 2.0 document that contains the information Oracle Cloud Infrastructure needs to complete the federation. See your IdP documentation for instructions on downloading this document.

Step 5: Federate the IdP with Oracle Cloud Infrastructure

Summary: Add the identity provider to your tenancy. You can set up the group mappings at the same time, or set them up later.

Details:

1. Go to the Console and sign in with your Oracle Cloud Infrastructure login and password.
2. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.
3. Click Add Identity Provider.
4. Enter the following:
   a. Name: A unique name for this federation trust. This is the name federated users see when choosing which identity provider to use when signing in to the Console, so consider making this a friendly, intuitive name your users will understand. The name must be unique across all identity providers you add to the tenancy. You cannot change this later.
   b. Description: A friendly description.
   c. Type: Select Microsoft Active Directory Federation Service (ADFS) or SAML 2.0 Compliant Identity Provider.
   d. XML: Upload the metadata.xml document that you downloaded from your IdP.
   e. Encrypt Assertion: Selecting the check box lets the IAM service know to expect the encryption from the IdP. If you select this check box, you must also set up encryption of the assertion in your IdP. For more information, see Encrypt Assertion under General Concepts on page 2363. See also your IdP's documentation.
   f. Force Authentication: Selected by default. When selected, users are required to provide their credentials to the IdP (re-authenticate) even when they are already signed in to another session.
   g. Authentication Context Class References: This field is required for Government Cloud customers. When one or more values are specified, Oracle Cloud Infrastructure (the relying party), expects the identity provider to use one of the specified authentication mechanisms when authenticating the user. The returned SAML response from the IdP must contain an authentication statement with that authentication context class reference. If the SAML response authentication context does not match what is specified here, the Oracle Cloud Infrastructure auth service rejects the SAML response with a 400. Several common authentication context class references are listed in the menu. To use a different context class, select Custom, then manually enter the class reference.
   h. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click Continue.
6. Set up the mappings between the IdP groups and IAM groups in Oracle Cloud Infrastructure. A given IdP group can be mapped to zero, one, or multiple IAM groups, and conversely. However, each individual mapping is
between only a single IdP group and a single IAM group. Changes to group mappings take effect typically within seconds in your home region, but may take several minutes to propagate to all regions.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you don't want to set up the group mappings now, you can simply click Create and come back to add the mappings later.</td>
</tr>
</tbody>
</table>

To create a group mapping:

**a.** Under **Identity Provider Group**, enter the name of the group in your IdP. You must enter the name exactly, including the correct case.

Choose the IAM group you want to map this group to from the list under **OCI Group**.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements for IAM group name: No spaces. Allowed characters: letters, numerals, hyphens, periods, underscores, and plus signs (+). The name cannot be changed later.</td>
</tr>
</tbody>
</table>

**b.** Repeat the above sub-steps for each mapping you want to create, and then click Create.

The identity provider is now added to your tenancy and appears in the list on the **Federation** page. Click the identity provider to view its details and the group mappings you just set up.

Oracle assigns the identity provider and each group mapping a unique ID called an Oracle Cloud ID (OCID). For more information, see **Resource Identifiers**.

In the future, come to the **Federation** page if you want to edit or add group mappings or delete the identity provider from your tenancy.

**Step 6: Set up IAM policies for the groups**

If you haven't already, set up IAM policies to control the access the federated users have to your organization's Oracle Cloud Infrastructure resources. For more information, see **Getting Started with Policies** on page 2135 and **Common Policies** on page 2142.

**Step 7: Give your federated users the name of the tenant and URL to sign in**

The federated users need the URL for the Oracle Cloud Infrastructure Console: https://cloud.oracle.com, and the name of your tenant. They'll be prompted to provide the tenant name when they sign in to the Console.

**Managing Identity Providers in the Console**

- **To add an identity provider**

  See **Instructions for Federating** on page 2401.

- **To delete an identity provider**

  All the group mappings for the identity provider will also be deleted.

1. Delete the identity provider from your tenancy:
   **a.** Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.

   A list of the identity providers in your tenancy is displayed.

   **b.** Click the identity provider to view its details.

   **c.** Click **Delete**.

   **d.** Confirm when prompted.

2. Follow your IdP's documentation to delete the application from your IdP.

- **To add group mappings for an identity provider**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.

   A list of the identity providers in your tenancy is displayed.

2. Click the identity provider to view its details.
3. Click **Add Mappings**.
   a. Enter the IdP group name exactly in the **Identity Provider Group** text box.
   b. Choose the IAM group you want to map this group to from the list under **OCI Group**.
   c. To add more mappings, click **+Another Mapping**.
   d. When you are finished, click **Add Mappings**.

Your changes take effect typically within seconds in your home region. Wait several more minutes for changes to propagate to all regions.

*To update a group mapping*

You can't update a group mapping, but you can delete the mapping and add a new one.

*To delete a group mapping*

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.
   A list of the identity providers in your tenancy is displayed.
2. Click the identity provider to view its details.
3. For the mapping you want to delete, select it, and then click **Delete**.
4. Confirm when prompted.

Your changes take effect typically within seconds in your home region. Wait several more minutes for changes to propagate to all regions.

**Managing Identity Providers in the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations:

**Identity providers:**
- CreateIdentityProvider
- ListIdentityProviders
- GetIdentityProvider
- UpdateIdentityProvider
- DeleteIdentityProvider: Before you can use this operation, you must first use DeleteIdpGroupMapping to remove all the group mappings for the identity provider.

**Group mappings:**
- CreateIdpGroupMapping: Each group mapping is a separate entity with its own OCID.
- ListIdpGroupMappings
- GetIdpGroupMapping
- UpdateIdpGroupMapping
- DeleteIdpGroupMapping

**User Provisioning for Federated Users**

This topic describes how you can use SCIM to provision federated users in Oracle Cloud Infrastructure. Provisioned federated users can have API keys and other service-specific credentials.

**Overview**

SCIM (System for Cross-domain Identity Management) is an IETF standard protocol that enables user provisioning across identity systems. Oracle Cloud Infrastructure hosts a SCIM endpoint for provisioning federated users into Oracle Cloud Infrastructure. If your IdP is Oracle Identity Cloud Service or Okta, you can set up SCIM user provisioning.
After you configure the SCIM integration between your IdP and Oracle Cloud Infrastructure, users that belong to groups mapped to Oracle Cloud Infrastructure groups are automatically provisioned in Oracle Cloud Infrastructure. Provisioned users are assigned a unique **OCID**, and can have API keys and other service-specific credentials.

The following functionality is supported for provisioned, federated users:

- Provisioned users are assigned a unique **OCID**
- Provisioned users can have API keys, auth tokens, and other service-specific credentials
- You can list the users in the Console
- Provisioned users can access the **User Settings** page to see and manage these credentials for themselves
- When you add or remove users to Oracle Cloud Infrastructure-mapped groups in your IdP, the updates are automatically synced with Oracle Cloud Infrastructure

**Understanding User Types**

The SCIM configuration introduces the concept of the *provisioned* or *synchronized* user. The following descriptions provide details to help you understand the user types you'll be managing.

- **Federated users**
  
  A federated user is created and managed in an identity provider. Federated users can sign in to the Console using a password managed in their identity provider. Federated users are granted access to Oracle Cloud Infrastructure based on their membership in groups that are mapped to Oracle Cloud Infrastructure groups.

- **Provisioned (or Synchronized) users**
  
  A synchronized user is systematically provisioned by the identity provider in Oracle Cloud Infrastructure. Synchronized users can have Oracle Cloud Infrastructure credentials, but not Console passwords. When listing users in the Console, you can identify synchronized users using the **User Type** filter.

- **Local users**
  
  A local user is a user created and managed in Oracle Cloud Infrastructure's IAM service. Federated tenancies typically would have few, if any, local users. When listing users in the Console, you can identify local users using the **User Type** filter.

The following graphic summarizes the characteristics of the user types:
Who Should Set Up This Integration?

Set up this integration if your IdP is Oracle Identity Cloud Service or Okta and your federated users need to have the specialized credentials required by some services and features. For example, if you need your federated users to access Oracle Cloud Infrastructure through the SDK or CLI, setting up this integration enables these users to get the API keys needed for this access.

Prerequisite

Perform this synchronization setup after you have successfully set up a federation between your IdP and Oracle Cloud Infrastructure. See Supported Identity Providers on page 2366.

Enabling User Provisioning

Instructions for Oracle Identity Cloud Service Federations

If your identity provider is Oracle Identity Cloud Service, you need to perform a one-time upgrade.

Important:

If your tenancy was created December 21, 2018 or later, your tenancy is automatically configured to provision your Oracle Identity Cloud Service users in Oracle Cloud Infrastructure. You do not need to perform the steps in this topic. See Understanding User Types on page 2405 and Managing User.
Upgrading Your Oracle Identity Cloud Service Federation

If your federation with Oracle Identity Cloud service was set up before December 21, 2018, perform this one-time upgrade task.

To upgrade your Oracle Identity Cloud Service federation:

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Federation.

   A list of the identity providers in your tenancy is displayed.

2. Click your Identity Cloud Service federation to view its details. If your tenancy was auto-federated, it is listed as OracleIdentityCloudService.

3. Click Edit Mapping.

4. When prompted, provide the client ID and client secret for the Oracle Identity Cloud Service application, and then click Continue.

   Where do I find the client ID and client secret?

   The client ID and client secret are stored in Oracle Identity Cloud Service. To get this information:

   a. 1. Sign in to the Oracle Identity Cloud Service console.
      2. In the Identity Cloud Service console, click Applications. The list of trusted applications is displayed.
      3. Click COMPUTEBAREMETAL.
      4. Click Configuration.
      5. Expand General Information. The client ID is displayed. Click Show Secret to display the client secret.

Allow several minutes for the changes to take effect.

Instructions for Okta Federations

If you do not have an existing federation with Okta, follow the instructions in the white paper, Oracle Cloud Infrastructure Okta Configuration for Federation and Provisioning. This paper includes instructions for both setting up your federation and provisioning with SCIM.

If you have an existing federation with Okta with group mappings that you want to maintain, you can add SCIM provisioning as follows:
1. In Okta, delete the existing SAML application you originally set up to federate with Oracle Cloud Infrastructure.
2. Set up a new SAML application in Okta according to the instructions in the white paper, Oracle Cloud Infrastructure Okta Configuration for Federation and Provisioning, with the following exceptions:
   - Skip the steps to Add Identity Provider to Oracle Cloud Infrastructure (you already have this resource in Oracle Cloud Infrastructure).
   - Instead, click Edit Identity Provider and upload the new metadata.xml document from the new Okta app you created.
   - Then, in Oracle Cloud Infrastructure, ensure that you Reset Credentials. Add the new Client ID and Secret to the API integration settings page in Okta (Step 7 in the white paper).

**What to Expect After the Upgrade**

When the system has had time to synchronize, you can manage user capabilities for federated users in the Console. Users that belong to a group mapped to a group in Oracle Cloud Infrastructure are listed on the Users page in the Console. Whenever you add new users to mapped groups in Oracle Identity Cloud Service, they will be available in the Console after the system synchronizes.

By default, the following user capabilities are enabled:

- API keys
- auth tokens
- SMTP credentials
- customer secret keys

Notice that you can't enable a local password. The Oracle Cloud Infrastructure console password is still managed only in your IdP.

For more information about user capabilities, see Managing User Capabilities for Federated Users on page 2408.

**Resetting Credentials**

Use the Reset Credentials button to reset your SCIM client credentials. You can perform this task periodically as a security measure to rotate your credentials. After you reset these credentials, you'll need to update the SAML app in your identity provider with the new credentials.

**Note:** If your IdP is Oracle Identity Cloud Service, Oracle Cloud Infrastructure automatically resets the credentials with Oracle Identity Cloud Service for you. You don't need to manually reset the configuration.

**Actions You Still Perform in Your Identity Provider**

After the integration is set up, continue to perform the following actions in your IdP:

- Create users and assign them to groups.
- Delete users.
  - Users that you delete from your IdP are removed from Oracle Cloud Infrastructure when the next synching cycle completes.
- Query for group membership.
- Manage sign-in passwords for users.

**Managing User Capabilities for Federated Users**

This topic describes managing user capabilities for federated users when your tenancy is federated and configured for user provisioning with a supported identity provider.

**About User Capabilities**

To access Oracle Cloud Infrastructure, a user must have the required credentials. Users who need to use the Console, must have a password. Users who need access through the API need API keys. Some service features require additional credentials, such as auth tokens, SMTP credentials, and Amazon S3 Compatibility API keys. For a user to get these credentials, the user must be granted the capability to have the credential type.
User capabilities are managed by an Administrator in the user's details. Each user can see their capabilities, but only an Administrator can enable or disable them. The user capabilities available to federated users are:

- API keys
- auth tokens
- SMTP credentials
- customer secret keys
- OAuth 2.0 client credentials

By default, these capabilities are enabled when you provision new users, allowing users to create these credentials for themselves. For information about these user credentials, see Managing User Credentials on page 2456.

**Important:**

The capability "Console password" is not available for federated users. Federated users authenticate to the Console through their IdP, where their sign-in passwords are managed.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for managing user capabilities. A user can't enable or disable user capabilities for themselves (except for Administrators). However, a user can manage their own credentials that have been enabled for them.

**Prerequisites**

Management of user capabilities for federated users is supported for Oracle Identity Cloud Service and Okta federations only.

- Oracle Identity Cloud Service federations:
  
  If your tenancy was created December 21, 2018 or later, your tenancy is automatically configured to manage user capabilities. There are no prerequisites.

  If your tenancy was created before December 21, 2018, you must perform a one-time upgrade. See Enabling User Provisioning on page 2406.

- If your tenancy is federated with Okta, see User Provisioning for Federated Users on page 2404.

**Viewing Provisioned Federated Users in the Console**

After the prerequisites are satisfied, you can view users that you create in your IdP that belong to groups mapped to Oracle Cloud Infrastructure groups. Whenever you add a user to a group mapped to an Oracle Cloud Infrastructure group, the user automatically displays in the Console.

**To list users in the Console:**

Open the navigation menu. Under Governance and Administration, go to Identity and click Users.

Notice that you can filter the list by user type to include only users that belong to a specified identity provider. Local Users are users created in Oracle Cloud Infrastructure's IAM service. The filter list includes all identity providers you have set up.

**Using the Console**

**To edit user capabilities**

If you're an Administrator, you can edit user capabilities.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.

2. Click the user to see its details.
3. Click **Edit User Capabilities**.
4. Select or clear the check box to add or remove a capability.
5. Click **Save**.

**To change a user's description**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. A list of the users in your tenancy is displayed.
2. Click the user you want to update. The user's details are displayed. The description is displayed under the user's login.
3. Click the pencil next to the description.
4. Edit the description and save it. This description is maintained in Oracle Cloud Infrastructure and is not synched back to your identity provider.

**To apply tags to a user**

For instructions, see **Resource Tags** on page 211.

**To delete a user**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. A list of the users in your tenancy is displayed.
2. Find the user you want to delete and click the Actions icon (three dots).
3. Click **Delete**.

**Important:** Deleting a user here does not delete the user in your IdP. If you later want the federated user to have a provisioned user in Oracle Cloud Infrastructure, you must remove the user from all OCI-mapped groups in Oracle Identity Cloud Service and re-add the user.

For information about managing user credentials in the Console, see **Managing User Credentials** on page 2456.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage user capabilities:

- **ListUsers**
- **GetUser**
- **UpdateUser**: You can update the user capabilities and the user's description.
- **UpdateUserCapabilities**
- **DeleteUser**: This operation deletes the provisioned user in Oracle Cloud Infrastructure, but not the user in the identity provider.

For information about the API operations for managing user credentials, see **Managing User Credentials** on page 2456.

The following operations are **not** supported for federated users:

- **ListUserGroupMemberships**
- **AddUserToGroup**
- **GetUserGroupMembership**
- **RemoveUserFromGroup**

**Calling Services from an Instance**

This topic describes how you can authorize instances to call services in Oracle Cloud Infrastructure.
Introduction
This procedure describes how you can authorize an instance to make API calls in Oracle Cloud Infrastructure services. After you set up the required resources and policies, an application running on an instance can call Oracle Cloud Infrastructure public services, removing the need to configure user credentials or a configuration file.

Concepts

DYNAMIC GROUP
Dynamic groups allow you to group Oracle Cloud Infrastructure instances as principal actors, similar to user groups. You can then create policies to permit instances in these groups to make API calls against Oracle Cloud Infrastructure services. Membership in the group is determined by a set of criteria you define, called matching rules.

MATCHING RULE
When you set up a dynamic group, you also define the rules for membership in the group. Resources that match the rule criteria are members of the dynamic group. Matching rules have a specific syntax you follow. See Writing Matching Rules to Define Dynamic Groups on page 2424.

INSTANCE PRINCIPALS
The IAM service feature that enables instances to be authorized actors (or principals) to perform actions on service resources. Each compute instance has its own identity, and it authenticates using the certificates that are added to it. These certificates are automatically created, assigned to instances and rotated, preventing the need for you to distribute credentials to your hosts and rotate them.

Security Considerations
Any user who has access to the instance (who can SSH to the instance), automatically inherits the privileges granted to the instance. Before you grant permissions to an instance using this procedure, ensure that you know who can access it, and that they should be authorized with the permissions you are granting to the instance.

All compute instance principals are granted the compartment_inspect permission. You cannot revoke this permission. This permission allows the instance to ListCompartments in the tenancy to retrieve the following information:

- Compartment names
- Compartment descriptions
- Free-form tags applied to compartments
- Automatic tag defaults applied to compartments. These tags, such as CreatedBy and CreatedOn, are in the Oracle-Tag namespace and are automatically added by Oracle.

Process Overview
The following steps summarize the process flow for setting up and using instances as principals. The subsequent sections provide more details.

1. Create a dynamic group. In the dynamic group definition, you provide the matching rules to specify which instances you want to allow to make API calls against services.
2. Create a policy granting permissions to the dynamic group to access services in your tenancy (or compartment).
3. A developer in your organization configures the application built using the Oracle Cloud Infrastructure SDK to authenticate using the instance principals provider. The developer deploys the application and the SDK to all the instances that belong to the dynamic group.
4. The deployed SDK makes calls to Oracle Cloud Infrastructure APIs as allowed by the policy (without needing to configure API credentials).
5. For each API call made by an instance, the Audit service logs the event, recording the OCID of the instance as the value of principalId in the event log.
Steps to Enable Instances to Call Services

Perform these tasks to enable an instance to call services:

Create a Dynamic Group and Matching Rules

Write Policies for Dynamic Groups

Configure the SDK, CLI, or Terraform

Creating a Dynamic Group and Matching Rules

See Managing Dynamic Groups on page 2422.

Writing Policies for Dynamic Groups

After you have created a dynamic group, you need to create policies to permit the dynamic groups to access Oracle Cloud Infrastructure services.

Policy for dynamic groups follows the syntax described in How Policies Work on page 2136. Review that topic to understand basic policy features.

The syntax to permit a dynamic group access to resources in a compartment is:

```
Allow dynamic-group <dynamic_group_name> to <verb> <resource-type> in compartment <compartment_name>
```

The syntax to permit a dynamic group access to a tenancy is:

```
Allow dynamic-group <dynamic_group_name> to <verb> <resource-type> in tenancy
```

Here are a few example policies:

To allow a dynamic group (FrontEnd) to use a load balancer in a specific compartment (ProjectA):

```
Allow dynamic-group FrontEnd to use load-balancers in compartment ProjectA
```

To allow a dynamic group to launch instances in a specific compartment:

```
Allow dynamic-group FrontEnd to manage instance-family in compartment ProjectA
Allow dynamic-group FrontEnd to use volume-family in compartment ProjectA
Allow dynamic-group FrontEnd to use virtual-network-family in compartment ProjectA
```

For more sample policies, see Common Policies on page 2142.

Configuring the SDK, CLI, or Terraform

For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For the SDK for Java:

In your SDK for Java, create an InstancePrincipalsAuthenticationDetailsProvider object. For example:

```java
public static void main(String[] args) throws Exception {
    InstancePrincipalsAuthenticationDetailsProvider provider =
        InstancePrincipalsAuthenticationDetailsProvider.builder().build();
    IdentityClient identityClient = new IdentityClient(provider);
}
For the SDK for Python:

In your SDK for Python, create an `oci.auth.signers.InstancePrincipalsSecurityTokenSigner` object. For example:

```python
# By default this will hit the auth service in the region returned by

signer = oci.auth.signers.InstancePrincipalsSecurityTokenSigner()
identity_client = oci.identity.IdentityClient(config={}, signer=signer)

...```

To refresh the token without waiting, use the following command:

```python
signer.refresh_security_token()
```

**Enabling Instance Principal Authorization for the CLI**

To enable instance principal authorization from the CLI, you can set the authorization option (`--auth`) for a command. For example:

```bash
oci os ns get --auth instance_principal
```

Alternatively, you can set the following environment variable:

```bash
OCI_CLI_AUTH=instance_principal
```

Note that if both are set, the value set for `--auth` takes precedence over the environment variable.

For information about using the CLI, see [Working with the Command Line Interface](#).

**Enabling Instance Principal Authorization for Terraform**

To enable instance principal authorization in Terraform, you can set the `auth` attribute to "InstancePrincipal" in the provider definition as shown in the following sample:

```hcl
variable "region" {}

provider "oci" {
  auth = "InstancePrincipal"
  region = "${var.region}"
}
```

Note that when you use instance principal authorization you do not need to include the `tenancy_ocid`, `user_ocid`, `fingerprint`, and `private_key_path` attributes.

**FAQs**

**How do I query the instance metadata service to query the certificate on the instance?**


**How frequently is the certificate rotated on each instance?**

The certificate is rotated multiple times each day.

**What happens if I try to use an expired certificate?**

You will get a 401-Not Authenticated error.
Can I change the frequency at which the certificate is rotated?
No. You can't change the frequency at which the certificate is rotated. However, you can change the policy on the dynamic group. If you think an instance has been compromised, you can either change the policy on the dynamic group to revoke permissions for all members of the group, or you can remove the instance from the dynamic group. See Can I remove an instance from a dynamic group? on page 2414

What happens if the certificate is rotated in the middle of a long running operation?
The token expiration is independent of the certificate expiration period. And, it also depends on the application you are interacting with. For example, if Object Storage does not have a multipart PUT operation, then it does not matter how long the operation runs.

Are the certificates accessible for all users on an instance?
Yes. Ensure that only users who should be granted the access that you have granted to the dynamic group, have access to the instance.

Are dynamic groups created at the tenancy level?
Yes.

Can I remove an instance from a dynamic group?
Yes. You can remove it by modifying the matching rule to exclude it. See below for an example.

Can I exclude specific instances in a compartment from the dynamic group?
Yes. For example, assume you want to exclude two specific instances in a compartment from the dynamic group. Write a matching rule like this:

```text
All {instance.compartment.id = '<compartment_ocid>',
    instance.id != '<instance1_to_exclude_ocid>', instance.id !=
    '<instance2_to_exclude_ocid>'}
```

The above rule includes all instances in the compartment except those with the OCIDs specified.

Managing Users
This topic describes the basics of working with users.

Important:
If your tenancy is federated with Oracle Identity Cloud Service, see Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372 to manage users.

Required IAM Policy
If you're in the Administrators group, then you have the required access for managing users.

- You can create a policy that gives someone the power to create new users and credentials but not control which groups those users are in. See Let the Help Desk manage users on page 2142.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for users or other IAM components, see Details for IAM on page 2280.

Tagging Resources
You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.
Working with Users

When creating a user, you must provide a unique, unchangeable name for the user. The name must be unique across all users within your tenancy. This name is the user's login to the Console. You might want to use a name that's already in use by your company's own identity system (for example, Active Directory, LDAP, etc.). You must also provide the user with a description (although it can be an empty string), which is a non-unique, changeable description for the user. This value could be the user's full name, a nickname, or other descriptive information. Oracle also assigns the user a unique ID called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

Note:
If you delete a user and then create a new user with the same name, the two users are considered different users, because they have different OCIDs.

Oracle recommends that you supply a password recovery email address for the user. If the user forgets their password, they can request to have a temporary password sent to them using the Forgot Password link on the sign-on page. If no email address is present for the user, an administrator must intervene to reset their password.

A new user has no permissions until you place the user in one or more groups and at least one policy gives that group permission to either the tenancy or to a compartment. Exception: each user can manage their own credentials they have been enabled to have. An administrator does not need to create a policy to give a user that ability. For more information, see User Credentials on page 2360.

Important:
After creating a user and putting them in a group, let them know which compartment(s) they have access to.

You also need to give the new user some credentials so they can access Oracle Cloud Infrastructure. A user can have one or both of the following credentials, depending on the type of access they need: A password for using the Console and an API signing key for using the API.

About User Capabilities

To access Oracle Cloud Infrastructure, a user must have the required credentials. Users who need to use the Console must have a password. Users who need access through the API need API keys. Some service features require additional credentials, such as auth tokens, SMTP credentials, and Amazon S3 Compatibility API keys. For a user to get these credentials, the user must be granted the capability to have the credential type.

Administrators manage user capabilities in the User details. Each user can see their capabilities, but only an Administrator can enable or disable those capabilities. The user capabilities are:

- Can use Console password (native users only)
- Can use API keys
- Can use auth tokens
- Can use SMTP credentials
- Can use customer secret keys

By default, all these capabilities are enabled when you create users, allowing users to create these credentials for themselves. For information about working with user credentials, see Managing User Credentials on page 2456.

Enabling Multi-Factor Authentication for a User

See Managing Multi-Factor Authentication on page 2470 for details.

Signing In to the Console

Users created through this procedure are created in IAM and are sometimes called "local users." If your tenancy is federated with another identity provider (such as Oracle Identity Cloud Service, Azure AD, or Okta), your sign-in page to the Console displays two options for signing in. The local users you create in IAM use the Oracle Cloud Infrastructure option to sign in, as shown in the following image:
If your tenancy is not federated, you only have one sign in option.

**Tracking Recent Sign-in Activity**

The Users list page displays information to assist administrators in determining whether user accounts are active. The **Last Sign In** field displays the date and time the user last signed in to Oracle Cloud Infrastructure using the Console. This field is displayed only on the list view of all users, it is not displayed on the individual user details page. This field only tracks sign in from the Console. If a user accesses Oracle Cloud Infrastructure through other access methods (for example, through the SDK), those occurrences are not tracked.

**Linking a User to a My Oracle Support Account**

To file support requests directly from the Console, each user must link their IAM user account with their My Oracle Support (MOS) account. You only need to complete this step once. For instructions, see To link a user to their My Oracle Support account on page 2418.

**Prerequisites**

- Before a user can create this link, they must set up an account in My Oracle Support. For information on setting up a My Oracle Support account, see Creating an Oracle Single Sign On (SSO) Account on page 130.
- Before a user can submit service requests for a tenancy, their My Oracle Support account must be associated to their tenancy CSI number. See Registering Your CSI for Oracle Cloud Infrastructure on page 131.

**Unblocking a User After Unsuccessful Sign-in Attempts**

If a user unsuccessfully tries to sign in to the Console 10 times in a row, they are blocked from further sign-in attempts. An administrator can unblock the user in the Console (see To unblock a user on page 2418) or with the UpdateUserState API operation.

**Deleting a User**

You can delete a user, but only if the user is not a member of any groups.

**Limits on Users**

For information about the number of users you can have, see Service Limits on page 215.
Using the Console
To create a user

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click Create User.
3. Enter the following:
   - **Name:** A unique name or email address for the user. For tips about what value to use, see Working with Users on page 2415. The name must be unique across all users in your tenancy. You cannot change this value later. The name must meet the following requirements: No spaces. Only Basic Latin letters (ASCII), numerals, hyphens, periods, underscores, +, and @.
   - **Description:** This value could be the user's full name, a nickname, or other descriptive information. You can change this value later.
   - **Email:** Enter an email address for the user. This email address is used for password recovery. The email address must be unique in the tenancy.
     If the user forgets their password, they can click Forgot Password on the sign on page, and a temporary password is generated and sent to the email address provided here. The user or an administrator can also update the email address can also later.
   - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
4. Click Create.

Next, you need to give the user permissions by adding them to at least one group. You also need to give the user the credentials they need (see Managing User Credentials on page 2456).

To add a user to a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Locate the user in the list.
3. Click the user. The user's details are displayed.
4. Click Groups.
5. Click Add User to Group.
6. Select the group from the drop-down list, and then click Add.

Let the user know which compartment(s) they have access to.

To remove a user from a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Locate the user in the list.
3. Click the user. The user's details are displayed.
4. Click Groups.
5. Click the Actions icon (three dots), and then click Remove.
6. Confirm when prompted.

To delete a user

Prerequisite: To delete a user, the user must not be in any groups.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. For the user you want to delete, click Delete.
3. Confirm when prompted.
To unblock a user

If you are an administrator, you can use the following procedure to unblock a user who has unsuccessfully tried to sign in to the Console 10 times in a row.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user. The user's details are displayed, including the current status.
3. Click Unblock.
4. Confirm when prompted.

To change a user's description

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user you want to update. The user's details are displayed. The description is displayed under the user's login.
3. Click the pencil next to the description.
4. Edit the description and save it.

To edit a user's email

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user you want to update. The user's details are displayed.
3. Under User Information, click the pencil next to Email.
4. Enter the email address and click the save icon. The email address must be unique in the tenancy.

To edit user capabilities

If you're an Administrator, you can edit user capabilities.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user to see its details.
3. Click Edit User Capabilities.
4. Select or clear the check box to add or remove a capability.
5. Click Save.

To apply tags to a user

For instructions, see Resource Tags on page 211.

To link a user to their My Oracle Support account

Important: Ensure that you meet the prerequisites before linking your account. See Linking a User to a My Oracle Support Account on page 2416.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user you want to update. The user's details are displayed.
3. Click Link Support Account. The Oracle account sign in page prompts you to enter your Oracle credentials.
4. Enter the User name and Password of the Oracle support account that you want to link to this user and click Sign in. The I AM user account is linked to the Oracle support account. The e-mail address associated with the support account is displayed in the user details in the field My Oracle Support account.

To unlink a user a user from a My Oracle Support account

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user you want to update. The user's details are displayed.
3. Click **Unlink Support Account**.
4. In the confirmation prompt, click **Unlink**.

For information about managing user credentials in the Console, see Managing User Credentials on page 2456.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

**Note:**

Updates Are Not Immediate Across All Regions

Your IAM resources reside in your home region. To enforce policy across all regions, the IAM service replicates your resources in each region. Whenever you create or change a policy, user, or group, the changes take effect first in the home region, and then are propagated out to your other regions. It can take several minutes for changes to take effect in all regions. For example, assume you have a group with permissions to launch instances in the tenancy. If you add UserA to this group, UserA is able to launch instances in your home region within a minute. However, UserA is not able to launch instances in other regions until the replication process is complete. This process can take up to several minutes. If UserA tries to launch an instance before replication is complete, they will get a not authorized error.

Use these API operations to manage users:

- CreateUser
- ListUsers
- GetUser
- UpdateUserState: Unblocks a user who has tried to sign in 10 times in a row unsuccessfully.
- UpdateUser: You can update the user's description, email, and tags.
- UpdateUserCapabilities
- DeleteUser
- ListUserGroupMemberships: Use this operation to get a list of which users are in a group, or which groups a user is in.
- AddUserToGroup: This operation results in a UserGroupMembership object with its own OCID.
- GetUserGroupMembership
- RemoveUserFromGroup: This operation deletes a UserGroupMembership object.

For information about the API operations for managing user credentials, see Managing User Credentials on page 2456.

**Managing Groups**

This topic describes the basics of working with groups.

**Important:**

If your tenancy is federated with Oracle Identity Cloud Service, see Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console on page 2372 to manage groups.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for managing groups.
If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.

### Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

### Working with Groups

When creating a group, you must provide a unique, unchangeable name for the group. The name must be unique across all groups within your tenancy. You must also provide the group with a description (although it can be an empty string), which is a non-unique, changeable description for the group. Oracle will also assign the group a unique ID called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

**Note:**

If you delete a group and then create a new group with the same name, they'll be considered different groups because they'll have different OCIDs.

A group has no permissions until you write at least one policy that gives that group permission to either the tenancy or a compartment. When writing the policy, you can specify the group by using either the unique name or the group's OCID. Per the preceding note, even if you specify the group name in the policy, IAM internally uses the OCID to determine the group. For information about writing policies, see Managing Policies on page 2450.

You can delete a group, but only if the group is empty.

For information about the number of groups you can have, see Service Limits on page 215.

If you're federating with an identity provider, you'll create mappings between the identity provider's groups and your IAM groups. For more information, see Federating with Identity Providers on page 2362.

### Using the Console

#### To create a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups. A list of the groups in your tenancy is displayed.
2. Click Create Group.
3. Enter the following:
   - **Name**: A unique name for the group. The name must be unique across all groups in your tenancy. You cannot change this later. The name must be 1-100 characters long and can include the following characters: lowercase letters a-z, uppercase letters A-Z, 0-9, and the period (.), dash (-), and underscore (_). Spaces are not allowed. Avoid entering confidential information.
   - **Description**: A friendly description. You can change this later if you want to.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
4. Click Create Group.

Next, you might want to add users to the group, or write a policy for the group. See To create a policy on page 2454.

#### To add a user to a group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups. A list of the groups in your tenancy is displayed.
2. Locate the group in the list.
3. Click the group. Its details are displayed
4. Click **Add User to Group**.
5. Select the user from the drop-down list, and then click **Add User**.

**To remove a user from a group**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Groups**. A list of the groups in your tenancy is displayed.
2. Locate the group in the list.
3. Click the group to display its details. A list of users in the group is displayed.
4. Locate the user in the list.
5. For the user you want to remove, click **Remove**.
6. Confirm when prompted.

**To delete a group**

Prerequisite: To delete a group, it must not have any users in it.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Groups**. A list of the groups in your tenancy is displayed.
2. Locate the group in the list.
3. For the group you want to delete, click **Delete**.
4. Confirm when prompted.

**To update a group's description**

This is available only through the API. If you don't have access to the API and need to update a group's description, contact Oracle Support.

**To apply tags to a group**

For instructions, see **Resource Tags** on page 211.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

**Note:**

Updates Are Not Immediate Across All Regions

Your IAM resources reside in your home region. To enforce policy across all regions, the IAM service replicates your resources in each region. Whenever you create or change a policy, user, or group, the changes take effect first in the home region, and then are propagated out to your other regions. It can take several minutes for changes to take effect in all regions. For example, assume you have a group with permissions to launch instances in the tenancy. If you add UserA to this group, UserA will be able to launch instances in your home region within a minute. However, UserA will not be able to launch instances in other regions until the replication process is complete. This process can take up to several minutes. If UserA tries to launch an instance before replication is complete, they will get a not authorized error.

Use these API operations to manage groups:

- **CreateGroup**
- **ListGroups**
- **GetGroup**
- **UpdateGroup**: You can update only the group's description.
- **DeleteGroup**
- **ListUserGroupMemberships**: Use to get a list of which users are in a group, or which groups a user is in.
• **AddUserToGroup**: This operation results in a `UserGroupMembership` object with its own OCID.
• **GetUserGroupMembership**
• **RemoveUserFromGroup**: This operation deletes a `UserGroupMembership` object.

For API operations related to group mappings for identity providers, see *Federating with Identity Providers* on page 2362.

**Managing Dynamic Groups**

This topic describes how to manage dynamic groups and define the rules to determine a dynamic group's members.

**About Dynamic Groups**

Dynamic groups allow you to group Oracle Cloud Infrastructure compute instances as "principal" actors (similar to user groups). You can then create policies to permit instances to make API calls against Oracle Cloud Infrastructure services. When you create a dynamic group, rather than adding members explicitly to the group, you instead define a set of matching rules to define the group members. For example, a rule could specify that all instances in a particular compartment are members of the dynamic group. The members can change dynamically as instances are launched and terminated in that compartment.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for managing dynamic groups.

If you're new to policies, see *Getting Started with Policies* on page 2135 and *Common Policies* on page 2142. If you want to dig deeper into writing policies for dynamic groups or other IAM components, see *Details for IAM* on page 2280.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see *Resource Tags* on page 211.

**Working with Dynamic Groups**

When creating a dynamic group, you must provide a unique, unchangeable name for the dynamic group. The name must be unique across all groups within your tenancy. You must also provide the dynamic group with a description (although it can be an empty string), which is a non-unique, changeable description for the group. Oracle will also assign the group a unique ID called an Oracle Cloud ID (OCID). For more information, see *Resource Identifiers*.

**Note:**

If you delete a dynamic group and then create a new dynamic group with the same name, they'll be considered different groups because they'll have different OCIDs.

A dynamic group has no permissions until you write at least one policy that gives that dynamic group permission to either the tenancy or a compartment. When writing the policy, you can specify the dynamic group by using either the unique name or the dynamic group's OCID. Per the preceding note, even if you specify the dynamic group name in the policy, IAM internally uses the OCID to determine the dynamic group. For information about writing policies, see *Managing Policies* on page 2450.

You can delete a dynamic group, but only if the group is empty.

**Updating Dynamic Groups**

You can update the matching rules that define the members of a dynamic group. For example, you might change a matching rule that includes all instances in a compartment to exclude a particular instance. Or, you might update a rule to include a new tag value.
Important:

When you make a change to a matching rule you must allow about one hour for the updated policy to take effect. For example, if you update tags on an instance to either include or exclude that instance from a dynamic group, you must wait for that policy to take effect to include or exclude the instance.

Limits on Dynamic Groups

A single compute instance can belong to a maximum of 5 dynamic groups.

You can have a maximum of 50 dynamic groups in your tenancy.

Using the Console

To create a dynamic group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Dynamic Groups.
2. Click Create Dynamic Group.
3. Enter the following:
   - Name: A unique name for the group. The name must be unique across all groups in your tenancy (dynamic groups and user groups). You can't change this later. Avoid entering confidential information.
   - Description: A friendly description.
4. Enter the Matching Rules. Resources that meet the rule criteria are members of the group.
   - Rule 1: Enter a rule following the guidelines in Writing Matching Rules to Define Dynamic Groups on page 2424. You can manually enter the rule in the text box or launch the rule builder.
   - Enter additional rules as needed. To add a rule, click Additional Rule.
5. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
6. Click Create Dynamic Group.
   
   The matching rule syntax is verified, but the OCIDs are not. Be sure that the OCIDs you enter are correct.

Next, to give the dynamic group permissions, you need to write a policy. See Writing Policies for Dynamic Groups on page 2412.

To delete a dynamic group

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Dynamic Groups.
   
   A list of the dynamic groups in your tenancy is displayed.
2. Locate the dynamic group in the list.
3. For the dynamic group you want to delete, click Delete.
4. Confirm when prompted.

To update a dynamic group's description

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Dynamic Groups.
   
   A list of the groups in your tenancy is displayed.
2. Click the dynamic group you want to update. The dynamic's group's details are displayed.
3. Click Edit Dynamic Group.
4. Edit the description. When finished, click Save Changes.

To update a dynamic group's matching rules

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Dynamic Groups.
   
   A list of the dynamic groups in your tenancy is displayed.
2. Click the dynamic group you want to update. The dynamic group's details are displayed.
3. Click **Edit All Matching Rules**.
4. Edit the matching rule in the text box; or, you can use the rule builder if the change is **supported by the rule builder.**

### Writing Matching Rules to Define Dynamic Groups

Matching rules define the resources that belong to the dynamic group. In the Console, you can either enter the rule manually in the provided text box, or you can use the **rule builder**. The rule builder lets you make selections and entries in a dialog, then writes the rule for you, based on your entries.

You can define the members of the dynamic group based on the following:

- **compartment ID** - include (or exclude) the instances that reside in that compartment based on compartment OCID
- **instance ID** - include (or exclude) an instance based on its instance OCID
- **tag namespace and tag key** - include (or exclude) instances tagged with a specific tag namespace and tag key. All tag values are included. For example, include all instances tagged with tag namespace `department` and the tag key `operations`.
- **tag namespace, tag key, and tag value** - include (or exclude) instances tagged with a specific value for the tag namespace and tag key. For example, include all instances tagged with the tag namespace `department` and the tag key `operations` and with the value '45'.

A matching rule has the following syntax:

For a single condition:

```
variable =|!= 'value'
```

For multiple conditions:

```
any|all {<condition>,<condition>,...}
```

Supported variables are:

- `instance.compartment.id` - the OCID of the compartment where the instance resides
- `instance.id` - the OCID of the instance
- `tag.<tagnamespace>.<tagkey>.value` - the tag namespace and tag key. For example, `tag.department.operations.value`.
- `tag.<tagnamespace>.<tagkey>.value='tagvalue'` - the tag namespace, tag key, and tag value. For example, `tag.department.operations.value='45'`

Here are some examples:

#### Include All Instances in a Specific Compartment in the Dynamic Group

To include all instances that are in a specific compartment, add a rule with the following syntax:

```
instance.compartment.id = '<compartment_ocid>'
```

You can type the rule directly in the text box, or you can use the **rule builder**.

Example entry in text box:

```
instance.compartment.id =
'ocid1:compartment:oc1:phx:samplecompartmentocid6q6igvfauxmima74jv'
```

To add the same rule using the Console rule builder:

- **For Include Instances That Match:** Select **All of the following**.
- **For Match Instances with:** Select **Compartment OCID**.
- **For Value:** Enter the compartment OCID. For this example, you would enter `ocid1:compartment:oc1:phx:samplecompartmentocid6q6igvfauxmima74jv`
All instances that currently exist or get created in the compartment (identified by the OCID) are members of this group.

### Include All Instances in Any of Two or More Compartments

To include all instances that reside in any of two (or more) compartments, add a rule with the following syntax:

```plaintext
Any {instance.compartment.id = '<compartment_ocid>', instance.compartment.id = '<compartment_ocid>'}
```

separating each compartment entry with a comma.

You can type the rule directly in the text box, or you can use the rule builder.

Example entry in the text box:

```plaintext
```

To add the same rule using the Console rule builder:

1. For **Include Instances That Match**: Select **Any of the following**.
2. For **Match Instances With**: Select **Compartment OCID**.
3. For **Value**: Enter the compartment OCID. For this example, you would enter `ocid1:compartment:oc1:phx:samplecompartmentocid6q6igvfauxmima74jv`
4. Click **+Additional Line**. Enter the following on the second line:
   - For **Match Instances With**: Select **Compartment OCID**.
   - For **Value**: Enter the additional compartment OCID. For this example, you would enter `ocid1:compartment:oc1:phx:samplecompartmentocidythksk89ekslsoelu2`

Instances that currently exist or are later created in either of the specified compartments are members of this group.

### Include All Instances Tagged with a Specific Namespace and Tag Key

To include all instances that are tagged with a specific tag namespace and tag key, add a rule with the following syntax:

```plaintext
tag.<tagnamespace>.<tagkey>.value
```

All instances assigned the tagnamespace.tagkey combination are included. Note that the tag value is not evaluated, so all values are included.

**Example**: Assume you have a tag namespace called `department` and a tag key called `operations`. You want to include all instances that are tagged with the namespace and tag key.

Enter the following rule in the text box:

```plaintext
tag.department.operations.value
```

All instances that currently exist or get created with the tag namespace and tag key `department.operations` are members of this group.

### Include All Instances In a Specific Compartment with a Specific Tag Namespace, Tag Key, and Tag Value

To include all instances in a specific compartment that are tagged with a specific tag namespace, key, and value, add a rule with the following syntax:

```plaintext
All {instance.compartment.id = '<compartment_ocid>', tag.<tagnamespace>.<tagkey>.value='<tagvalue>'}
```
All instances that are in the identified compartment and that are assigned the tagnamespace.tagkey with the specified tag value are included.

**Example:** Assume you have a tag namespace called `department` and a tag key called `operations`. You want to include all instances that are tagged with the value 45, that are in a particular compartment.

Enter the following statement in the text box:

```java
All
{instance.compartment.id='ocid1:compartment:oc1:phx:oc1:phx:samplecompartmentocid6q6igvfauxmima74jv,'
tag.department.operations.value='45'}
```

**Using the Rule Builder**

The rule builder is a tool available from the Console to help you write matching rules. The rule builder provides menus and text boxes for you to make entries and then writes the rule for you. The rule builder does have some limitations, so you can't use it for all cases.

**Limitations of the Rule Builder**

The rule builder does not support the following:

- Exclusion rules - the rule builder lets you select compartment IDs and instance IDs to include only.
- Rules based on tags - the rule builder does not allow you to select tags to include in your rule. To add a rule based on tag values, you need to enter the rule in the Rule text box using the syntax above.

**Launching the Rule Builder**

When you click **Create Dynamic Group**, the Rule Builder is displayed in the **Create Dynamic Group** dialog.

To create a matching rule using the rule builder:

1. Under the **Matching Rules** section, click **Rule Builder**.
2. From the **Include Instances That Match** menu, select **All of the following** or **Any of the following**.
   - **All of the following** includes only instances that match all of the statements in the rule.
   - **Any of the following** includes instances that match any of the statements in the rule.
3. Select a resource type from the **Match Instances With** menu, and then enter the OCID for the resource in the **Value** field:
   - **Compartment OCID** includes instances in the compartment you specify.
   - **Instance OCID** includes the instances with the OCIDs you specify.
4. Click **+Additional line** to add more statements to this rule.
   - When you add multiple statements to a rule, remember that **Any of the following** includes instances that match any of the statements. If you choose **All of the following**, instances must match all of the specifications in the statements to be included in the group.

**Examples Using the Rule Builder**

**Include All Instances in a Specific Compartment in the Dynamic Group**

To include all instances that are in a specific compartment, using the rule builder:

- Select **All of the following**.
- For **Match Instances With**: Select **Compartment OCID**.
- For **Value**: Enter the compartment OCID, for example,
  ocid1:compartment:oc1:phx:samplecompartmentocidythksk89ekslsoel1u2

All instances that currently exist or are later created in the compartment (identified by the OCID) are members of this group.

**Include All Instances in Any of Two or More Compartments**

To include all instances that reside in any of two (or more) compartments using the rule builder:
1. From the **Include Instances That Match** menu, select **Any of the following**.
2. In the first line, enter:
   - For **Match Instances With**, select **Compartment OCID**.
   - For **Value**, enter the compartment OCID, for example:
     `ocid1:compartment:oci:phx:samplecompartmentocid6q6igvfauxmima74jv`
3. Click **Additional Line**. Enter the following on the second line:
   - For **Match Instances With**, select **Compartment OCID**
   - For **Value**, enter the compartment OCID, for example:
     `ocid1:compartment:oci:phx:samplecompartmentocidythksk89ekslsoelu2`
4. Continue adding additional lines as needed for each compartment you want to include.

Instances that currently exist or get created in any of the specified compartments are members of this group.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage dynamic groups:

- CreateDynamicGroup
- ListDynamicGroups
- GetDynamicGroup
- UpdateDynamicGroup
- DeleteDynamicGroup

**Managing Network Sources**

This topic describes the basics of working with network sources.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for managing network sources. To write policies specifically for network sources, use the network-sources resource type, found with the other IAM components, in Details for IAM on page 2280.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Tagging Resources**

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

**Introduction to Network Sources**

A network source is a set of defined IP addresses. The IP addresses can be public IP addresses or IP addresses from VCNs within your tenancy. After you create the network source, you can reference it in policy or in your tenancy’s authentication settings to control access based on the originating IP address.

Network resources can only be created in the tenancy (or root compartment) and, like other Identity resources, reside in the home region. For information about the number of network sources you can have, see IAM Limits on page 225.

You can use network sources to help secure your tenancy in the following ways:
• Specify the network source in IAM policy to restrict access to resources.

When specified in a policy, IAM validates that requests to access a resource originate from an allowed IP address.

For example, you can restrict access to Object Storage buckets in your tenancy to only users that are signed in to Oracle Cloud Infrastructure through your corporate network. Or, you can allow only resources belonging to specific subnets of a specific VCN to make requests over a service gateway.

• Specify the network source in your tenancy's authentication settings to restrict sign in to the Console.

You can set up your tenancy's authentication policy to allow sign in to the Console from only those IP addresses specified in your network source. Users attempting to sign in from an IP address not on the allowed list in your network source will be denied access. For information on using a network source restriction in authentication policy, see Managing Authentication Settings on page 2468.

Support for Network Sources

The following services support using network sources in policy to restrict access to their resources:

Services that support network sources

• Analytics Cloud
• API Gateway
• Application Migration
• Audit
• Blockchain Platform Cloud
• Block Volume
• Budgets
• Compute
• Container Engine for Kubernetes
• Content and Experience
• Data Flow
• Data Safe
• Database
• Digital Assistant
• Events
• IAM
• Load Balancing
• Monitoring
• MySQL Database
• Notifications
• Object Storage
• Operations Insights
• OS Management
• Resource Manager
• Service Limits
• Streaming
• Tagging
• Unified Billing
• WAF

Allowing Access to Resources from Only Specified IP Addresses

To restrict access to requests made from a set of IP addresses, do the following:

1. Create a network source that specifies the allowed IP addresses.
2. Write a policy that uses the network source variable in a condition.
1. Create the Network Source

Follow the instructions provided for the Console or the API to create the network source.

A single network source can include IP addresses from a specific VCN, public IP addresses, or both.

To specify the VCN, you need the VCN OCID and the subnet IP ranges that you want to allow.

Examples:

- **Public IP addresses or CIDR blocks**: 192.0.2.143 or 192.0.2.0/24
- **VCN OCID**: ocid1.vcn.oc1.iad.aaaaaaaaexampleuniqueID
  - **Subnet IP addresses or CIDR blocks**: 10.0.0.4, 10.0.0.0/16

To allow any IP address from a specific VCN, use 0.0.0.0/0.

2. Write the Policy

The IAM service includes a variable to use in policy that allows you to scope your policy using a condition. The variable is:

```
request.networkSource.name
```

After you have created your network source, you can scope policies by using this variable in a condition. For example, assume you create a network source named "corpnet". You can restrict users of the group "CorporateUsers" to access your Object Storage resources only when their requests originate from IP addresses you specified in corpnet.

To do this, write a policy like the following:

```allow group CorporateUsers to manage object-family in tenancy where
request.networkSource.name='corpnet'
```

This policy allows users in the CorporateUsers group to manage Object Storage resources only when their requests originate from an allowed IP address specified in the network source "corpnet". Requests made from outside the specified IP ranges are denied. For general information about writing policies, see How Policies Work on page 2136.

Using the Console to Manage Network Sources

To create a network source

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Network Sources.
   A list of the network sources in your tenancy is displayed.
2. Click Create Network Source.
3. Enter the following:
   - **Name**: A unique name for the network source. The name must be unique in your tenancy. You cannot change this later. Avoid entering confidential information.
   - **Description**: A friendly description. You can change this later if you want to.
   - **Allow OCI Services**: This check box is selected by default to allow Oracle Cloud Infrastructure services access, even if the request comes from outside the specified IP addresses. Typically, you want this option enabled, for example, to allow a service to interact with objects in a bucket.
   - **Network Type**: Select one of the following:
     - **Public Network**: Enter a specific IP address or CIDR block range. For example: 192.0.2.143.
       Click **Another IP Address/CIDR Block** to add another allowed address or range.
     - **Virtual Cloud Network**: Enter the following for this option:
       - **VCN OCID**: Enter the OCID from the VCN you want to allow. For example: ocid1.vcn.oc1.iad.aaaaaaaaexampleuniqueID
       - **IP Address/CIDR Block**: Enter an IP address from the VCN or a subnet CIDR block. For example: 10.0.0.0/16 or 10.0.0.4.
         If you want to allow all subnets from the specified VCN, enter 0.0.0.0/0.
       Click **Another IP Address/CIDR Block** to add another allowed address or range from the same VCN.
   4. To add more IP ranges to this network source, click **Add Source**.
   5. **Show Advanced Options**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
   6. Click **Create**.

**To update a network source**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Network Sources**. A list of the network sources in your tenancy is displayed.
2. Locate the network source in the list and click its name to view its details.
3. Edit the network source:
   - To add more allowed IP addresses to this network source, click **Add Sources**. In the **Add Sources** dialog, click **Add Source** again, and enter the details for each IP address or CIDR block you want to add to this network source.
   - To remove an allowed source, click the Actions icon (three dots) and click **Delete**.
   - To change the setting of **Allow OCI Services**, click **Add Sources**. Update the check box setting and click **Update**.

**To delete a network source**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Groups**. The list of network sources in your tenancy is displayed.
2. Locate the network source in the list and click the Actions icon (three dots) for the item.
3. Click **Delete**.
4. Confirm when prompted.

**To apply tags to a network source**

For instructions, see **Resource Tags** on page 211.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.
Use these API operations to manage network sources:

- CreateNetworkSource
- ListNetworkSources
- GetNetworkSource
- UpdateNetworkSource
- DeleteNetworkSource

Creating the Network Source Object

A sample network source object looks like the following example:

```json
{
    "compartmentId" : "ocid1.tenancy.oc1..aaaaaaaabaexampleuniqueID",
    "description" : "Corporate IP ranges to be used for IP-based authorization",
    "name" : "corpnet",
    "virtualSourceList": [{
        "vcnId": "ocid1.vcn.oc1.iad.aaaaaaaaexampleuniqueID",
        "ipRanges": [ "129.213.39.0/24" ]
    }],
    "publicSourceList": [ "192.0.2.5", "192.0.2.6" ],
    "services": ["all"]
}
```

The elements are:

- **virtualSourceList** - specifies the VCN (OCID) and subnet IP ranges within that VCN that are allowed access. The `virtualSourceList` must contain both the VCN OCID and the subnet IP ranges:
  - **vcnID** - the OCID of the VCN
  - **IpRanges** - comma-separated list of the IP addresses or CIDR blocks of the subnets belonging to the specified VCN that are allowed to access the resource. To allow all ranges in the specified VCN, enter 0.0.0.0/0.

- **publicSourceList** - comma-separated list of the public IP ranges that are allowed access.
- **services** - currently, "all" or "none" are the only supported values. The default is "all". Specifying "all" allows Oracle Cloud Infrastructure services to access the resource.

Example:

```json
{
    "virtualSourceList": [{
        "vcnId": "ocid1.vcn.oc1.iad.aaaaaaaaexampleuniqueID",
        "ipRanges": [ "129.213.39.0/24" ]
    }],
    "publicSourceList": [ "192.0.2.0/25", "192.0.2.200" ],
    "services": ["all"]
}
```

Managing Compartments

This topic describes the basics of working with compartments.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for managing compartments.

For an additional policy related to compartment management, see Let a compartment admin manage the compartment on page 2154.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for compartments or other IAM components, see Details for IAM on page 2280.
Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Working with Compartments

When you first start working with Oracle Cloud Infrastructure, you need to think carefully about how you want to use compartments to organize and isolate your cloud resources. Compartments are fundamental to that process. Most resources can be moved between compartments. However, it’s important to think through your compartment design for your organization up front, before implementing anything. For more information, see "Setting Up Your Tenancy" in the Oracle Cloud Infrastructure Getting Started Guide.

The Console is designed to display your resources by compartment within the current region. When you work with your resources in the Console, you must choose which compartment to work in from a list on the page. That list is filtered to show only the compartments in the tenancy that you have permission to access. If you're an administrator, you'll have permission to view all compartments and work with any compartment's resources, but if you're a user with limited access, you probably won't.

Compartments are tenancy-wide, across regions. When you create a compartment, it is available in every region that your tenancy is subscribed to. You can get a cross-region view of your resources in a specific compartment with the tenancy explorer. See Viewing All Resources in a Compartment on page 235.

For added security, you can associate a compartment with a security zone. For more information, see Security Zones.

Creating Compartments

When creating a compartment, you must provide a name for it (maximum 100 characters, including letters, numbers, periods, hyphens, and underscores) that is unique within its parent compartment. You must also provide a description, which is a non-unique, changeable description for the compartment, from 1 through 400 characters. Oracle will also assign the compartment a unique ID called an Oracle Cloud ID. For more information, see Resource Identifiers.

You can create subcompartments in compartments to create hierarchies that are six levels deep.

For information about the number of compartments you can have, see Service Limits on page 215.

Access Control for Compartments

After creating a compartment, you need to write at least one policy for it, otherwise no one can access it (except administrators or users who have permissions set at the tenancy level). When creating a compartment inside another
compartment, the compartment inherits access permissions from compartments higher up its hierarchy. For more information, see Policy Inheritance on page 2140.

When you create an access policy, you need to specify which compartment to attach it to. This controls who can later modify or delete the policy. Depending on how you've designed your compartment hierarchy, you might attach it to the tenancy, a parent, or to the specific compartment itself. For more information, see Policy Attachment on page 2141.

Putting Resources in a Compartment
To place a new resource in a compartment, you simply specify that compartment when creating the resource (the compartment is one of the required pieces of information to create a resource). If you're working in the Console, you just make sure you're first viewing the compartment where you want to create the resource. Keep in mind that most IAM resources reside in the tenancy (this includes users, groups, compartments, and any policies attached to the tenancy) and can't be created in or managed from a specific compartment.

Moving Resources to a Different Compartment
Most resources can be moved after they are created. There are a few resources that you can't move from one compartment to another. Also, you can't move certain resources from a security zone to a standard compartment because it might be less secure. For details about restrictions for resources in security zones, see Restrict Resource Movement.

Some resources have attached resource dependencies and some don’t. Not all attached dependencies behave the same way when the parent resource moves.

For some resources, the attached dependencies move with the parent resource to the new compartment. The parent resource moves immediately, but in some cases attached dependencies move asynchronously and are not visible in the new compartment until the move is complete.

For other resources, the attached resource dependencies do not move to the new compartment. You can move these attached resources independently.

After you move the resource to the new compartment, the policies that govern the new compartment apply immediately and affect access to the resource. Depending on the structure of your compartment organization, metering, billing, and alarms can also be affected.

See the service documentation for individual resources to familiarize yourself with the behavior of each resource and its attachments.

Viewing Resources in a Compartment
It's not possible to get a list of all the resources in a compartment by using a single API call. Instead you can list all the resources of a given type in the compartment (e.g., all the instances, all the block storage volumes, etc.).

Tip:
In the Console, the tenancy explorer allows you to get a list of resources in a compartment, across regions, with some limitations. For more information, see Viewing All Resources in a Compartment on page 235.

Discovering Resources in Compartments
With Resource Manager you can capture deployed resources as Terraform configuration and state files using resource discovery. The created stack provides you with a Terraform configuration that you can use to programmatically manage, version, and persist your IT infrastructure as "infrastructure as code."

A stack created from a compartment represents all supported resources in the entire compartment, at the appropriate scope. If you select the root compartment for your tenancy, then the scope is the tenancy level, such as users and groups. If you select a non-root compartment, then the scope is compartment level, such as Compute instances.

Stack creation is supported from a single compartment only. Stacks cannot be created from nested compartments.

For instructions, see To create a stack on page 3557.
Deleting Compartments

To delete a compartment, it must be empty of all resources. Before you initiate deleting a compartment, be sure that all its resources have been moved, deleted, or terminated, including any policies attached to the compartment.

Important:

Some resource types can't be deleted, therefore, compartments containing these resource types can't be deleted. A resource type that can't be deleted is:

- Data transfer jobs

The delete action is asynchronous and initiates a work request. The state of the compartment changes to Deleting while the work request is executing. It typically takes several minutes for the work request to complete. While it is in the Deleting state it is not displayed on the compartment picker. If the work request fails, the compartment is not deleted and it returns to the Active state.

After a compartment is deleted, its state is updated to Deleted and a random string of characters is appended to its name, for example, CompartmentA might become CompartmentA.qR5hP2BD. Renaming the compartment allows you to reuse the original name for a different compartment. Oracle displays the deleted compartment on the Compartments page for 365 days. The deleted compartment is removed from the compartment picker. If any policy statements reference the deleted compartment, the name in the policy statement is updated to the new name.

Troubleshooting tips for when a compartment fails to delete

If the compartment fails to delete, verify that you have removed all the resources:

- For most resources, you can use the tenancy explorer to help you locate them. See Resources Supported by the Tenancy Explorer on page 236 for the list of supported resources.

To view resources in a compartment

Open the navigation menu. Under Governance and Administration, go to Governance and click Tenancy Explorer.

The tenancy explorer opens with a view of the root compartment. Select the compartment you want to explore from the compartment picker on the left side of the Console. After you select a compartment, the resources that you have permission to view are displayed. The Name and Description of the compartment you are viewing are displayed at the top of the page. To also list all resources in the subcompartments of the selected compartment, select Show resources in subcompartments. When viewing resources in all subcompartments, it is helpful to use the Compartment column in the results list to see the compartment hierarchy where the resource resides.

- Verify that there are no policies in the compartment (polices are not included in Search results).

To find policies in a compartment

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
2. From the compartments list on the left, select the compartment you want to delete.

Policies attached to the compartment are displayed.

- If you can't locate any resources in the compartment, check with your Administrator; you might not have permission to view all resources.

Important:

There is a known issue causing deleted compartments to continue to count against your service limit of compartments. See Deleted compartments continue to count against service limits.

Recovering Compartments

To recover a compartment, you must first select it from the list on the Compartment page. You may have to use the state filter to see the deleted compartment. Remember that deleted compartments are renamed by appending a random string of characters to the original compartment name. For example, CompartmentA might become CompartmentA.qR5hP2BD. Oracle displays the deleted compartment on the Compartments page for 365 days.
When you recover a deleted compartment, the name is not changed. For example, if you recover a deleted compartment named CompartmentA.qR5hP2BD, the name remains the same. Because policy statements are updated to use the new names of deleted compartments, any policy statements that had referenced the deleted compartment now reference the recovered compartment.

Adding Tag Defaults for a Compartment

Tag defaults let you specify tags to be applied automatically to all resources, at the time of creation, in the current compartment. For more information, see Managing Tag Defaults on page 3927.

Moving a Compartment to a Different Parent Compartment

You can move a compartment to a different parent compartment within the same tenancy. When you move a compartment, all its contents (subcompartments and resources) are moved with it. Moving a compartment has implications for the contents. These implications are described in the following sections. Ensure that you are aware of these before you move a compartment.

- Required IAM Policy on page 2431
- Restrictions on Moving Compartments on page 2435
- Understanding the Policy Implications When You Move a Compartment on page 2436
- Understanding Compartment Quota Implications When You Move a Compartment on page 2442
- Understanding Tagging Implications When You Move a Compartment on page 2442

Required IAM Policy

To move a compartment, you must belong to a group that has manage all-resources permissions on the lowest shared parent compartment of the current compartment and the destination compartment.

Restrictions on Moving Compartments

- A security zone compartment can only have subcompartments that are also security zone compartments. You can't move a standard compartment that's not in a security zone to a destination compartment that is in a security zone. For more information, see Security Zones.
• You can't move a compartment to a destination compartment with the same name as the compartment being moved.

For example, assume compartment A and compartment B are both under the root compartment. Under compartment A is a subcompartment, also called compartment B. You cannot move the compartment B to the parent compartment B.

You can’t move a compartment under a parent compartment with the same name

• Two compartments within the same parent cannot have the same name. Therefore you can't move a compartment to a destination compartment where a compartment with the same name already exists.

Understanding the Policy Implications When You Move a Compartment

After you move a compartment to a new parent compartment, the access policies of the new parent take effect and the policies of the previous parent no longer apply. Before you move a compartment, ensure that:

• You are aware of the policies that govern access to the compartment in its current position.
• You are aware of the policies in the new parent compartment that will take effect when you move the compartment.
In some cases, when moving nested compartments with policies that specify the hierarchy, the policies are automatically updated to ensure consistency.

**Policy Examples**

**Groups with Permissions in the Current Compartment Lose Access; Groups with Permissions in the Destination Compartment Gain Access**

The following figure shows a compartment hierarchy in which compartment C, a child of A:B is moved to the hierarchy A:D.

![Diagram showing compartment hierarchy]

The tenancy has the following policies defined for compartments B and D:

**Policy1:** Allow group G1 to manage instance-family in compartment A:B

**Policy2:** Allow group G2 to manage instance-family in compartment A:D

Impact when compartment C is moved from B to D:
Group G1 can no longer manage instance-families in compartment C.
Group G2 can now manage instance-families in compartment C.

Ensure that you are aware not only of what groups lose permissions when you move a compartment, but also what groups will gain permissions.

**Automatic Update of Policies**

When you move a compartment, some policies will be automatically updated. Policies that specify the compartment hierarchy down to the compartment being moved will automatically be updated when the policy is attached to a shared ancestor of the current and target parent. Consider the following examples:

**Example 1: Policy automatically updated**

![Diagram showing policy automatically updated](Image)
In this example, you move compartment A from Operations:Test to Operations:Dev. The policy that governs compartment A is attached to the shared parent, Operations. When the compartment is moved, the policy statement is automatically updated by the IAM service to specify the new compartment location.

The policy

Allow group G1 to manage buckets in compartment Test:A

is updated to

Allow group G1 to manage buckets in compartment Dev:A

No manual intervention is required to allow group G1 to continue to access compartment A in its location.

**Example 2: Policy not updated**
In this example, you move compartment A from Operations:Test to Operations:Dev. However, the policy that governs compartment A here is attached directly to the Test compartment. When the compartment is moved, the policy is not automatically updated. The policy that specifies compartment A is no longer valid and must be manually removed. Group G1 no longer has access to compartment A in its new location under Dev. Unless another existing policy grants access to group G1, you must create a new policy to allow G1 to continue to manage buckets in compartment A.

Example 3: Policy attached to the tenancy is updated
In this example, you move compartment A from Operations:Test to HR:Prod. The policy that governs compartment A is attached to the tenancy, which is a shared ancestor by the original parent compartment and the new parent compartment. Therefore, when the compartment is moved, the policy statement is automatically updated by the IAM service to specify the new compartment location.

The policy statement:

| Allow group G1 to manage buckets in compartment Operations:Test:A |

is updated to

| Allow group G1 to manage buckets in compartment HR:Prod:A |

No manual intervention is required to allow group G1 to continue to access compartment A.
Understanding Compartment Quota Implications When You Move a Compartment

When you move one compartment to another, resource quotas in the destination compartment are not verified and are not enforced. Therefore, if the compartment move results in a quota violation in the destination compartment, the move is not blocked. After the move is complete, the destination compartment will be in an over-quota state. You will not be able to create new resources that are over-quota until you either adjust the quotas for the destination compartment or remove resources to comply with the existing quota. For more information on managing compartment quotas, see Compartment Quotas on page 243.

Understanding Tagging Implications When You Move a Compartment

Tags are not automatically updated after a compartment move. If you have implemented a tagging strategy based on compartment, you must update the tags on the resources after the move. For example, assume CompartmentA has a child compartment, CompartmentB. CompartmentA is set up with tag defaults so that every resource in CompartmentA is tagged with TagA. Therefore CompartmentB and all its resources are tagged with default tag, TagA. When you move CompartmentB to CompartmentC, it will still have the default tags from CompartmentA. If you have set up default tags for CompartmentC, you'll need to add those to the resources in the moved compartment.

Using the Console

To create a compartment

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A list of the compartments you have access to is displayed.
2. Navigate to the compartment in which you want to create the new compartment:
   - To create the compartment in the tenancy (root compartment) click Create Compartment.
   - Otherwise, click through the hierarchy of compartments until you reach the detail page of the compartment in which you want to create the compartment. On the Compartment Details page, click Create Compartment.
3. Enter the following:

- **Name:** A unique name for the compartment (maximum 100 characters, including letters, numbers, periods, hyphens, and underscores). The name must be unique across all the compartments in your tenancy. Avoid entering confidential information.
- **Description:** A friendly description. You can change this later if you want to.
- **Compartment:** The compartment you are in is displayed. To choose another compartment to create this compartment in, select it from the list.
- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

4. Click **Create Compartment.**

Next, you might want to write a policy for the compartment. See To create a policy on page 2454.

**To update a compartment's name**

You can't update the name of a compartment that is associated with a security zone. For more information, see Security Zones.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Compartments**.

   A list of the compartments in your tenancy is displayed.

2. For the compartment you want to rename, click the Actions icon (three dots), and then click **Rename Compartment**.

   **Tip:**
   
   You can't change the name of your root compartment.

3. Enter the new **Name**. The name must be unique across all the compartments in your tenancy. The name can have a maximum of 100 characters, including letters, numbers, periods, hyphens, and underscores. Avoid entering confidential information.

4. Click **Rename Compartment**.

**To update a compartment's description**

You can't update the description of a compartment that is associated with a security zone. For more information, see Security Zones.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Compartments**.

   A list of the compartments in your tenancy is displayed.

2. For the compartment you want to update, click the Actions icon (three dots), and then click **Edit Compartment Description**.

3. Enter the new description. Avoid entering confidential information.

4. Click **Save**.

**To view the contents of a compartment**

1. Open the Console,

2. Open the navigation menu and select the type of resource you want to view. For example, click **Compute** to view all your Compute resources.

3. Choose the compartment from the list on the left side of the page. The page updates to show only the resources in that compartment.

Remember that most IAM resources reside in the tenancy (this includes users, groups, and compartments). Policies can reside in either the tenancy (root compartment) or other compartments.

**To move a compartment**

To move a compartment, you must belong to a group that has **manage all-resources** permissions on the lowest shared parent compartment of the current compartment and the destination compartment.
1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A list of the compartments in your tenancy is displayed. If the compartment you want to move is not directly beneath the root compartment, click through the hierarchy of compartments to view the wanted compartment.

2. For the compartment you want to move, click the Actions icon (three dots), and then click Move Compartment.

3. Select the destination compartment.

4. Confirm that you are aware of the implications of the move.

5. Click Move Compartment.

To move a resource to a different compartment

1. Open the Console.

2. Open the navigation menu and select the type of resource you want to work with. For example, click Compute to view all your Compute resources.

3. In the List Scope section, select a compartment. Resources in the selected compartment are displayed.

4. Find the resource in the list, click the the Actions icon (three dots), and follow the prompts to move the resource to a new compartment. See the resource documentation for specific steps.

The resource is moved immediately. If attached resource dependencies move with the parent resource, the resource dependencies are moved asynchronously, and do not appear in the new compartment until the move is complete.

To apply tags to a compartment

For instructions, see Resource Tags on page 211.

To manage tag defaults for a compartment

See Managing Tag Defaults on page 3927.

To delete a compartment

You must remove all resources from a compartment before you can delete it.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A list of the compartments in your tenancy is displayed.

2. For the compartment you want to delete, click the Actions icon (three dots), and then click Delete Compartment.

3. At the prompt, click OK.

After you click OK, a work request is submitted to delete the compartment. The compartment state changes to Deleting. If the work request fails, the state returns to Active.

To recover a compartment

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments. A list of the compartments in your tenancy is displayed.

2. In State, select Deleted.

3. For the compartment you want to recover, click the Actions icon (three dots), and then click Recover.

4. At the prompt, click OK.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage compartments:

- CreateCompartment
- ListCompartments
- GetCompartment: Returns the metadata for the compartment, not its contents.
- UpdateCompartment
- DeleteCompartment
- MoveCompartment
IAM

- **GetWorkRequest**: Gets the work requests spawned by the DeleteCompartment operation.
- **RecoverCompartment**

You can retrieve the contents of a compartment only by resource type. There's no API call that lists all resources in the compartment. For example, to list all the instances in a compartment, call the Core Services API `ListInstances` operation and specify the compartment ID as a query parameter.

### Managing Regions

This topic describes the basics of managing your region subscriptions. For more information about regions in Oracle Cloud Infrastructure, see Regions and Availability Domains on page 180. For information about Platform Services regions, see Managing Platform Services Regions on page 2447.

### Required IAM Policy

If you're in the Administrators group, then you have the required access to manage region subscriptions.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for managing regions or other IAM components, see Details for IAM on page 2280.

### The Home Region

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your *home region*. Your home region is where your IAM resources are defined. When you subscribe to another region, your IAM resources are available in the new region, however, the master definitions reside in your home region and can only be changed there.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your home region contains your account information and identity resources. It is not changeable after your tenancy is provisioned. If you are unsure which region to select as your home region, contact your sales representative before you create your account</td>
</tr>
</tbody>
</table>

Resources that you can create and update only in the home region are:

- Users
- Groups
- Policies
- Compartments
- Dynamic groups
- Federation resources

When you use the API to update your IAM resources, you must use the endpoint for your home region. IAM automatically propagates the updates to all regions in your tenancy.

When you use the Console to update your IAM resources, the Console sends the requests to the home region for you. You don't need to switch to your home region first. IAM then automatically propagates the updates to all regions in your tenancy.

When you subscribe your tenancy to a new region, all the policies from your home region are enforced in the new region. If you want to limit access for groups of users to specific regions, you can write policies to grant access to specific regions only. For an example policy, see Restrict admin access to a specific region on page 2154.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM Updates Are Not Immediate Across All Regions</td>
</tr>
<tr>
<td>When you create or update an IAM resource, be aware that you need to allow up to several minutes for the changes in your home region to become available in all regions.</td>
</tr>
</tbody>
</table>
**Using the Console to Manage Infrastructure Regions**

To view the list of infrastructure regions

Open the Console, open the Region menu, and then click Manage Regions. A list of the regions offered by Oracle Cloud Infrastructure is displayed. Regions that you have not subscribed to provide a button to create a subscription.

**To subscribe to an infrastructure region**

1. Open the Console, open the Region menu, and then click Manage Regions. The list of regions available to your tenancy Oracle Cloud Infrastructure is displayed. Your home region is labeled.
2. Locate the region you want to subscribe to and click Subscribe.

   Note that it could take several minutes to activate your tenancy in the new region.

   Remember, your IAM resources are global, so when the subscription becomes active, all your existing policies are enforced in the new region.

   To switch to the new region, use the Region menu in the Console. See Switching Regions on page 45 for more information.

You cannot unsubscribe from a region.

**Using the API to Work with Infrastructure Regions**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage infrastructure regions:

- GetTenancy
- ListRegions: Returns a list of regions offered by Oracle Cloud Infrastructure in your selected realm.
- CreateRegionSubscription
- ListRegionSubscriptions

You cannot unsubscribe from a region.

**Region FAQs**

Can an individual user subscribe to a region?

A region subscription is at the tenancy level. An administrator can subscribe the tenancy to a region. All IAM policies are enforced in the new region, so all users in the tenancy will have the same access and permissions in the new region.

Can I see my existing resources in the new region?

When you select a region in the Console, you are shown a view of the resources in your selected region. Most cloud resources (instances, VCNs, buckets, etc.) exist only in a specific region, so you only see them when you select the region where they were created. The exception is IAM resources: compartments, users, groups, and policies are global across all regions. See also Working Across Regions on page 46.

How do my service limits apply to the new region?

Service limits can be scoped to the tenant level, the region level, or the availability domain level. When you subscribe to a new region, you get access to the region and its availability domains. Service limits apply accordingly. The service limits page lists the scope of each resource limit.

Can I restrict access to a specific region?

Yes. You can write policies that grant permissions in a specified region only. For an example policy, see Restrict admin access to a specific region on page 2154.

Can I change my home region?

No. Oracle assigns your home region and you can't change it.
Managing Platform Services Regions

This topic describes how to manage Platform Services region subscriptions.

About the Platform Services Regions

You can manage Platform Services regions in the Console.

To use Platform Services that are not natively integrated with Oracle Cloud Infrastructure, you need to subscribe to the Platform Services region as well as the Infrastructure region. For example, to create a Platform Service instance in the Germany Central (Frankfurt) region, you need to subscribe your tenancy to both the Infrastructure region: Germany Central (Frankfurt) and to the Platform Service region: Europe and Middle East.

To know which services require the Platform Service region subscription, you can view the list under More Oracle Cloud Services on the Console navigation menu. A sample of the navigation to these services is shown in the following screenshot:
Before you can view these services in the Console or access the Manage Platform Services Regions page, your tenancy must have entitlements to use the Platform Services.

**Managing Platform Services Regions**

**To view and subscribe to Platform Services regions**

1. Open the Console, open the Region menu, and then click Manage Regions.
2. On the **Manage Regions** page, click **Platform Services Regions**.

   The list of geographical regions is displayed. Regions that you have not subscribed to provide a button to create a subscription. A sample of the **Platform Services Regions** page is shown in the following screenshot:

   ![Platform Services Regions](image)

3. To subscribe to a region, locate the region in the list and click **Subscribe**.

   It might take several minutes to activate your tenancy in the new region.

### Managing the Tenancy

This topic describes options on the tenancy details page in the Console.

#### Required IAM Policy

If you're in the Administrators group, then you have the required access to manage the tenancy.

If you're new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142. If you want to dig deeper into writing policies for your tenancy and other IAM components, see [Details for IAM](#) on page 2280.

#### Viewing the Tenancy Details Page

To view the tenancy details page:

Open the **Profile** menu (Ƈ) and click **Tenancy**: `<your_tenancy_name>`.

#### Details About Your Tenancy

The tenancy details page provides the following information about your tenancy:

**TENANCY OCID**

Every Oracle Cloud Infrastructure resource has an Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). You need your tenancy's OCID to use the API. You'll also need it when contacting support.
HOME REGION

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one of the available regions. This is your home region. Your home region is where your IAM resources are defined. For more information about the home region, see The Home Region on page 2445.

NAME

Your tenancy name. Your tenancy name is typically chosen when you set up your Oracle Cloud account.

CSI NUMBER

Your Customer Service Identifier for Oracle Support.

OBJECT STORAGE DESIGNATED COMPARTMENTS AND NAMESPACE

The Object Storage service provides API support for both Amazon S3 Compatibility API and Swift API. By default, buckets created using the Amazon S3 Compatibility API or the Swift API are created in the root compartment of the Oracle Cloud Infrastructure tenancy. You can designate a different compartment for the Amazon S3 Compatibility API or Swift API to create buckets in. For more information, see Designating Compartments for the Amazon S3 Compatibility and Swift APIs on page 3497.

For information about your Object Storage namespace, see Understanding Object Storage Namespaces on page 3395.

TAGS

Tagging allows you to define keys and values and associate them with resources. You can then use the tags to help you organize and list resources based on your business needs. If you have permissions to manage the tenancy, you also have permissions to apply free-form tags. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211.

SERVICE LIMITS

The limits allotted to your tenancy and usage against these limits. Not all service resources are included in the list shown here on the Console. For more information or to request an increase, see Service Limits on page 215.

Using the API

Many of the options set on this page are managed through the owning service. For example, the Object Storage settings are managed with the Object Storage service API, and setting the Audit log retention period is handled by the Audit service API.

To get information about your tenancy use the following operation:

- GetTenancy

To tag a tenancy, use the following operations:

- GetCompartment
- UpdateCompartment

In the above operations, use the tenancy OCID for the compartmentID parameter.

Managing Policies

This topic describes how to create, edit, and delete policies.

Required IAM Policy

If you're in the Administrators group, then you have the required access for managing policies.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies to control who else can write policies or manage other IAM components, see Let a compartment admin manage the compartment on page 2154, and also Details for IAM on page 2280.
Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Working with Policies

If you haven't already, make sure to read How Policies Work on page 2136 to understand the basics of how policies work.

When creating a policy, you must specify the compartment where it should be attached, which is either the tenancy (the root compartment) or another compartment. Where it's attached governs who can later modify or delete it. For more information, see Policy Attachment on page 2141. When creating the policy in the Console, you attach the policy to a compartment by creating the policy in that compartment. If you're using the API, you specify the identifier of the compartment in the CreatePolicy request.

When creating a policy, you must also provide a non-changeable name for it. The name must be unique across all policies in the compartment where you create it. You must also provide a description, which is a non-unique, changeable description for the policy. Oracle will also assign the policy a unique ID called an Oracle Cloud ID. For more information, see Resource Identifiers.

Note:
If you delete a policy and then create a new policy with the same name, they'll be considered different policies because they'll have different OCIDs.

For information about how to write a policy, see How Policies Work on page 2136 and Policy Syntax on page 2164. When using the Console to write policies, you can use the policy builder to help you construct the syntax of the policies you want to add.

When you create a policy, make changes to an existing policy, or delete a policy, your changes go into effect typically within 10 seconds.

You can view a list of your policies in the Console or with the API. In the Console, the list is automatically filtered to show only the policies attached to the compartment you're viewing. To determine which policies apply to a particular group, you must view the individual statements inside all your policies. There isn't a way to automatically obtain that information in the Console or API.

For information about the number of policies you can have, see Service Limits on page 215.

Writing Policy Statements with the Policy Builder

The policy builder in the Console helps you quickly create common policies without the need to manually type the policy statements. The policy builder automatically suggests the permissions that an administrator can grant to groups of users or resources in their tenancy, as well as target resources like instances, networks, and buckets. Most of the policies suggested in the policy builder can also be found in Common Policies on page 2142, where you can learn more details about the access provided by each policy and the use cases for each. Users who don't need the suggestions offered by the policy builder or who have more complex policy requirements can bypass the builder's basic option and go straight to the advanced editor, where you can directly enter the policy statements in a free-form text box.

Features of the Policy Builder

The policy builder provides policy templates that you can complete to create policies for your tenancy. A policy template includes all the statements needed to provide the permissions to perform a task or set of related tasks in a service in OCI. To complete the template, select the group from a menu of existing groups and select the location from the list of compartments in your tenancy.

The policy templates in the policy builder are grouped by use case, such as network management, storage management, and account management, to make them easy to browse and find the permission set you need.
For example, assume you are setting up the network administrators for your tenancy. You need to grant a group of users the permissions required to work with all the resources in the Networking service. To create this policy in the policy builder:

- First, find the policy you want: From the Policy Use Cases menu, select Network Management. If you are not sure which use case a policy belongs to, you can leave this option set to All to browse all the templates.
- From the Common Policy Templates menu, select Let network admins manage a cloud network.

The policy builder displays the policy statements that will be created. In this case, there is only one statement:

```
Allow {group name} to manage virtual-network-family in {location}
```

- Now, all you need to do is select the group and location for the policy: When you select a group, the {group name} in the displayed policy statement also updates with your selection.
- Finally, select the location. You can traverse the compartment hierarchy to find and select the appropriate compartment. To create the policy in the tenancy, choose the root compartment.

### Customizing Policies

If you find that a template doesn't fit your needs exactly, then you can customize the policies provided by adding statements, removing statements, adding conditions, or other changes to create the policy you need. Click **Customize (Advanced)** to edit the statements in a free-form text box. When entering statements directly in the text box, ensure that you follow the Policy Syntax on page 2164 rules.

Examples of customizing the Network Admins policy:

- You need to include another group, GroupB to this policy. To add a group:
  
  Click **Customize (Advanced)**. In the text box, type the changes to the policy (following the required syntax).

```
Allow group GroupA, GroupB to manage virtual-network-family in
compartment CompartmentA
```

---

**Oracle Cloud Infrastructure User Guide**  
2452
• You need to add a condition to the statement. For example, you want to ensure that only users who have been verified by MFA can manage your networks. You can add that condition to the statement as follows:

```
Allow group GroupA to manage virtual-network-family in compartment CompartmentA where request.user.mfaTotpVerified='true'
```

• You want to add another statement to the policy. For example, you want GroupA to be allowed to use instances. To add another statement, enter it on the next line:

```
Allow group GroupA to manage virtual-network-family in compartment CompartmentA
Allow group GroupA to use instance-family in compartment CompartmentA
```

**Editing Policies with the Policy Builder**

After you have created the policy, you can enter any statement changes you need to make directly in the policy text. The template selector is only available when creating a new policy. The editor lets you delete, add, edit, or change the statement order.
Using the Console
To create a policy

Prerequisite: The group and compartment that you're writing the policy for must already exist.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed.
2. Click Create Policy.
3. Enter the following:
   - **Name**: A unique name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later. Avoid entering confidential information.
   - **Description**: A friendly description. You can change this later if you want to.
   - **Compartment**: If you want to attach the policy to a compartment other than the one you're viewing, select it from list. Where the policy is attached controls who can later modify or delete it (see Policy Attachment on page 2141).
4. Enter the policy statements using the policy builder. Use the Basic option if you want to choose from common policy templates, which you can also customize. Use the Customize (Advanced) option if you already know how to write the statements you need and you want to simply type them in a text box.

   To use the policy builder Basic option:
   a. Select from the Policy Use Cases menu to filter the list of policy templates. If you're not sure which use case to choose, you can browse all the templates in the Common Policies Templates list.
   b. Select the template that best matches your requirements from the Common Policies Templates list.

      The policy builder displays the description of the chosen policy and lists the policy statements that it includes.
   c. Select the Group that this policy applies to.
   d. Select a Location. The location is the compartment that this policy grants access to. The compartment you choose here must be either the compartment you chose to attach the policy to in Step 3, or a compartment within the hierarchy of that compartment.
   e. If you need to modify the policy statements, click Customize (Advanced).

   To use the Customize (Advanced) option:
   a. Click Customize (Advanced).
   b. Enter or edit policy statements following the format described in Policy Syntax on page 2164, entering one statement per line.
5. To add tags to this policy, click Show Advanced Options. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
6. If you want to create another policy, select Create Another Policy.
7. Click Create.

   The new policy will go into effect typically within 10 seconds.

To get a list of your policies

Open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're currently viewing is displayed. If you want to view policies attached to a different compartment, select that compartment from the list on the left. You can't get a single list of all policies; they're always displayed by compartment.

To determine which policies apply to a particular group, you must view the individual statements inside all your policies. There isn't a way to automatically obtain that information in the Console.

To update the description for an existing policy

This is available only through the API. A workaround is to create a new policy with the new description and delete the old policy.
To update the statements in an existing policy

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed. If you don't see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).
2. Click the policy you want to update. The policy's details and statements are displayed.
3. Click Edit Policy Statements. Use the Basic policy builder option if you want to interact with the statements using graphical controls. Use the Advanced policy builder option to edit the statements in a simple text box.

   To use the Basic option:
   • To revise a statement, enter the changes following the format in Policy Basics on page 2137 and Policy Syntax on page 2164.
   • To add a statement, click +Another Statement and enter the statement following the required format.
   • To delete a statement, click the X next to the statement.
   • To rearrange the order of the statements, use the up and down arrows to move statements to the correct order, or grab the handle to drag and drop statements to the preferred position.

   To use the Advanced option:
   • Select Advanced.
   • Revise the policy statements in the text box following the format in Policy Basics on page 2137 and Policy Syntax on page 2164.
4. Click Save Changes when you are finished editing.

Your changes will go into effect typically within 10 seconds.

To delete a policy

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies. A list of the policies in the compartment you're viewing is displayed. If you don't see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).
2. For the policy you want to delete, click Delete.
3. Confirm when prompted.

Your changes will go into effect typically within 10 seconds.

To apply tags to a policy

For instructions, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Note:

Updates Are Not Immediate Across All Regions

Your IAM resources reside in your home region. To enforce policy across all regions, the IAM service replicates your resources in each region. Whenever you create or change a policy, user, or group, the changes take effect first in the home region, and then are propagated out to your other regions. It can take several minutes for changes to take effect in all regions. For example, assume you have a group with permissions to launch instances in the tenancy. If you add UserA to this group, UserA will be able to launch instances in your home region within a minute. However, UserA will not be able to launch instances in other regions until the replication process is complete. This process can take up to several minutes. If UserA tries to launch an instance before replication is complete, they will get a not authorized error.
Use these API operations to manage policies:

• CreatePolicy
• ListPolicies
• GetPolicy
• UpdatePolicy
• DeletePolicy

Managing User Credentials

This topic describes the basics of working with Oracle Cloud Infrastructure Identity and Access Management (IAM) user credentials. If you're not already familiar with the available credentials, see User Credentials on page 2360.

Working with Console Passwords and API Keys

Each user automatically has the ability to change or reset their own Console password, as well as manage their own API keys. An administrator does not need to create a policy to give a user those abilities.

To manage credentials for users other than yourself, you must be in the Administrators group or some other group that has permission to work with the tenancy. Having permission to work with a compartment within the tenancy is not sufficient. For more information, see The Administrators Group and Policy on page 2125.

IAM administrators (or anyone with permission to the tenancy) can use either the Console or the API to manage all aspects of both types of credentials, for themselves and all other users. This includes creating an initial one-time password for a new user, resetting a password, uploading API keys, and deleting API keys.

Users who are not administrators can manage their own credentials. In the Console, users can:

• Change or reset their own password.
• Upload an API key in the Console for their own use (and also delete their own API keys).

And with the API, users can:

• Reset their own password with CreateOrResetUIPassword.
• Upload an additional API key to the IAM service for their own use with UploadApiKey (and also delete their own API keys with DeleteApiKeyValue). Remember that a user can't use the API to change or delete their own credentials until they themselves upload a key in the Console, or an administrator uploads a key for that user in the Console or the API.

A user can have a maximum of three API keys at a time.

Working with Auth Tokens

Note:

"Auth tokens" were previously named "Swift passwords". Any Swift passwords you had created are now listed in the Console as auth tokens. You can continue to use the existing passwords.

Auth tokens are Oracle-generated token strings that you can use to authenticate with third-party APIs that do not support Oracle Cloud Infrastructure's signature-based authentication. Each user created in the IAM service automatically has the ability to create, update, and delete their own auth tokens in the Console or the API. An administrator does not need to create a policy to give a user those abilities. Administrators (or anyone with permission to the tenancy) also have the ability to manage auth tokens for other users.

Note that you cannot change your auth token to a string of your own choice. The token is always an Oracle-generated string.

Auth tokens do not expire. Each user can have up to two auth tokens at a time. To get an auth token in the Console, see To create an auth token on page 2463.

Oracle Cloud Infrastructure User Guide 2456
Using an Auth Token with Swift

Swift is the OpenStack object store service. If you already have an existing Swift client, you can use it with the Recovery Manager (RMAN) to back up an Oracle Database System (DB System) database to Object Storage. You will need to get an auth token to use as your Swift password. When you sign in to your Swift client, you provide the following:

- Your Oracle Cloud Infrastructure Console user login
- Your Swift-specific auth token, provided by Oracle
- Your organization's Oracle tenant name

Any user of a Swift client that integrates with Object Storage needs permission to work with the service. If you're not sure if you have permission, contact your administrator. For information about policies, see How Policies Work on page 2136. For basic policies that enable use of Object Storage, see Common Policies on page 2142.

Working with Customer Secret Keys

Note:

"Customer Secret keys" were previously named "Amazon S3 Compatibility API keys". Any keys you had created are now listed in the Console as Customer Secret keys. You can continue to use the existing keys.

Object Storage provides an API to enable interoperability with Amazon S3. To use this Amazon S3 Compatibility API, you need to generate the signing key required to authenticate with Amazon S3. This special signing key is an Access Key/Secret Key pair. Oracle provides the Access Key that is associated with your Console user login. You or your administrator generates the Customer Secret key to pair with the Access Key.

Each user created in the IAM service automatically has the ability to create, update, and delete their own Customer Secret keys in the Console or the API. An administrator does not need to create a policy to give a user those abilities. Administrators (or anyone with permission to the tenancy) also have the ability to manage Customer Secret keys for other users.

Any user of the Amazon S3 Compatibility API with Object Storage needs permission to work with the service. If you're not sure if you have permission, contact your administrator. For information about policies, see How Policies Work on page 2136. For basic policies that enable use of Object Storage, see Common Policies on page 2142.

Customer Secret keys do not expire. Each user can have up to two Customer Secret keys at a time. To create keys using the Console, see To create a Customer Secret key on page 2464.

Working with OAuth 2.0 Client Credentials

Note:

OAuth 2.0 Client Credentials are not available in the United Kingdom Government Cloud (OC4).

OAuth 2.0 client credentials are required to interact programmatically with those services that use the OAuth 2.0 authorization protocol. The credentials enable you to obtain a secure token to access those service REST API endpoints. The allowed actions and endpoints granted by the token depend on the scopes (permissions) that you select when you generate the credentials. The services that use the OAuth 2.0 protocol are:

- Oracle Analytics Cloud
- Oracle Integration

An OAuth 2.0 access token is valid for 3600 seconds (1 hour).

To create the credentials, you need to know the service resource and scope. Typically, you can select these from a drop-down list. However, if the information is not available in the list, you can manually enter the resource and scope. The scope defines the allowed permissions for the token, so ensure to set the scope at the minimum required access level.
A user can create the credentials for themselves or an Administrator can create the credentials for another user. The lists of available resources and scopes display only those resources and permission levels that the user has been granted access to.

**OAuth 2.0 Client Credential Limits**

Each user can have up to 10 OAuth 2.0 client credentials. You can increase this limit by [Requesting a Service Limit Increase](#) on page 217.

Each OAuth 2.0 client credential can have up to 10 scopes.

**Obtaining an OAuth 2.0 Access Token**

To obtain the token, use your credentials in a request against the OAuth2 token service endpoint as follows:

1. Create the OAuth 2.0 client credentials. See [To create OAuth 2.0 client credentials](#) on page 2465.

   After you create the OAuth 2.0 client credential note the following information:
   - The generated secret
   - The OCID of the OAuth 2.0 client credential
   - The scope and audience (fully-qualified scope)

2. Using the information from the previous step, make a request against the /oauth2/token endpoint to obtain a token as follows:

   ```bash
   curl -k -X POST -H "Content-Type: application/x-www-form-urlencoded; charset=UTF-8" --user '<Oauth 2.0 client credential OCID>:<credential secret>' https://auth.<oci_region>.oraclecloud.com/oauth2/token -d 'grant_type=client_credentials&scope=<audience>-<scope>'
   ```

   Where:
   - `<Oauth 2.0 client credential OCID>:<credential secret>` is the OCID of the OAuth 2.0 client credential that you created joined by a colon (:) with the generated secret for the credential. Note that this secret is only displayed at the time you generate it and it must be copied immediately. You can retrieve the OCID from the details of the credential at any time.
   - `https://auth.<oci_region>.oraclecloud.com/oauth2/token` is the Oracle Cloud Infrastructure OAuth 2.0 authorization endpoint where `<OCI_region>` is a region your tenancy is subscribed to. For example, us-ashburn-1.
   - `<scope>-<audience>` is the fully-qualified scope, that is, the scope and audience joined by a hyphen (-). The scope and audience are available from the details page of the credential.

   **Example request:**
   ```bash
   curl -k -X POST -H "Content-Type: application/x-www-form-urlencoded; charset=UTF-8" --user 'ocid1.credential.region1..aaaaaexamplestringaapgpedxq:{SAMplESeCreta5y' https://auth.us-ashburn-1.oraclecloud.com/oauth2/token -d 'grant_type=client_credentials&scope=https://2aexampley3uytc.analytics.ocp.oraclecloud.com:urn:opc:resource:consumer::all'
   ```

   The response will include the token. Example response:
   ```json
   {
   "access_token": "eyJraWQiOiJhcDVfwqKdi...8I7ILrzcz4cof2A",
   "token_type": "Bearer",
   "expires_in": "3600"
   }
   ```

   The token string is truncated in the example response. Copy the entire `access_token` string (within the quotation marks) as shown in your response.
Using the OAuth 2.0 Token in a Request

After you obtain an OAuth 2.0 access token, you provide the token in a bearer token header of the REST API request. For example:

```
```

What to Do When the Token Expires

The token expires after 3600 seconds (1 hour). When the token expires, request a new token following the instructions in Obtaining an OAuth 2.0 Access Token on page 2458.

Adding Scopes

You can add scopes to an existing OAuth 2.0 client credential to add access to more services with the same credential. After you add scopes, you do not need to regenerate the secret.

To request a token for multiple scopes, You can include additional scopes in a token request by appending

```
&scope=<scope>-<<audience>
```

to the final argument of the request and specifying the scope and audience for the scope you want to add.

Working with SMTP Credentials

Simple Mail Transfer Protocol (SMTP) credentials are needed in order to send email through the Email Delivery service. Each user is limited to a maximum of two SMTP credentials. If more than two are required, they must be generated on other existing users or additional users must be created.

**Note:**

You cannot change your SMTP username or password to a string of your own choice. The credentials are always Oracle-generated strings.

Each user created in the IAM service automatically has the ability to create and delete their own SMTP credentials in the Console or the API. An administrator does not need to create a policy to give a user those abilities. Administrators (or anyone with permission to the tenancy) also have the ability to manage SMTP credentials for other users.

**Tip:**

Although each user can create and delete their own credentials, it is a security best practice to create a new user and generate SMTP credentials on this user rather than generating SMTP credentials on your Console user that already has permissions assigned to it.

SMTP credentials do not expire. Each user can have up to two credentials at a time. To get SMTP credentials in the Console, see To generate SMTP credentials on page 2466.

For information about using the Email Delivery service, see Overview of the Email Delivery Service on page 1738.

Using the Console

To change your Console password

You're prompted to change your initial one-time password the first time you sign in to the Console. The following procedure is for changing your password again later.

**Note:**

For Federated Users
If your company uses an identity provider (other than Oracle Identity Cloud Service) to manage user logins and passwords, you can't use the Console to update your password. You do that with your identity provider.

1. Sign in to the Console using the Oracle Cloud Infrastructure Username and Password.
2. After you sign in, go to the top-right corner of the Console, open the **Profile** menu (👤) and then click **Change Password**.

![Change Password](image)

3. Enter the current password.
4. Follow the prompts to enter the new password, and then click **Save New Password**.

**To create or reset another user's Console password**

If you're an administrator, you can use the following procedure to create or reset a user's password. The procedure generates a new one-time password that the user must change the next time they sign in to the Console.

1. View the user's details: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.
2. Click **Create/Reset Password**.

   The new one-time password is displayed. If you're an administrator performing the task for another user, you need to securely deliver the new password to the user. The user will be prompted to change their password the next time they sign in to the Console. If they don't change it within 7 days, the password will expire and you'll need to create a new one-time password for the user.

**To reset your password if you forgot it**

If you have an email address in your user profile, you can use the **Forgot Password** link on the sign on page to have a temporary password sent to you. If you don't have an email address in your user profile, you must ask an administrator to reset your password for you.

**To unblock a user**

If you're an administrator, you can unblock a user who has tried 10 times in a row to sign in to the Console unsuccessfully. See **To unblock a user** on page 2460.
To add an API signing key

You can use the Console to generate the private/public key pair for you. If you already have a key pair, you can choose to upload the public key. When you use the Console to add the key pair, the Console also generates a configuration file preview snippet for you.

The following procedures work for a regular user or an administrator. Administrators can manage API keys for either another user or themselves.

About the Config File Snippet

When you use the Console to add the API signing key pair, a configuration file preview snippet is generated with the following information:

- **user** - the OCID of the user for whom the key pair is being added.
- **fingerprint** - the fingerprint of the key that was just added.
- **tenancy** - your tenancy's OCID.
- **region** - the currently selected region in the Console.
- **key_file** - the path to your downloaded private key file. You must update this value to the path on your file system where you saved the private key file.

If your config file already has a DEFAULT profile, you'll need to do one of the following:

- Replace the existing profile and its contents.
- Rename the existing profile.
- Rename this profile to a different name after pasting it into the config file.

You can copy this snippet into your config file, to help you get started. If you don't already have a config file, see SDK and CLI Configuration File on page 4184 for details on how to create one. You can also retrieve the config file snippet later for an API signing key whenever you need it. See: To get the config file snippet for an API signing key.

To generate an API signing key pair

**Prerequisite:** Before you generate a key pair, create the .oci directory in your home directory to store the credentials. See SDK and CLI Configuration File on page 4184 for more details.

1. **View the user's details:**
   - If you're adding an API key for **yourself:**
     
     Open the Profile menu and click User Settings.
   - If you're an administrator adding an API key for **another user:** Go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. **Click Add API Key.**

3. **In the dialog, select Generate API Key Pair.**

4. **Click Download Private Key** and save the key to your .oci directory. In most cases, you do not need to download the public key.

   **Note:** If your browser downloads the private key to a different directory, be sure to move it to your .oci directory.

5. **Click Add.**

   The key is added and the Configuration File Preview is displayed. The file snippet includes required parameters and values you'll need to create your configuration file. Copy and paste the configuration file snippet from the text.
box into your ~/.oci/config file. (If you have not yet created this file, see SDK and CLI Configuration File on page 4184 for details on how to create one.)

After you paste the file contents, you'll need to update the key_file parameter to the location where you saved your private key file.

If your config file already has a DEFAULT profile, you'll need to do one of the following:

• Replace the existing profile and its contents.
• Rename the existing profile.
• Rename this profile to a different name after pasting it into the config file.

6. Update the permissions on your downloaded private key file so that only you can view it:

a. Go to the .oci directory where you placed the private key file.

b. Use the command chmod go-rwx ~/.oci/<oci_api_keyfile>.pem to set the permissions on the file.

To upload or paste an API key

Prerequisite: You have generated a public RSA key in PEM format (minimum 2048 bits). The PEM format looks something like this:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoTFqF...
....
-----END PUBLIC KEY-----
```

1. View the user's details:

   • If you're adding an API key for yourself:

   Open the Profile menu ( ) and click User Settings.

   • If you're an administrator adding an API key for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. Click Add API Key.

3. In the dialog, select Choose Public Key File to upload your file, or Paste Public Key, if you prefer to paste it into a text box

4. Click Add.

   The key is added and the Configuration File Preview is displayed. The file snippet includes required parameters and values you'll need to create your configuration file. Copy and paste the configuration file snippet from the text box into your ~/.oci/config file. (If you have not yet created this file, see SDK and CLI Configuration File on page 4184 for details on how to create one.)

   After you paste the file contents, you'll need to update the key_file parameter to the location where you saved your private key file.

   If your config file already has a DEFAULT profile, you'll need to do one of the following:

   • Replace the existing profile and its contents.
   • Rename the existing profile.
   • Rename this profile to a different name after pasting it into the config file.

   To get the config file snippet for an API signing key

   The following procedure works for a regular user or an administrator.
1. View the user's details:
   - If you're getting an API key config file snippet for yourself:
     Open the Profile menu (🔗) and click User Settings.
     If you're an administrator getting an API key config file snippet for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.
   - If you're an administrator getting an API key config file snippet for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.
2. On the left side of the page, click API Keys. The list of API key fingerprints is displayed.
3. Click the the Actions icon (three dots) for the fingerprint, and select View configuration file.
   The Configuration File Preview is displayed. The file snippet includes required parameters and values you'll need to create your configuration file. Copy and paste the configuration file snippet from the text box into your ~/.oci/config file. (If you have not yet created this file, see SDK and CLI Configuration File on page 4184 for details on how to create one.) After you paste the file contents, you'll need to update the key_file parameter to the location where you saved your private key file.
   If your config file already has a DEFAULT profile, you'll need to do one of the following:
   - Replace the existing profile and its contents.
   - Rename the existing profile.
   - Rename this profile to a different name after pasting it into the config file.

To delete an API signing key
The following procedure works for a regular user or an administrator. Administrators can delete an API key for either another user or themselves.
1. View the user's details:
   - If you're deleting an API key for yourself:
     Open the Profile menu (🔗) and click User Settings.
   - If you're an administrator deleting an API key for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.
2. For the API key you want to delete, click Delete.
3. Confirm when prompted.
The API key is no longer valid for sending API requests.

To create an auth token
1. View the user's details:
   - If you're creating an auth token for yourself:
     Open the Profile menu (🔗) and click User Settings.
     If you're an administrator creating an auth token for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.
2. On the left side of the page, click Auth Tokens.
3. Click Generate Token.
4. Enter a description that indicates what this token is for, for example, "Swift password token".
5. Click Generate Token.
The new token string is displayed.
6. Copy the token string immediately, because you can't retrieve it again after closing the dialog box.
   If you're an administrator creating an auth token for another user, you need to securely deliver it to the user by providing it verbally, printing it out, or sending it through a secure email service.
To delete an auth token

The following procedure works for a regular user or an administrator. Administrators can delete an auth token for either another user or themselves.

1. View the user's details:
   • If you're deleting an auth token for yourself:
     Open the Profile menu () and click User Settings.
   • If you're an administrator deleting an auth token for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click Auth Tokens.
3. For the auth token you want to delete, click Delete.
4. Confirm when prompted.

The auth token is no longer valid for accessing third-party APIs.

To create a Customer Secret key

1. View the user's details:
   • If you're creating a Customer Secret key for yourself:
     Open the Profile menu () and click User Settings.
   • If you're an administrator creating a Customer Secret key for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click Customer Secret Keys.

   A Customer Secret key consists of an Access Key/Secret key pair. Oracle automatically generates the Access Key when you or your administrator generates the Secret Key to create the Customer Secret key.

3. Click Generate Secret Key.
4. Enter a friendly description for the key and click Generate Secret Key.
   The generated Secret Key is displayed in the Generate Secret Key dialog box. At the same time, Oracle generates the Access Key that is paired with the Secret Key. The newly generated Customer Secret key is added to the list of Customer Secret Keys.
5. Copy the Secret Key immediately, because you can't retrieve the Secret Key again after closing the dialog box for security reasons.
   If you're an administrator creating a Secret Key for another user, you need to securely deliver it to the user by providing it verbally, printing it out, or sending it through a secure email service.
6. Click Close.
7. To show or copy the Access Key, click the Show or Copy action to the left of the Name of a particular Customer Secret key.

To delete a Customer Secret key

The following procedure works for a regular user or an administrator. Administrators can delete a Customer Secret key for either another user or themselves.

1. View the user's details:
   • If you're deleting a Customer Secret key for yourself:
     Open the Profile menu () and click User Settings.
   • If you're an administrator deleting a Customer Secret key for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.
2. On the left side of the page, click **Customer Secret Keys**.
3. For the Customer Secret key you want to delete, click **Delete**.
4. Confirm when prompted.

The Customer Secret key is no longer available to use with the Amazon S3 Compatibility API.

**To create OAuth 2.0 client credentials**

<table>
<thead>
<tr>
<th>Note:</th>
<th>OAuth 2.0 Client Credentials are not available in the following realms:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• the commercial realm (OC1)</td>
</tr>
<tr>
<td></td>
<td>• the United Kingdom Government Cloud (OC4)</td>
</tr>
</tbody>
</table>

1. View the user's details:
   - If you're creating an OAuth 2.0 client credential for yourself:
     a. Open the **Profile** menu and click **User Settings**.
   - If you're an administrator creating an OAuth 2.0 client credential for another user: Open the navigation menu.
     a. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click **OAuth 2.0 Client Credentials**.
3. Click **Generate OAuth 2.0 Client Credential**.
4. Enter a **Name** and **Description** for this credential.
5. Add the URI for the OAuth 2.0 services that this credential will provide access to.

   **To Select a Resource-Scope Pair**
   a. Select the **Select a Resource-Scope Pair** option.
   b. The **Resource** list displays the resources you have permission to view. Select the resource you want to add credentials for. After you select the resource, the **Audience** field is automatically populated.
   c. Next, select the **Scope** for this credential. Always select the minimum required privileges.

   **To Enter Fully Qualified Scope:**
   a. Select the **Enter Fully Qualified Scope** option.
   b. Enter the **Audience** and **Scope** for this credential.
6. To add more permissions to this credential, click **+ Another Scope** and follow the instructions in the previous step.
7. Click **Generate**. The new secret string is generated.

   Copy the token string immediately, because you can't retrieve it again after closing the dialog box.

   If you're an administrator creating a Secret Key for another user, you need to securely deliver it to the user.

   You will need the following information from the credential for the token request:
   - The generated secret
   - The OCID of the OAuth 2.0 client credential
   - The scope and audience (fully-qualified scope)

**To add scopes to an existing OAuth 2.0 client credential**

1. View the user's details:
   - If you're creating an OAuth 2.0 client credential for yourself:
     a. Open the **Profile** menu and click **User Settings**.
   - If you're an administrator creating an OAuth 2.0 client credential for another user: Open the navigation menu.
     a. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.
2. On the left side of the page, click **OAuth 2.0 Client Credentials**.
3. Click the name of the credential that you want to add scopes to.
4. Click **Add Scopes**.
5. Add the URI for the OAuth 2.0 services that you want to add access to.

   **To Select a Resource-Scope Pair**
   
   a. Select the **Select a Resource-Scope Pair** option.
   
   b. The **Resource** list displays the resources you have permission to view. Select the resource you want to add credentials for. After you select the resource, the **Audience** field is automatically populated.
   
   c. Next, select the **Scope** for this credential. Always select the minimum required privileges.

   **To Enter Fully Qualified Scope**:
   
   a. Select the **Enter Fully Qualified Scope** option.
   
   b. Enter the **Audience** and **Scope** for this credential.

   6. To add more permissions to this credential, click **+ Another Scope** and follow the instructions in the previous step.

   7. Click **Save Changes**.

**To regenerate the OAuth 2.0 client credential secret**

**IMPORTANT:** When you regenerate the secret for a credential, requests made with the previous secret will be denied access to target scopes.

1. View the user's details:
   
   • If you're creating an OAuth 2.0 client credential for yourself:
   
      Open the **Profile** menu ( ) and click **User Settings**.
   
   • If you're an administrator creating an OAuth 2.0 client credential for another user: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click **OAuth 2.0 Client Credentials**.

3. Click the name of the credential that you want to regenerate the secret for.

4. Click **Add Scopes**.

5. Click **Regenerate Secret**.

6. Acknowledge the warning dialog and click **Regenerate Secret**.

7. Copy the token string immediately, because you can't retrieve it again after closing the dialog box.

Ensure to update existing token requests with the new secret string.

**To generate SMTP credentials**

1. View the user's details:
   
   • If you're generating SMTP credentials for yourself:
   
      Open the **Profile** menu ( ) and click **User Settings**.
   
   • If you're an administrator generating SMTP credentials for another user: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. Click **SMTP Credentials**.

3. Click **Generate SMTP Credentials**.

4. Enter a **Description** of the SMTP Credentials in the dialog box.

5. Click **Generate SMTP Credentials**. A user name and password is displayed.
6. Copy the user name and password for your records and click Close. Copy the credentials immediately, because you can't retrieve the password again after closing the dialog box for security reasons.

If you're an administrator creating the credential set for another user, you need to securely deliver it to the user by providing it verbally, printing it out, or sending it through a secure email service.

To delete SMTP credentials

The following procedure works for a regular user or an administrator. Administrators can delete SMTP credentials for either another user or themselves.

1. View the user's details:
   • If you're deleting SMTP credentials for yourself:
     Open the Profile menu ( ) and click User Settings.
   • If you're an administrator deleting SMTP credentials for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click SMTP Credentials.

3. For the SMTP credentials you want to delete, click Delete.

4. Confirm when prompted.

The SMTP credentials are no longer available to use with the Email Delivery service.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to manage Console passwords and access:

- CreateOrResetUIPassword: This generates a new one-time Console password for the user. The next time the user signs in to the Console, they'll be prompted to change the password.
- UpdateUserState: Unblocks a user who has tried to sign in 10 times in a row unsuccessfully.

Use these API operations to manage API signing keys:

- ListApiKeys
- UploadApiKey
- DeleteApiKey

Use these API operations to manage auth tokens:

- CreateAuthToken
- UpdateAuthToken: You can only update the auth token's description, not change the token string itself.
- ListAuthTokens
- DeleteAuthToken

Use these API operations to manage Customer Secret keys:

- CreateCustomerSecretKey
- UpdateCustomerSecretKey: You can only update the secret key's description, not change the key itself.
- ListCustomerSecretKeys
- DeleteCustomerSecretKey

Use these API operations to manage OAuth 2.0 client credentials:

- CreateOAuthClientCredential
- UpdateOAuthClientCredential
- ListOAuthClientCredentials
- DeleteOAuthClientCredential
Use these API operations to manage SMTP credentials:

- CreateSmtpCredential
- UpdateSmtpCredential: You can only update the description.
- ListSmtpCredentials
- DeleteSmtpCredential

Managing Authentication Settings

This topic describes how to set authentication rules for your tenancy. Authentication settings include policy rules for local IAM users in your tenancy and network source restrictions for all users in your tenancy.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for authentication policy and network sources.

To view authentication policy and network sources, you must be granted `inspect` access on the `authentication-policies` resource and the `network-sources` resource. For example:

```
Allow group GroupA to inspect authentication-policies in tenancy
```

```
Allow group GroupA to inspect network-sources in tenancy
```

To manage authentication policy and network sources, you must be granted `manage` permissions for both resources. For example:

```
Allow group GroupA to manage authentication-policies in tenancy
```

```
Allow group GroupA to manage network-sources in tenancy
```

If you're new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see [Details for IAM](#) on page 2280.

**Working with Password Policy Rules**

A password policy that you set in the IAM service is applicable for all local (or non-federated) users.

When a user is created or when a user changes their password, the IAM service validates the password that is provided against the password policy to ensure that it meets the criteria for the policy. When a user logs in for the first time to change the password, or resets the password at any time, the password policy is evaluated and enforced.

**When Do Changes to Password Policy Rules Take Effect**

Changes to password policy rules take effect immediately so that the next time any user changes their password they must create a password that meets the criteria. Existing passwords will continue to work even if they would be invalid under the new rules. Users are not forced to change existing passwords to meet the new criteria. Passwords are evaluated against the rules only at the time they are created or changed.

**About the Password Policy Rules**

The following table describes the rules that you can include in your password policy:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Setting Options</th>
<th>Default IAM Service Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>Minimum value is 8 (characters). Maximum value is 100.</td>
<td>12 characters</td>
</tr>
<tr>
<td>Rule</td>
<td>Setting Options</td>
<td>Default IAM Service Setting</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Special characters</strong></td>
<td>Require passwords to contain at least 1 special character. Special characters allowed in passwords are: !#$%&amp;'()*+,-./:;&lt;&gt;? @{}^`{}~ Special characters not listed are not allowed.</td>
<td>Enforced</td>
</tr>
<tr>
<td><strong>Lowercase characters</strong></td>
<td>Require passwords to contain at least 1 lowercase alphabetic character a-z.</td>
<td>Enforced</td>
</tr>
<tr>
<td><strong>Uppercase characters</strong></td>
<td>Require passwords to contain at least 1 uppercase alphabetic character A-Z.</td>
<td>Enforced</td>
</tr>
<tr>
<td><strong>Numeric characters</strong></td>
<td>Require passwords to contain at least 1 number 0-9.</td>
<td>Enforced</td>
</tr>
</tbody>
</table>

Oracle recommends that you enforce all the password rules.

**Using the Console to Manage Password Policy Rules**

To edit password policy rules

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Authentication Settings. The authentication settings for your tenancy are displayed.
2. Click Edit.
3. Enter the following to set the password policy:
   - **Minimum Password Length**: Enter a number to define the minimum number of characters that a user's password must contain. Allowed values are 8 through 100.
4. Select the Password Rules you want to enforce:
   - **Must contain at least 1 numeric character**: Select the check box to require at least 1 number (0-9) in the password.
   - **Must contain at least 1 special character**: Select the check box to require at least 1 special character. Allowed special characters are: !#$%&'()\*+,-./:;<>? @\{\}^`{\}\~
   - **Must contain at least 1 lowercase character**: Select the check box to require at least 1 lowercase alphabetic character (a-z).
   - **Must contain at least 1 uppercase character**: Select the check box to require at least 1 uppercase alphabetic character (A-Z).
5. Click Save Changes.

**Working with Network Source Restrictions in Authentication Policy**

Network source restrictions let you specify an allowed set of IP ranges from which users can sign in to the Console. Users attempting to sign in from an IP address not on the allowed list will be denied access.

To enforce a network source restriction for your tenancy:

1. Set up a network source that specifies the allowed IP addresses. See Managing Network Sources on page 2427 for information on setting up the network source.
2. Select the network source in the Authentication settings page.

An administrator can set only one network source in the authentication settings, but a single network source can include multiple allowed IP addresses.
A network source restriction is applied for every user in the tenancy. If an administrator is unable to access a network with an allowed IP address to sign in from, then they must do one of the following to gain access to the tenancy:

- Use the authentication SDK to sign in and change the network source restriction setting programmatically.
- Contact Oracle Support. If you do not have an API signing key to enable access through the authentication SDK, then you must contact support to regain access to your tenancy.

**Caution:**
Before you set up a network source restriction, ensure that you have an API key set up to enable access to your tenancy in case an allowed network is not available. If you do not set up an API key and an allowed network is not available, then all users will be locked out of the tenancy until you contact Oracle Support. For information about setting up the API signing key, see Required Keys and OCIDs on page 4179.

**When Do Changes to Network Source Restrictions Take Effect**

After a network source restriction is defined, users signed in to the Console can continue with their current session, but after they sign out, the network restriction will be applied the next time they try to sign in.

**Using the Console to Manage Network Source Restrictions**

**To set up a network source restriction**

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Authentication Settings. The authentication settings for your tenancy are displayed.
2. Click Edit.
3. From the Select Network Source menu, select the network source that specifies the IP range restrictions you want to apply to all Console sign-ins.
4. Click Save Changes.

**To view or edit the value of a network source**

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Authentication Settings. The authentication settings for your tenancy are displayed.
2. Click the name of the network source displayed for Network Source Restrictions.

   The details page of the network source is displayed. From here, you can edit or delete the definition. See Managing Network Sources on page 2427 for information on managing network sources.

**Using the API to Work with Authentication Settings**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage authentication settings:

- GetAuthenticationPolicy
- UpdateAuthenticationPolicy

**Managing Multi-Factor Authentication**

This topic describes how users can manage multi-factor authentication (MFA) in Oracle Cloud Infrastructure.

**Required IAM Policy**

Only the user can enable multi-factor authentication (MFA) for their own account. Users can also disable MFA for their own accounts. Members of the Administrators group can disable MFA for other users, but they cannot enable MFA for another user.
About Multi-Factor Authentication

Multi-factor authentication is a method of authentication that requires the use of more than one factor to verify a user’s identity.

With MFA enabled in the IAM service, when a user signs in to Oracle Cloud Infrastructure, they are prompted for their user name and password, which is the first factor (something that they know). The user is then prompted to provide a second verification code from a registered MFA device, which is the second factor (something that they have). The two factors work together, requiring an extra layer of security to verify the user’s identity and complete the sign-in process.

In general, MFA may include any two of the following:

- Something that you know, like a password.
- Something that you have, like a device.
- Something that you are, like your fingerprint.

The IAM service supports two-factor authentication using a password (first factor) and a device that can generate a time-based one-time password (TOTP) (second factor).

General Concepts

Here's a list of the basic concepts you need to be familiar with.

MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user’s identity. Examples of authentication factors are a password (something you know) and a device (something you have).

AUTHENTICATOR APP

An app you install on your mobile device that can provide software-based secure tokens for identity verification. Examples of authenticator apps are Oracle Mobile Authenticator and Google Authenticator. To enable MFA for the IAM service, you'll need a device with an authenticator app installed. You'll use the app to register your device and then you'll use the same app (on the same device) to generate a time-based one-time passcode every time you sign in.

REGISTERED MOBILE DEVICE

Multi-factor authentication is enabled for a specific user and for a specific device. The procedure to enable MFA for a user includes the registration of the mobile device. This same device must be used to generate the time-based one-time passcode every time the user signs in. If the registered mobile device becomes unavailable, an administrator must disable MFA for the user so that MFA can be re-enabled with a new device.

TIME-BASED ONE-TIME PASSWORD (TOTP)

A TOTP is a password (or passcode) that is generated by an algorithm that computes a one-time password from a shared secret key and the current time, as defined in RFC 6238. The authenticator app on your registered mobile device generates the TOTP that you need to enter every time you sign in to Oracle Cloud Infrastructure.

Supported Authenticator Apps

The following authenticator apps have been tested with the Oracle Cloud Infrastructure IAM service:

- Oracle Mobile Authenticator
- Google Authenticator

You can find these apps in your mobile device's app store. You must install one of these apps on your mobile device before you can enable MFA.
Working with MFA

Keep the following in mind when you enable MFA:

• You must install a supported authenticator app on the mobile device you intend to register for MFA.
• Each user must enable MFA for themselves using a device they will have access to every time they sign in. An administrator cannot enable MFA for another user.
• To enable MFA, you use your mobile device’s authenticator app to scan a QR code that is generated by the IAM service and displayed in the Console. The QR code shares a secret key with the app to enable the app to generate TOTPs that can be verified by the IAM service.
• A user can register only one device to use for MFA.
• After you add your Oracle Cloud Infrastructure account to your authenticator app, the account name displays in the authenticator app as Oracle <tenancy_name> - <username>.

Restricting Access to Only MFA-Verified Users

You can restrict access to resources to only users that have been authenticated through the IAM service’s time-based one-time password authentication. You set up this restriction in the policy that allows access to the resource.

To restrict the access granted through a policy to only MFA-verified users, add the following where clause to the policy:

```plaintext
where request.user.mfaTotpVerified='true'
```

For example, assume your company has this policy in place to allow GroupA to manage instances:

```plaintext
allow group GroupA to manage instance-family in tenancy
```

To enhance security, you want to ensure that only users who have been verified through MFA can manage instances. To restrict access to only these users, revise the policy statement as follows:

```plaintext
allow group GroupA to manage instance-family in tenancy where request.user.mfaTotpVerified='true'
```

With this policy in place, only the members of GroupA who have successfully signed in by entering both their password and the time-based one-time passcode generated by their registered mobile device, are allowed to access and manage instances. Users who have not enabled MFA and sign in using only their password, will not be allowed access to manage instances.

For information on writing policies, see Policy Syntax on page 2164.

Sign in Process After Enabling MFA

After you have enabled MFA, use one of the following procedures to sign in to Oracle Cloud Infrastructure:

To sign in using the Console

1. Navigate to the Console sign-in page.
2. Enter your Oracle Cloud Infrastructure **User Name** and **Password** and then click **Sign In**.

After your user name and password are authenticated, you have successfully supplied the first factor for authentication. The secondary authentication page displays and prompts you to enter a one-time passcode, as shown in the following screenshot.

![Multi-Factor Authentication](image)

3. Open the authenticator app on your registered mobile device and then open the account for your Oracle Cloud Infrastructure tenancy. The following screenshot shows an example from Oracle Mobile Authenticator.

![Authenticator App Screenshot](image)

4. Enter the passcode displayed by your authenticator app (for example, 219604) and then click **Sign In**.

**Important:** The authenticator app generates a new time-based one-time passcode every 30 seconds. You must enter a code while the code is still valid. If you miss the time window for one passcode, you can enter the next one that is generated. Just ensure that you enter the code that is currently displayed by your app.

**To sign in using the command line interface (CLI)**

1. To sign in with the CLI, run the following command:

   ```sh
ci session authenticate --region US East (Ashburn)
   ```

   A browser window opens, and a prompt instructs you to use the browser to sign in.

   ```
   Please switch to newly opened browser window to log in!
   ```
2. In the browser window, enter your Oracle Cloud Infrastructure **User Name** and **Password** and then click **Sign In**.

After your user name and password are authenticated, you have successfully supplied the first factor for authentication. The secondary authentication page displays and prompts you to enter a one-time passcode, as shown in the following screenshot.

![Multi-Factor Authentication](image)

3. Open the authenticator app on your registered mobile device and then open the account for your Oracle Cloud Infrastructure tenancy. The following screenshot shows an example from Oracle Mobile Authenticator.

![Authenticator App Example](image)

4. Enter the passcode displayed by your authenticator app (for example, 219604) and then click **Sign In**.

**Important:** The authenticator app generates a new time-based one-time passcode every 30 seconds. You must enter a code while the code is still valid. If you miss the time window for one passcode, you can enter the next one that is generated. Just ensure that you enter the code that is currently displayed by your app.

After you authenticate, prompts instruct you to return to the CLI and enter the name of a profile.

5. In the CLI, type a name for the profile.

**Tip:**

For more information about working with the CLI, see **Quickstart** on page 4195 and **Getting Started with the Command Line Interface** on page 83.
IAM

What To Do If You Lose Your Registered Mobile Device
If you lose your registered mobile device, you will not be able to authenticate to Oracle Cloud Infrastructure through the Console. Contact your administrator to disable multi-factor authentication for your account. You can then repeat the process to enable multi-factor authentication with a new mobile device.

Unblocking a User After Unsuccessful Sign-in Attempts
If a user tries 10 times in a row to sign in to the Console unsuccessfully, they will be automatically blocked from further sign-in attempts. An administrator can unblock the user in the Console (see To unblock a user on page 2418) or with the UpdateUserState API operation.

Disabling MFA
Each user can disable MFA for themselves. An administrator can also disable MFA for another user.

Caution:
Do not disable MFA unless you are instructed to by your administrator.

Using the Console
Use the following procedures to manage MFA in the Console.

To enable MFA for your user account
Prerequisite: You must install a supported authenticator app on the mobile device you intend to register for MFA.

1. In the upper-right corner of the Console, open the Profile menu and then select User Settings. Your user details are displayed.
2. Click Enable Multi-Factor Authentication.
3. Scan the QR code displayed in the dialog with your mobile device’s authenticator app.
   Note: If you close the browser, or if the browser crashes before you can enter the verification code, you must generate a new QR code and scan it again with your app. To generate a new QR code, click the Enable Multi-Factor Authentication button again.
4. In the Verification Code field, enter the code displayed on your authenticator app.
5. Click Enable.

Your mobile device is now registered with the IAM service and your account is enabled for MFA. Every time you sign in, you are prompted for your username and password first. After you provide the correct credentials, you will be prompted for a TOTP code generated by the authenticator app on your registered mobile device. You must have your registered mobile device available every time you sign in to Oracle Cloud Infrastructure.

To disable MFA for your user account

1. In the upper-right corner of the Console, open the Profile menu and then select User Settings. Your user details are displayed.
2. Click Disable Multi-Factor Authentication.
3. Confirm when prompted.

To disable MFA for another user

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users. A list of the users in your tenancy is displayed.
2. Click the user you want to update. The user's details are displayed.
3. Click Disable Multi-Factor Authentication.
4. Confirm when prompted.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Note:

Updates Are Not Immediate Across All Regions

Your IAM resources reside in your home region. To enforce policy across all regions, the IAM service replicates your resources in each region. Whenever you create or change a policy, user, or group, the changes take effect first in the home region, and then are propagated out to your other regions. It can take several minutes for changes to take effect in all regions.

Use these API operations to manage multi-factor authentication devices:

- CreateMfaTotpDevice
- ListMfaTotpDevices
- GetMfaTotpDevice
- DeleteMfaTotpDevice
- ActivateMfaTotpDevice
- GenerateTotpSeed

Policies for Managing Resources Used with Resource Manager

This section provides example policies for managing the resources used with the Resource Manager service: stacks, jobs, private templates, and configuration source providers. For guidance using the syntax for creating policies, see Policy Syntax on page 2164.

Important:

Policies for managing Oracle Cloud Infrastructure resources are also required for Resource Manager operations that access resources. For example, running an apply job on a stack that includes Compute instances and subnets requires policies that grant you permissions for those resource types, in the compartments where you want to provision the resources. To see examples of policies for managing Oracle Cloud Infrastructure resources, see Common Policies on page 2142.

Stacks and jobs

The following example grants a specified group permission to manage both stacks and jobs in the tenancy, and also to manage Oracle Cloud Infrastructure resources on the tenancy stacks.

Allow group <group_name> to manage orm-stacks in tenancy
Allow group <group_name> to manage orm-jobs in tenancy

In addition to granting users permission to act on resources, you can also explicitly prevent users from running destroy jobs. The following policy modifies the policy we just created so that it prohibits members of the specified group from running destroy jobs.

Allow group <group_name> to use orm-stacks in tenancy
Allow group <group_name> to read orm-jobs in tenancy
Allow group <group_name> to manage orm-jobs in tenancy where any
{target.job.operation = 'PLAN', target.job.operation = 'APPLY'}

In this policy statement, you must include the new permission to read orm-jobs because the third statement includes a condition that uses variables that are not relevant to listing or getting jobs.
For more details about stack permissions, see `orm-stacks` on page 2338. For more details about job permissions, see `orm-jobs` on page 2338.

**Private templates**

The following example grants a specified group permission to create, update, move, and delete private templates in the tenancy.

```
Allow group <group_name> to manage orm-template in tenancy
```

The following example grants a specified group permission to create stacks from private templates, in addition to managing stacks and jobs.

```
Allow group <group_name> to manage orm-stacks in tenancy
Allow group <group_name> to manage orm-jobs in tenancy
Allow group <group_name> to read orm-templates in tenancy
```

For more details about private template permissions, see `orm-template` on page 2339.

**Configuration source providers**

The following example grants a specified group permission to create, update, move, and delete configuration source providers in the tenancy.

```
Allow group <group_name> to manage orm-config-source-providers in tenancy
```

The following example grants a specified group permission to create stacks from configuration files in source code control systems (using existing configuration source providers), in addition to managing stacks and jobs.

```
Allow group <group_name> to read orm-config-source-providers in tenancy
Allow group <group_name> to manage orm-stacks in tenancy
Allow group <group_name> to manage orm-jobs in tenancy
```

For more details about configuration source provider permissions, see `orm-config-source-providers` on page 2337.

**Deprecated IAM Service APIs**

This topic lists deprecated APIs for the IAM service.

**Federation Management APIs**

Date of Notification: October 15, 2020

**What is changing?**

The following APIs for the management of federations are deprecated. Support for these APIs will end **October 15, 2021**. The replacement solution for managing federations is to set up the federation for your tenancy between the identity provider and your tenancy’s Oracle Identity Cloud Service identity domain. See `Manage Oracle Identity Cloud Service Identity Providers` for information on managing identity providers in IDCS.

<table>
<thead>
<tr>
<th>Deprecated API</th>
<th>Replacement API in IDCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateIdentityProvider</td>
<td>Create an Identity Provider</td>
</tr>
<tr>
<td>ListIdentityProviders</td>
<td>Search Identity Providers</td>
</tr>
<tr>
<td>GetIdentityProvider</td>
<td>Get an Identity Provider</td>
</tr>
<tr>
<td>UpdateIdentityProvider</td>
<td>Update an Identity Provider</td>
</tr>
<tr>
<td>DeleteIdentityProvider</td>
<td>Delete an Identity Provider</td>
</tr>
<tr>
<td>Deprecated API</td>
<td>Replacement API in IDCS</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>ListIdentityProviderGroups</td>
<td>Search Identity Providers</td>
</tr>
<tr>
<td>CreateIdpGroupMapping</td>
<td>Not used in replacement solution.</td>
</tr>
<tr>
<td>ListIdpGroupMappings</td>
<td>Not used in replacement solution.</td>
</tr>
<tr>
<td>GetIdpGroupMapping</td>
<td>Not used in replacement solution.</td>
</tr>
<tr>
<td>UpdateIdpGroupMapping</td>
<td>Not used in replacement solution.</td>
</tr>
<tr>
<td>DeleteIdpGroupMapping</td>
<td>Not used in replacement solution.</td>
</tr>
</tbody>
</table>
Load Balancing

This chapter explains how to set up a load balancer.

Overview of Load Balancing

The Oracle Cloud Infrastructure Load Balancing service provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). The service offers a load balancer with your choice of a public or private IP address, and provisioned bandwidth.

A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability. You can configure multiple load balancing policies and application-specific health checks to ensure that the load balancer directs traffic only to healthy instances. The load balancer can reduce your maintenance window by draining traffic from an unhealthy application server before you remove it from service for maintenance.

How Load Balancing Works

The Load Balancing service enables you to create a public or private load balancer within your VCN. A public load balancer has a public IP address that is accessible from the internet. A private load balancer has an IP address from the hosting subnet, which is visible only within your VCN. You can configure multiple listeners for an IP address to load balance transport Layer 4 and Layer 7 (TCP and HTTP) traffic. Both public and private load balancers can route data traffic to any backend server that is reachable from the VCN.

Public Load Balancer

To accept traffic from the internet, you create a public load balancer. The service assigns it a public IP address that serves as the entry point for incoming traffic. You can associate the public IP address with a friendly DNS name through any DNS vendor.

A public load balancer is regional in scope. If your region includes multiple availability domains, a public load balancer requires either a regional subnet (recommended) or two availability domain-specific (AD-specific) subnets, each in a separate availability domain. With a regional subnet, the Load Balancing service creates a primary load balancer and a standby load balancer, each in a different availability domain, to ensure accessibility even during an availability domain outage. If you create a load balancer in two AD-specific subnets, one subnet hosts the primary load balancer and the other hosts a standby load balancer. If the primary load balancer fails, the public IP address switches to the secondary load balancer. The service treats the two load balancers as equivalent and you cannot specify which one is "primary".

Whether you use regional or AD-specific subnets, each load balancer requires one private IP address from its host subnet. The Load Balancing service supplies a floating public IP address to the primary load balancer. The floating public IP address does not come from your backend subnets.

If your region includes only one availability domain, the service requires just one subnet, either regional or AD-specific, to host both the primary and standby load balancers. The primary and standby load balancers each require
a private IP address from the host subnet, in addition to the assigned floating public IP address. If there is an availability domain outage, the load balancer has no failover.

| Caution: |
| You cannot specify a private subnet for your public load balancer. |

**Private Load Balancer**

To isolate your load balancer from the internet and simplify your security posture, you can create a private load balancer. The Load Balancing service assigns it a private IP address that serves as the entry point for incoming traffic.

When you create a private load balancer, the service requires only one subnet to host both the primary and standby load balancers. The load balancer can be regional or AD-specific, depending on the scope of the host subnet. The load balancer is accessible only from within the VCN that contains the host subnet, or as further restricted by your security rules.

The assigned floating private IP address is local to the host subnet. The primary and standby load balancers each require an extra private IP address from the host subnet.

If there is an availability domain outage, a private load balancer created in a regional subnet within a multi-AD region provides failover capability. A private load balancer created in an AD-specific subnet, or in a regional subnet within a single availability domain region, has no failover capability in response to an availability domain outage.

**All Load Balancers**

Your load balancer has a backend set to route incoming traffic to your Compute instances. The backend set is a logical entity that includes:

- A list of backend servers.
- A load balancing policy.
- A health check policy.
- Optional SSL handling.
- Optional session persistence configuration.

The backend servers (Compute instances) associated with a backend set can exist anywhere, as long as the associated network security groups (NSGs), security lists, and route tables allow the intended traffic flow.

If your VCN uses network security groups (NSGs), you can associate your load balancer with an NSG. An NSG has a set of security rules that controls allowed types of inbound and outbound traffic. The rules apply only to the resources in the group. Contrast NSGs with a security list, where the rules apply to all the resources in any subnet that uses the list. For more information about NSGs, see **Network Security Groups** on page 2841.

If you prefer to use security lists for your VCN, the Load Balancing service can suggest appropriate security list rules. You also can configure them yourself through the Networking service. See **Security Lists** on page 2850 for more information.

See **Security Rules** on page 2833 for detailed information comparing NSGs and security lists.

Oracle recommends that you create your load balancer in a regional subnet.

Oracle recommends that you distribute your backend servers across all availability domains within the region.

To create a minimal system with a functioning load balancer, you must:

- For a public load balancer, create a VCN with an internet gateway and a public regional subnet.

  | Caution: |
  | You cannot specify a private subnet for your public load balancer. |

  - For a private load balancer, create a VCN with at least one private subnet.
  - Create at least two Compute instances, each in a separate availability domain.
  - Create a load balancer.
- Create a backend set with a health check policy.
- Add backend servers (Compute instances) to the backend set.
- Create a listener, with optional SSL handling.
- Update the load balancer subnet security rules so they allow the intended traffic.

**Note:**

Private IP Address Consumption

A public load balancer created in one public subnet consumes two private IP addresses from the host subnet.

A public load balancer created in two public subnets consumes two private IP addresses, one from each host subnet.

A private load balancer created in a single subnet consumes three private IP addresses from the host subnet.

The following diagram provides a high-level view of a simple public load balancing system configuration. Far more sophisticated and complex configurations are common.
Load Balancing Concepts

The following concepts are essential to working with Load Balancing.

**BACKEND SERVER**

An application server responsible for generating content in reply to the incoming TCP or HTTP traffic. You typically identify application servers with a unique combination of overlay (private) IPv4 address and port, for example, 10.10.10.1:8080 and 10.10.10.2:8080.

For more information, see Managing Backend Servers on page 2515.

**BACKEND SET**

A logical entity defined by a list of backend servers, a load balancing policy, and a health check policy. SSL configuration is optional. The backend set determines how the load balancer directs traffic to the collection of backend servers.

For more information, see Managing Backend Sets on page 2510.

**CERTIFICATES**

If you use HTTPS or SSL for your listener, you must associate an SSL server certificate (X.509) with your load balancer. A certificate enables the load balancer to terminate the connection and decrypt incoming requests before passing them to the backend servers.

For more information, see Managing SSL Certificates on page 2551.

**health check**

A health check is a test to confirm the availability of backend servers. A health check can be a request or a connection attempt. Based on a time interval you specify, the load balancer applies the health check policy to continuously monitor backend servers. If a server fails the health check, the load balancer takes the server temporarily out of rotation. If the server subsequently passes the health check, the load balancer returns it to the rotation.

You configure your health check policy when you create a backend set. You can configure TCP-level or HTTP-level health checks for your backend servers.

- TCP-level health checks attempt to make a TCP connection with the backend servers and validate the response based on the connection status.
- HTTP-level health checks send requests to the backend servers at a specific URI and validate the response based on the status code or entity data (body) returned.

The service provides application-specific health check capabilities to help you increase availability and reduce your application maintenance window.

For more information on health check configuration, see Editing Health Check Policies on page 2558.

**HEALTH STATUS**

An indicator that reports the general health of your load balancers and their components.

For more information, see the Health Status section of Editing Health Check Policies.

**LISTENER**

A logical entity that checks for incoming traffic on the load balancer's IP address. You configure a listener's protocol and port number, and the optional SSL settings. To handle TCP, HTTP, and HTTPS traffic, you must configure multiple listeners.

Supported protocols include:

- TCP
- HTTP/1.0
- HTTP/1.1

For more information, see Managing Listeners on page 2522.
LOAD BALANCING POLICY

A load balancing policy tells the load balancer how to distribute incoming traffic to the backend servers. Common load balancer policies include:

- Round robin
- Least connections
- IP hash

For more information, see How Load Balancing Policies Work on page 2488.

PATH ROUTE SET

A set of path route rules to route traffic to the correct backend set without using multiple listeners or load balancers.

For more information, see Managing Request Routing on page 2534.

REGIONS AND availability domains

The Load Balancing service manages application traffic across availability domains within a region. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of several availability domains.

For more information, see Regions and Availability Domains on page 180.

SESSION PERSISTENCE

A method to direct all requests originating from a single logical client to a single backend web server.

For more information, see Session Persistence on page 2491.

shape

A template that determines the load balancer's total pre-provisioned maximum capacity (bandwidth) for ingress plus egress traffic. Available shapes include 10Mbps, 100 Mbps, 400 Mbps, and 8000 Mbps.

The 10Mbps shape is Always Free eligible. For more information about Always Free resources, including additional capabilities and limitations, see Oracle Cloud Infrastructure Free Tier on page 140.

Tip:

Pre-provisioned maximum capacity applies to aggregated connections, not to a single client attempting to use the full bandwidth.

SSL

Secure Sockets Layer (SSL) is a security technology for establishing an encrypted link between a client and a server. You can apply the following SSL configurations to your load balancer:

SSL TERMINATION

The load balancer handles incoming SSL traffic and passes the unencrypted request to a backend server.

END TO END SSL

The load balancer terminates the SSL connection with an incoming traffic client, and then initiates an SSL connection to a backend server.

SSL TUNNELING

If you configure the load balancer's listener for TCP traffic, the load balancer tunnels incoming SSL connections to your application servers.

Load Balancing supports the TLS 1.2 protocol with a default setting of strong cipher strength. The default supported ciphers include:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
Load Balancing

- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256

For more information, see Managing SSL Certificates on page 2551.

subnet

A subdivision you define in a VCN, such as 10.0.0.0/24 and 10.0.1.0/24. A subnet can span a region or exist within a single availability domain. A subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. For each subnet, you specify the routing and security rules that apply to it.

For more information on subnets, see VCNs and Subnets on page 2821 and Public IP Address Ranges on page 2754.

TAGS

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

VIRTUAL HOSTNAME

A virtual server name applied to a listener to enhance request routing.

For more information, see Managing Request Routing on page 2534.

VIRTUAL CLOUD NETWORK (VCN)

A private network that you set up in the Oracle data centers, with firewall rules and specific types of communication gateways that you can choose to use. A VCN covers a single, contiguous IPv4 CIDR block of your choice in the allowed IP address ranges.

You need at least one virtual cloud network before you launch a load balancer.

For information about setting up virtual cloud networks, see Networking Overview on page 2748.

VISIBILITY

Specifies whether your load balancer is public or private.

PUBLIC

A public load balancer has a public IP address that clients can access from the internet.

PRIVATE

A private load balancer has a private IP address from a VCN local subnet. Clients can access the private load balancer using methods and technology that can provide access to a private IP, such as:

- Cross-VCN (via LPG peering)
- From another region (via RPC)
- From on-prem (via FC private peering)
Load Balancing

For more information, see Managing Load Balancers on page 2494.

WORK REQUEST

An object that reports on the current state of a Load Balancing request.
The Load Balancing service handles requests asynchronously. Each request returns a work request ID (OCID) as the response. You can view the work request item to see the status of the request.
For more information, see Viewing the State of a Work Request on page 2565.

Troubleshooting an HTTP 502 Bad Gateway

Apart from proactive monitoring and management, load balancing logging will help you to identify, isolate, and troubleshoot issues with your load balancer infrastructure. In this example scenario, you are deploying a new web application, ociexample.com, with an Oracle Cloud Infrastructure public load balancer as the front end in your development environment. However, when you try to access the application, you see an HTTP 502 response on the browser. Use the following procedure to help you troubleshoot the issue by using LBaaS Access and Error Logs.

1. When you browse to a load-balanced IP address, you see 502 Bad Gateway error.
2. You can confirm this behavior by running a curl test:

   ```
curl -v http://ociexample.com
   > GET / HTTP/1.1
   > Host: 129.146.93.99
   > User-Agent: curl/7.54.0
   > Accept: */*
   >
   < HTTP/1.1 502 Bad Gateway
   < Content-Type: text/html
   < Content-Length: 161
   < Connection: keep-alive
   
   3. Use the OCI Logging Service Load Balancer Logs and check for lbStatusCode: "502".
   4. Check for

   ```

   ```
   backendStatusCode
   ```

   You will then correlate this status code with one of the following scenarios below.

502 from Backend

Possible causes

- Backend application is returning a 502
- Issue is misconfigured backend
- Backend is likely another reverse proxy or LB

504 from Backend

Possible resolutions

- Examine upstream proxy logs to determine why it is returning 502
- Resolve any issues on the ultimate backend that is causing the upstream proxy to return a 502

Possible causes

- When receiving a 504 from the Backend it typically means that the backend is another proxy or LBaaS instance. This code is typically returned when a proxy is unable to connect to an upstream server in a specified time.
- It is recommended to examine the logs of the upstream system and see what is causing that upstream proxy from connection to its backend.
Possible resolutions

- Increase the connection timeout.
- Determine why backend is taking longer time to respond than usual using a utility such as tcpdump, and built-in application tools.

**500 from Backend**

Possible causes

- Receiving a 500 from the backend is typically indicative of a server side error, commonly known as an "Internal Server Error". This typically is a result of the backend application.

Possible resolutions

- Resolve application level issue that is causing
- Common causes, inability to connect to upstream resources such as databases, APIs, services, etc.

**No Status Code from the Backend**

- You typically see no backend status code accompanied by a 502 lbStatusCode, when no Backend is available to send the connections.
- You will also notice "No healthy backends available in associated backendSet" in the OCI Logging Load Balancer Error Logs.
- It is recommended to ensure the backends are healthy, if they are healthy you will need to confirm that your health check is properly configured.

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

**Monitoring Resources**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring the traffic passing through your load balancer, see Load Balancing Metrics on page 2567.
Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Limits on Load Balancing Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

Other limits include:

• You cannot convert an AD-specific load balancer to a regional load balancer or the reverse.
• The Load Balancing services supports IPv6 addresses for load balancers in the US Government Cloud only. IPv6 support is only for the load balancer itself, and not the backend.
• The maximum number of concurrent connections is limited when you use stateful security rules for your load balancer subnets. In contrast, there is no theoretical limit on concurrent connections if you use stateless security rules. The practical limitations depend on various factors. The larger your load balancer shape, the greater the connection capacity. Other considerations include system memory, TCP timeout periods, TCP connection state, and so forth.

Tip:
To accommodate high-volume traffic, Oracle strongly recommends that you use stateless security rules for your load balancer subnets.

• Each load balancer has the following configuration limits:
  • One IP address
  • 16 backend sets
  • 512 backend servers per backend set
  • 1024 backend servers total
  • 16 listeners

How Load Balancing Policies Work

After you create a load balancer, you can apply policies to control traffic distribution to your backend servers. The Load Balancing service supports three primary policy types:

• Round Robin
• Least Connections
• IP Hash

When processing load or capacity varies among backend servers, you can refine each of these policy types with backend server weighting. Weighting affects the proportion of requests directed to each server. For example, a server weighted ‘3’ receives three times the number of connections as a server weighted ‘1’. You assign weights based on criteria of your choosing, such as each server’s traffic-handling capacity.

Load balancer policy decisions apply differently to TCP load balancers, cookie-based session persistent HTTP requests (sticky requests), and non-sticky HTTP requests.

• A TCP load balancer considers policy and weight criteria to direct an initial incoming request to a backend server. All subsequent packets on this connection go to the same endpoint.
• An HTTP load balancer configured to handle cookie-based session persistence forwards requests to the backend server specified by the cookie’s session information.
• For non-sticky HTTP requests, the load balancer applies policy and weight criteria to every incoming request and determines an appropriate backend server. Multiple requests from the same client could be directed to different servers.

**Round Robin**

Round Robin is the default load balancer policy. This policy distributes incoming traffic sequentially to each server in a backend set list. After each server has received a connection, the load balancer repeats the list in the same order.

Round Robin is a simple load balancing algorithm. It works best when all the backend servers have similar capacity and the processing load required by each request does not vary significantly.

**Least Connections**

The Least Connections policy routes incoming non-sticky request traffic to the backend server with the fewest active connections. This policy helps you maintain an equal distribution of active connections with backend servers. As with the round robin policy, you can assign a weight to each backend server and further control traffic distribution.

**Tip:**

In TCP use cases, a connection can be active but have no current traffic. Such connections do not serve as a good load metric.

**IP Hash**

The IP Hash policy uses an incoming request's source IP address as a hashing key to route non-sticky traffic to the same backend server. The load balancer routes requests from the same client to the same backend server as long as that server is available. This policy honors server weight settings when establishing the initial connection.

IP Hash ensures that requests from a particular client are always directed to the same backend server, as long as it is available.

You cannot add a backend server marked as **Backup** to a backend set that uses the IP Hash policy.

**Caution:**

Multiple clients that connect to the load balancer through a proxy or NAT router appear to have the same IP address. If you apply the IP Hash policy to your backend set, the load balancer routes traffic based on the incoming IP address and sends these proxied client requests to the same backend server. If the proxied client pool is large, the requests could flood a backend server.

**Connection Management**

Oracle Cloud Infrastructure load balancers support connection multiplexing. The load balancer can route many incoming requests from multiple clients to the destination backend server through a few (one or multiple) backend connections.

After your load balancer connects a client to a backend server, the connection can be closed due to inactivity. Also, you can configure load balancer listeners to control the maximum idle time allowed during each TCP connection or HTTP request and response pair. Oracle recommends that you do not allow your backend servers to close connections to the load balancer.

**Highlights**

Three different timeout settings affect your load balancer's behavior:

• **Keep-alive setting between the load balancer and backend server**

  The load balancer closes backend server connections that are idle for more than 300 seconds.
• **Keep-alive setting between the load balancer and the client**
  
  The Load Balancing service sets the keep-alive value to maintain the connection for 10,000 transactions or until it has been idle for 65 seconds, whichever limit occurs first. You cannot change the value of this setting.

• **Idle timeout**
  
  You can set the duration of the idle timeout when you create a listener. This setting applies to the time allowed between two successive receive or two successive send network input/output operations during the HTTP request-response phase.

---

**Keep-Alive Settings**

The load balancing service does not honor keep-alive settings from backend servers. The load balancer closes backend server connections that are idle for more than 300 seconds. Oracle recommends that you do not allow your backend servers to close connections to the load balancer. To prevent possible 502 errors, ensure that your backend servers do not close idle connections in less than 310 seconds.

The Load Balancing service sets the keep-alive value to maintain the connection for 10,000 transactions or until it has been idle for 65 seconds, whichever limit occurs first. You cannot change the value of this setting.

---

**Connection Configuration**

When you create a TCP or HTTP listener, you can specify the maximum idle time in seconds. This setting applies to the time allowed between two successive receive or two successive send network input/output operations during the HTTP request-response phase. If the configured timeout has elapsed with no packets sent or received, the client's connection is closed. For HTTP and WebSocket connections, a send operation does not reset the timer for receive operations and a receive operation does not reset the timer for send operations.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This timeout setting does not apply to idle time between a completed response and a subsequent HTTP request.</td>
</tr>
</tbody>
</table>

The default timeout values are:

• 300 seconds for TCP listeners.
• 60 seconds for HTTP listeners.

Modify the timeout parameter if either the client or the backend server requires more time to transmit data. Some examples include:

• The client sends a database query to the backend server and the database takes over 300 seconds to execute. Therefore, the backend server does not transmit any data within 300 seconds.
• The client uploads data using the HTTP protocol. During the upload, the backend does not transmit any data to the client for more than 60 seconds.
• The client downloads data using the HTTP protocol. After the initial request, it stops transmitting data to the backend server for more than 60 seconds.
• The client starts transmitting data after establishing a WebSocket connection, but the backend server does not transmit data for more than 60 seconds.
• The backend server starts transmitting data after establishing a WebSocket connection, but the client does not transmit data for more than 60 seconds.

The maximum timeout value is 7200 seconds. Contact My Oracle Support to file a service request if you want to increase this limit for your tenancy. For more information, see Service Limits on page 215.

**HTTP "X-" Headers**

HTTP requests and responses often include header fields that provide contextual information about the message. RFC 2616 defines a standard set of HTTP header fields. Some non-standard header fields, which begin with X-., are common. The Load Balancing service adds or modifies the following X- headers when it passes requests to your servers.
**X-Forwarded-For**

Provides a list of connection IP addresses.

The load balancer appends the last remote peer address to the X-Forwarded-For field from the incoming request. A comma and space precede the appended address. If the client request header does not include an X-Forwarded-For field, this value is equal to the X-Real-IP value. The original requesting client is the first (left-most) IP address in the list, assuming that the incoming field content is trustworthy. The last address is the last (most recent) peer, that is, the machine from which the load balancer received the request. The format is:

```
X-Forwarded-For: <original_client>, <proxy1>, <proxy2>
```

Example incoming field:

```
X-Forwarded-For: 202.1.112.187
```

Example field with appended proxy IP address:

```
X-Forwarded-For: 202.1.112.187, 192.168.0.10
```

**X-Forwarded-Host**

Identifies the original host and port requested by the client in the **Host** HTTP request header. This header helps you determine the original host, since the hostname or port of the reverse proxy (load balancer) might differ from the original server handling the request.

```
X-Forwarded-Host: www.oracle.com:8080
```

**X-Forwarded-Port**

Identifies the listener port number that the client used to connect to the load balancer. For example:

```
X-Forwarded-Port: 443
```

**X-Forwarded-Proto**

Identifies the protocol that the client used to connect to the load balancer, either http or https. For example:

```
X-Forwarded-Proto: https
```

**X-Real-IP**

Identifies the client's IP address. For the Load Balancing service, the "client" is the last remote peer.

Your load balancer intercepts traffic between the client and your server. Your server's access logs, therefore, include only the load balancer's IP address. The X-Real-IP header provides the client's IP address. For example:

```
X-Real-IP: 192.168.0.10
```

**Session Persistence**

Session persistence is a method to direct all requests originating from a single logical client to a single backend web server. Backend servers that use caching to improve performance, or to enable log-in sessions or shopping carts, can benefit from session persistence.

You enable session persistence when you create a load balancer or when you create a backend set. You can also edit an existing backend set to enable, disable, or change the session persistence configuration.
Sticky Cookies

The Load Balancing service offers two mutually exclusive cookie-based configurations for enabling session persistence:

- Application cookie stickiness
- Load balancer cookie stickiness

**Note:**

**IP Address-driven Session Persistence**

Some products offer session persistence support without cookies. These products depend on the IP address of the incoming request. ISP proxies and company exit gateways can issue many requests from a single IP address. In this case, a single backend server can be subject to high traffic volumes. Your backend fleet can become overwhelmed, one server at a time, even though effective load balancing is possible.

Another weakness of IP address-driven session persistence is that the originating IP address can change. In this case, session persistence can be lost or the request redirected to the wrong backend server.

**Application Cookie Stickiness**

To configure application cookie session persistence, you specify a cookie name and decide whether to disable fallback for unavailable servers.

The Load Balancing service activates application cookie session persistence (stickiness) when a backend server sends a `Set-Cookie` response header containing a recognized cookie name. The cookie name must match the name specified in the backend set configuration. If the configuration specifies a match-all pattern, `*`, any cookie set by the server activates session persistence. Unless a backend server activates session persistence, the service follows the load balancing policy specified when you created the load balancer.

**Requirements:**

- Your load balancer must operate in HTTP mode to support server side, cookie-driven session persistence.
- The client computer must accept cookies for Load Balancing session persistence feature to work.

**How It Works**

The Load Balancing service calculates a hash of the configured cookie and other request parameters, and sends that value to the client in a cookie. The value stored in the cookie enables the service to route subsequent client requests to the correct backend server. If your backend servers change any of the defined cookies, the service recomputes the cookie's value and resends it to the client.

**Caution:**

Oracle recommends that you treat cookie data as an opaque entity. Do not use it in your applications.

The backend server can stop application cookie persistence by deleting the session persistence cookie. If you used the match-all pattern, it must delete all cookies. You can delete cookies by sending a `Set-Cookie` response header with a past expiration date. The Load Balancing service routes subsequent requests using the configured load balancing policy.

**Load Balancer Cookie Stickiness**

When you configure load balancer cookie stickiness, the load balancer inserts a cookie into the response. The parameters configured within the cookie enable session stickiness. This method is useful when you have applications and web backend services that cannot generate their own cookies.
To configure load balancer cookie session persistence, you specify:

- **The cookie name.**
  
  If you do not specify a cookie name, the default name is X-Oracle-BMC-LBS-Route.

  Ensure that the cookie name used at the backend application servers is different from the cookie name used at the load balancer. To minimize the chance of name collision, Oracle recommends that you use a prefix such as X-Oracle-OCI-.

  If a backend server and the load balancer both insert cookies with the same name, the client or browser behavior can vary depending on the domain value associated with the cookie. If the name and domain values of the Set-cookie header generated by a backend server and the Set-cookie header generated by the load balancer are the same, the client or browser treats them as one cookie. The client returns only one of the cookie values in subsequent requests. If both Set-cookie names are the same, but the domain names are different, the client or browser treats them as two different cookies.

  **Note:**

  - RFC 6265 - HTTP State Management Mechanism describes client and browser behavior when the domain attribute is present or not present in the Set-cookie header.

  If the value of the Domain attribute is example.com in the Set-cookie header, the client includes the same cookie in the Cookie header when making HTTP requests to example.com, www.example.com, and www.abc.example.com. If the Domain attribute is not present, the client returns the cookie only for the domain to which the original request was made.

  - Ensure that this attribute specifies the correct domain value. If the Domain attribute in the Set-cookie header does not include the domain to which the original request was made, the client or browser might reject the cookie. As specified in RFC 6265, the client accepts a cookie with the Domain attribute value example.com or www.example.com sent from www.example.com. It does not accept a cookie with the Domain attribute abc.example.com or www.abc.example.com sent from www.example.com.

- **The domain in which the cookie is valid.** The Set-cookie header inserted by the load balancer contains a domain attribute with the specified value.

  This attribute has no default value. If you do not specify a value, the load balancer does not insert the domain attribute into the Set-cookie header.

- **The URI path in which the cookie is valid.** The Set-cookie header inserted by the load balancer contains a Path attribute with the specified value.

  Clients include the cookie in an HTTP request only if the path portion of the request-uri matches, or is a subdirectory of, the cookie's Path attribute.

  The default value is `/`.
Load Balancing

- **The amount of time the cookie remains valid.** The `Set-cookie` header inserted by the load balancer contains a `Max-Age` attribute with the specified value.

  The specified value must be at least one second. There is no default value for this attribute. If you do not specify a value, the load balancer does not include the `Max-Age` attribute in the `Set-cookie` header. Usually, the client or browser retains the cookie until the current session ends, as defined by the client.

- **Whether the `Set-cookie` header should contain the `Secure` attribute.** The `Secure` attribute directs the client or browser to send the cookie only using a secure protocol.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you set this field to true, you cannot associate the corresponding backend set with an HTTP listener.</td>
</tr>
</tbody>
</table>

- **Whether the `Set-cookie` header should contain the `HttpOnly` attribute.** The `HttpOnly` attribute limits the scope of the cookie to HTTP requests. This attribute directs the client or browser to omit the cookie when providing access to cookies through non-HTTP APIs. For example, it restricts the cookie from JavaScript channels.

- **Whether to disable fallback for unavailable servers.**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path route rules take precedence to determine the target backend server. The load balancer verifies that session stickiness is enabled for the backend server and that the cookie configuration is valid for the target. The system ignores invalid cookies.</td>
</tr>
</tbody>
</table>

**Fallback**

By default, the Load Balancing service directs traffic from a persistent session client to a different backend server when the original server is unavailable. You can configure the backend set to disable this fallback behavior. When you disable fallback, the load balancer fails the request and returns an HTTP 502 code. The service continues to return an HTTP 502 until the client no longer presents a persistent session cookie.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If fallback is disabled, cookies with a distant future expiration date can cause a client outage.</td>
</tr>
</tbody>
</table>

The Load Balancing service considers a server marked drain available for existing persisted sessions. New requests that are not part of an existing persisted session are not sent to that server.

**Managing Load Balancers**

This topic describes how to create or delete a load balancer on your system.

**Prerequisites**

To implement a working load balancer, you need:

- For a public load balancer in a region with multiple `availability domains`, you need a VCN with a public regional subnet or at least two public AD-specific subnets. In the latter case, each AD-specific subnet must reside in a separate availability domain. For more information on subnets, See VCNs and Subnets on page 2821 and Public IP Address Ranges on page 2754.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot specify a private subnet for your public load balancer.</td>
</tr>
</tbody>
</table>

- For a public load balancer in a region with only one availability domain, you need a VCN with at least one public subnet.

- For a private load balancer in any region, you need a VCN with at least one private subnet.
Load Balancing

- Two or more backend servers (Compute instances) running your applications. For more information on Compute instances, see Creating an Instance on page 695.

**Note:**

Private IP Address Consumption

A public load balancer created in one public regional subnet consumes two private IP addresses from the host subnet. The primary and secondary load balancers reside within the same subnet. Each load balancer requires a private IP address from that subnet. The Load Balancing service assigns a floating public IP address, which does not come from the host subnet.

A public load balancer created in two public AD-specific subnets consumes two private IP addresses, one from each host subnet. The primary and secondary load balancers reside within different subnets. Each load balancer requires one private IP address from its host subnet. The Load Balancing service assigns a floating public IP address, which does not come from the host subnets.

A private load balancer created in a single subnet consumes three private IP addresses from the host subnet. The primary and secondary load balancers reside within the same subnet. Each load balancer requires a private IP address from that subnet. The floating private IP address also comes from the host subnet.

**Working with Load Balancers**

For background information on Oracle Cloud Infrastructure Load Balancing, see Overview of Load Balancing on page 2480.

For the purposes of access control, you must specify the compartment where you want the load balancer to reside. Consult an administrator in your organization if you're not sure which compartment to use. For information about compartments and access control, see Managing Compartments on page 2431.

When you create a load balancer within your VCN, you get a public or private IP address, and provisioned total bandwidth. If you need another IP address, you can create another load balancer.

A public load balancer in a region with multiple availability domains requires one public regional subnet or two public AD-specific subnets to host the primary load balancer and a standby. In the latter case, each AD-specific subnet must reside in a separate availability domain. A public load balancer in a region with only one availability domain requires a single public subnet to host the primary load balancer and a standby. For more information on VCNs and subnets, see Networking Overview on page 2748. You can associate the public IPv4 address with a DNS name from any vendor. You can use the public IP address as a front end for incoming traffic. The load balancer can route data traffic to any backend server that is reachable from the VCN.

A private load balancer requires only one subnet to host the primary load balancer and a standby. The private IP address is local to the subnet. The load balancer is accessible only from within the VCN that contains the associated subnet, or as further restricted by your security list rules. The load balancer can route data traffic to any backend server that is reachable from the VCN.

The essential components for load balancing include:

- A load balancer with pre-provisioned bandwidth.
- A **backend set** with a health check policy. See Managing Backend Sets on page 2510.
- Backend servers for your backend set. See Managing Backend Servers on page 2515.
Load Balancing

- One or more listeners. See Managing Listeners on page 2522.
- Load balancer subnet security rules to allow the intended traffic. To learn more about these rules, see Security Rules on page 2833.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To accommodate high-volume traffic, Oracle strongly recommends that you use stateless security rules for your load balancer subnets.</td>
</tr>
</tbody>
</table>

Optionally, you can associate your listeners with SSL server certificate bundles to manage how your system handles SSL traffic. See Managing SSL Certificates on page 2551.

For information about the number of load balancers you can have, see Service Limits on page 215.

Configuration Changes and Service Disruption

For a running load balancer, some configuration changes lead to service disruptions. The following guidelines help you understand the effect of changes to your load balancer.

- Operations that add, remove, or modify a backend server create no disruptions to the Load Balancing service.
- Operations that edit an existing health check policy create no disruptions to the Load Balancing service.
- Operations that trigger a load balancer reconfiguration can produce a brief service disruption with the possibility of some terminated connections.

Health Status

The Load Balancing service provides health status indicators that use your health check policies to report on the general health of your load balancers and their components. You can see health status indicators on the Console List and Details pages for load balancers, backend sets, and backend servers. You also can use the Load Balancing API to retrieve this information.

For general information about health status indicators, see Editing Health Check Policies.

Load Balancer Health Summary

The Console list of load balancers provides health status summaries that indicate the overall health of each load balancer. Health status indicators have four levels. The meaning of each level is:

The Console list of load balancers provides health status summaries that indicate the overall health of each load balancer. Health status indicators come in four levels. The meaning of each level is:

- **OK:** All backend sets associated with the load balancer return a status of OK.
- **WARNING:** All the following conditions are true:
  - At least one backend set associated with the load balancer returns a status of WARNING or UNKNOWN.
  - No backend sets return a status of CRITICAL.
  - The load balancer life-cycle state is ACTIVE.
- **CRITICAL:** At least one backend set associated with the load balancer returns a status of CRITICAL.
- **UNKNOWN:** Any one of the following conditions is true:
  - The load balancer life-cycle state is not ACTIVE.
  - No backend sets are defined for the load balancer.
  - All the following conditions are true:
    - More than half of the backend sets associated with the load balancer return a status of UNKNOWN.
    - None of the backend sets return a status of WARNING or CRITICAL.
    - The load balancer life-cycle state is ACTIVE.
  - The system could not retrieve metrics for any reason.

For guidance on detecting and correcting common issues, see Health Status on page 2559.
Load Balancer Health Details

The load balancer Details page provides the same Overall Health status indicator found in the list of load balancers. It also includes counters for the Backend Set Health status values reported by the load balancer’s child backend sets.

The health status counter badges indicate the following:

- The number of child entities reporting the indicated health status level.
- If a counter corresponds to the overall health, the badge has a fill color.
- If a counter has a zero value, the badge has a light gray outline and no fill color.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Creating Load Balancers

To create a load balancer:

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose a Compartment you have permission to work in under Scope, and then click Create Load Balancer.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select a different compartment in the Management tab under the Advanced Options, that compartment contains the load balancer you are creating instead of the compartment specified here.</td>
</tr>
</tbody>
</table>
3. Follow these workflows:

   **Step 1 - Add Details**

   Specify the attributes of the load balancer.

   - **Load Balancer Name:** Required. Accept the default name or specify a friendly name for the load balancer. It does not have to be unique, but it cannot be changed in the Console. (You can, however, change it with the API.) Avoid entering confidential information.

   - **Choose Visibility Type:** Specify whether your load balancer is public or private.
     - **Public:** Choose this option to create a public load balancer. You can use the assigned public IP address as a front end for incoming traffic and to balance that traffic across all backend servers.
     - **Private:** Choose this option to create a private load balancer. You can use the assigned private IP address as a front end for incoming internal VCN traffic and to balance that traffic across all backend servers.

   - **Choose IP Address Type:** Specify whether the public IP address is reserved or ephemeral.
     - **Ephemeral IP Address:** Choose this option to let Oracle specify an ephemeral IP address for you from the Oracle IP pool. This is the default.
     - **Reserved IP Address:** Choose this option to specify an existing reserved IP address by name, or to create a new reserved IP address by assigning a name and selecting a source IP pool for the address. If you don't select a pool you've created, the default Oracle IP pool is used.

   - **Bandwidth:** The Bandwidth shape options are the following:
     - **Flexible Shapes:** Specify Minimum Bandwidth and Maximum Bandwidth values to create an upper and lower size range for the load balancer's bandwidth shape. Possible sizes range from 10 Mbps to 8000 Mbps. You can use the slider to specify the value or enter it directly into the box to the left of each slider.

       The minimum bandwidth reflects the amount of bandwidth that is always available to provide instant readiness for the workloads.

       The maximum bandwidth is the upper amount of bandwidth the load balancer supports during time of peak workload.

       If you want to specify a fixed shape size, for example 500 Mbps, set the minimum and maximum sliders to the same value.

       If you are creating the load balancer as a paid account user, you can create various shape options based on your limits and later adjust the bandwidth by changing the shape after the load balancer has been created. You can view your service limits and quotas in the Console by navigating to Governance > Limits, Quotas and Usage. Select "LbaaS" from the Service list. Your bandwidth size options are listed. See Service Limits on page 215 for more information.

       Billing is per minute for your load balancer base instance, plus a bandwidth usage fee. If the actual usage is below or equal to your specified minimum bandwidth, you are billed for the minimum bandwidth. If actual usage exceeds the minimum bandwidth, you are billed for the actual bandwidth used for that minute.

       The Always Free option is incorporated into your paid account in your home region. The first 10 Mbps of your bandwidth is free, and is indicated as such on your bill.

       **Note:**

       Government accounts using pre-paid dynamic (fixed) shape sizes run the risk of overage charges if using flexible bandwidth shapes exceeds the predetermined size. Government accounts should be updated to the flexible load balancer SKU, with the appropriate bandwidth quantity, in their contract before using the flexible load balancer feature.
If you are using non-universal credit SKUs, ensure that your contract includes the shape you are updating to so you can prevent incurring overage charges.

- **Always Free**: If you are creating the load balancer as an Always Free user, you can only select the Always Free (10 Mbps) option. Switching away from Always Free prompts you to upgrade to a paid account. Always Free shape options are not available to Government accounts.

**Note:**

If you are creating a load balancer in an Always Free tenancy, the Always Free feature is enabled by default, and only Always Free shape options are available. Upgrading is the only way an Always Free tenancy can select a bandwidth shape option other than the default Always Free size. For more information about Always Free resources, including other capabilities and limitations, see Oracle Cloud Infrastructure Free Tier on page 140.

You can adjust the bandwidth shape to a different size after you have completed creating the load balancer. See Changing the Load Balancer Bandwidth on page 2508 for more information.

- **Enable IPv6 Address Assignment**: Available only in the US Government Cloud. Specify whether the load balancer supports IPv6 addresses for incoming requests.

**Note:**

- When you create a load balancer, you can optionally choose to have an IPv4/IPv6 dual-stack configuration. When you choose the IPv6 option, the Load Balancing service assigns both an IPv4 and an IPv6 address to the load balancer. The load balancer receives client traffic sent to the assigned IPv6 address. The load balancer uses only IPv4 addresses to communicate with backend servers. There is no IPv6 communication between the load balancer and the backend servers.
- IPv6 address assignment occurs only at load balancer creation. You cannot assign an IPv6 address to an existing load balancer.
- **Only VCNs in the US Government Cloud currently support IPv6 addressing.** For more information about Oracle Cloud
Infrastructure's IPv6 implementation, see IPv6 Addresses on page 2889.

- **Choose Networking**

  If the current compartment contains at least one VCN, the Console provides a drop-down list of VCNs for you to choose from.

  - **Virtual Cloud Network in <compartment>:** Required. Specify a VCN for the load balancer.

    By default, the Console shows a list of VCNs in the compartment you’re currently working in. Click the Change Compartment link to select a VCN from a different compartment.

  - **Subnet in <compartment>:** Required. Select an available subnet. For a public load balancer, it must be a public subnet.

    By default, the Console shows a list of subnets in the compartment you’re currently working in. Click the Change Compartment link to select a subnet from a different compartment.

    **Tip:**

    In addition to public or private, subnets can be either regional or AD-specific. Oracle recommends using regional subnets. For more information, see Overview of VCNs and Subnets on page 2822.

  - **Subnet (2 of 2) in <compartment>:** Required for a public load balancer when you specify an AD-specific subnet for Subnet. Select a second public subnet. The second subnet must reside in a separate availability domain from the first subnet.

    **Tip:**

    - If you chose to create a private load balancer under Visibility Type, the form prompts you to select only one subnet.
If you're working in a region that includes only one availability domain, a second subnet is not required. The form prompts you to select only one subnet.

If the current compartment contains no virtual cloud networks, the Load Balancing service offers to create a VCN for you.

- **Virtual Cloud Network in `<compartment>`**: When the current compartment contains no virtual cloud networks, the drop-down list is disabled. The system offers to create a VCN for you.

  If you want to use an existing VCN in another compartment, click the Change Compartment link and choose that compartment from the drop-down list.

  **Virtual Cloud Network Name**: Optional, when the system creates a VCN for you. Specify a friendly name for the new cloud network. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

  If you do not specify a name for the new VCN, the system generates a name for you.

- **Use Network Security Groups to Control Traffic**: Check this box if you want to add your load balancer to a network security group (NSG). For more information about NSGs, see Network Security Groups on page 2841.

- **Network Security Groups in `<compartment>`**: Choose an NSG to add your load balancer to.

  By default, the Console shows a list of NSGs in the compartment you're currently working in. Click the Change Compartment link to select an NSG from a different compartment.

  (Optional) Click **+ Another Network Security Group** to add your load balancer to another NSG.

  **Tip**: You can change the NSGs that your load balancer belongs to after you create it. On the Load Balancer Details page, click the Edit link that appears beside the list of associated network security groups.

- **Show Advanced Options**: Click this link to display the following options:

  - **Management**:
    - **Create in Compartment**: Optionally, you can select a different compartment to host the load balancer. The compartment you select here overrides the compartment listed under Scope selected when first creating the load balancer.

  - **Tagging**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

  **Note**: The following describes the Dynamic Shapes feature, which is only available to certain legacy customer accounts:

  **Dynamic Shapes**: Choose one of the following predefined shape sizes.
  
  - 10 Mbps
  - 100 Mbps
  - 400 Mbps
  - 8000 Mbps

  If you are creating the load balancer as a paid account user, you can create various shape options based on your limits and later adjust the bandwidth by changing the shape after the load balancer has been created. You can view your service limits and quotas in the Console by navigating to Governance > Limits, Quotas and Usage. Select "LbaaS" from the
Load Balancing

| Service list. Your bandwidth size options are listed. See Service Limits on page 215 for more information. You can also select the Always Free option if you have not used your one free tier account.  

You can adjust the bandwidth shape to a different size after you have completed creating the load balancer. See Changing the Load Balancer Bandwidth on page 2508 for more information.  

If you adjust a dynamic size value to a flexible size using the sliders, you cannot revert to a dynamic shape of any size. You can achieve the effect of having a dynamic (fixed) size by setting the minimum and maximum sliders to the same size. |

| Step 2 - Choose Backends |

A load balancer distributes traffic to backend servers within a backend set. A backend set is a logical entity defined by a load balancing policy, a list of backend servers (Compute instances), and a health check policy.  

The load balancer creation workflow creates one backend set for your load balancer. Optionally, you can add backend sets and backend servers after you create the load balancer.  

- **Specify a Load Balancing Policy:** Required. Choose the load balancer policy for the backend set. The available options are:  
  - **Weighted Round Robin:** This policy distributes incoming traffic sequentially to each server in a backend set list.  
  - **IP Hash:** This policy ensures that requests from a particular client are always directed to the same backend server.  
  - **Least Connections:** This policy routes incoming request traffic to the backend server with the fewest active connections.  
  
For more information on these policies, see How Load Balancing Policies Work on page 2488.  
- **Select Backend Servers:** Optional. Add backend servers to the backend set. Click **Add Backends** to select resources from a list of available Compute instances.  
  
| Important: |

When you add backend servers, the Load Balancing service automatically creates security list rules for you. If you prefer to create security list rules manually, click **Show Advanced Options** and choose the option to **Manually configure security list rules after the load balancer is created**.  

- **Add Backends:** Select (check) the instances you want to include in the load balancer's backend set.  
  
To select instances from a different compartment, use the **Change Compartment** link and choose a compartment from the drop-down list.  

After you select the instances you want to add from the current compartment, click **Add Selected Backends**.  

| Tip: |

- You can choose instances from one compartment at a time. After you add instances from one compartment, you can choose **Add More Backends** to add instances from another compartment. |
After you add instances to the backend set, they appear in the Select Backend Servers table. You can:

- Specify the server Port to which the load balancer must direct traffic. The default is port 80.
- Click the Actions icon for a server and choose Delete to remove it from the backend set.

**Specify Health Check Policy:** Required. Specify the test parameters that confirm the health of your backend servers.

- **Protocol:** Required. Specify the protocol to use for health check queries, either HTTP or TCP.

  **Important:**
  
  Configure your health check protocol to match your application or service.

- **Port:** Optional. Specify the backend server port against which to run the health check.

  **Tip:**
  
  You can enter the value '0' to have the health check use the backend server's traffic port.

- **Interval in ms:** Optional. Specify how frequently to run the health check, in milliseconds. The default is 10000 (10 seconds).
- **Timeout in ms:** Optional. Specify the maximum time in milliseconds to wait for a reply to a health check. A health check is successful only if a reply returns within this timeout period. The default is 3000 (3 seconds).
- **Number of retries:** Optional. Specify the number of retries to attempt before a backend server is considered "unhealthy." This number also applies when recovering a server to the "healthy" state. The default is 3.
- **Status Code:** (HTTP only) Optional. Specify the status code a healthy backend server must return.
- **URL Path (URI):** (HTTP only) Required. Specify a URL endpoint against which to run the health check.
- **Response Body Regex:** (HTTP only) Optional. Provide a regular expression for parsing the response body from the backend server.
- **Use SSL:** Optional. Check to apply SSL to the load balancer backend. If you select this option, complete the following:

  - **SSL Certificate:** Select one of these options:
    - **Choose SSL Certificate File:** Drag and drop the certificate file into the SSL Certificate field. Alternatively, click Select Files and navigate your system to where you can select the certificate file
Load Balancing

Certificate files must be in PEM format and must have the .pem, .cer, or .crt file extensions.

**Important:**
If you submit a self-signed certificate for backend SSL, you must submit the same certificate in the corresponding CA Certificate field.

- **Paste SSL Certificate:** Copy and paste a certificate directly into this field.
- **Specify CA Certificate:** Optional. (Recommended for backend SSL termination configurations.) Check this box if you want to provide a CA certificate. See Working with SSL Certificates on page 2551 for more information.
- **Specify Private Key:** Optional. (Required for SSL termination.) Check this box if you want to provide a private key for the certificate.
- **Show Advanced Options:** Click this link to access additional options. Select the tab for the corresponding functionality:
  - **Backend Set Name:** Specify a name for the backend set. It must be unique within the load balancer, and it cannot be changed. If you do not specify a name, the Load Balancing service creates one for you.
    Use only alphanumeric characters, dashes ('-'), and underscores ('_') for backend set names. Backend set names cannot contain spaces. Avoid entering confidential information.
  - **Security List:** Choose to manually configure subnet security list rules to allow the intended traffic or allow the system to create security list rules for you. To learn more about these rules, see Parts of a Security Rule on page 2837.
    - **Manually configure security list rules after the load balancer is created:** When you choose this option, you must configure security list rules after load balancer creation.
    - **Automatically add security list rules:** Default. When you choose this option, the Load Balancing service creates security list rules for you.
      The system displays a table for egress rules and a table for ingress rules. Each table lets you choose the security list that applies to the relevant subnet.
      You can choose whether to apply the proposed rules for each affected subnet.
  - **Session Persistence:** Specify how the load balancer manages session persistence.
    **Important:**
    See Session Persistence on page 2491 for important information on configuring these settings.
    - **Disable Session Persistence:** Choose this option to disable cookie-based session persistence.
    - **Enable Application Cookie Persistence:** Choose this option to enable persistent sessions from a single logical client when the backend application server response includes a Set-cookie header with the cookie name you specify.
      - **Cookie Name:** The cookie name used to enable session persistence. Specify * to match any cookie name. Avoid entering confidential information.
      - **Disable Fallback:** Check this box to disable fallback when the original server is unavailable.
    - **Enable Load Balancer Cookie Persistence:** Choose this option to enable persistent sessions based on a cookie inserted by the load balancer.
      - **Cookie Name:** Specify the name of the cookie used to enable session persistence. If blank, the default cookie name is X-Oracle-BMC-LBS-Route.
        Ensure that any cookie names used at the backend application servers are different from the cookie name used at the load balancer. Avoid entering confidential information.
      - **Disable Fallback:** Check this box to disable fallback when the original server is unavailable.
      - **Domain Name:** Optional. Specify the domain in which the cookie is valid.
Load Balancing

This attribute has no default value. If you do not specify a value, the load balancer does not insert the domain attribute into the Set-cookie header.

- **Path:** Optional. Specify the path in which the cookie is valid. The default value is `/`.
- **Expiration Period in Seconds:** Optional. Specify the amount of time the cookie remains valid. If blank, the cookie expires at the end of the client session.

**Attributes**

- **Secure:** Specify whether the Set-cookie header should contain the Secure attribute. If selected, the client sends the cookie only using a secure protocol.

  If you enable this setting, you cannot associate the corresponding backend set with an HTTP listener.

- **HTTP Only:** Specify whether the Set-cookie header should contain the HttpOnly attribute. If selected, the cookie is limited to HTTP requests. The client omits the cookie when providing access to cookies through non-HTTP APIs such as JavaScript channels.

- **SSL Policy:** Specify the type of cipher suite to use:

  - **TLS Version:** Required. Specify each of the Transport Layer Security (TLS) versions you want:
    - 1.0
    - 1.1
    - 1.2 (recommended)

  You can select any combination of versions.

  - **Specify the Cipher Suite:** Required. Choose one of the following options:

    - **Select Cipher Suite** - Select a set of cipher suites from the list. (default).
      
      All cipher suites listed have at least one cipher from each of the TLS versions you selected.

    - **Create Custom Cipher Suite** - Add ciphers to a new suite.

      Perform the following:

    a. Enter the name of the customer cipher suite in the Suite Name field.
    b. Click Choose Ciphers.

      The Select Ciphers page appears.
    c. Check each cipher that you want to include in the suite.

      The TLS versions associated with each cipher are listed in the Version column. Ensure that any cipher you choose is compatible with the TLS versions you previously chose.
    d. Deselect any ciphers you want to exclude.

    e. Click Select. Then select that custom cipher suite (or whatever suite you want to use) from the Select Cipher Suite list.

    - Click Show Cipher Suite Details to display the individual ciphers the selected cipher suite contains.

**Step 3 - Configure Listener**

- **Listener Name:** Required. Specify a friendly name for the listener. The name must be unique, and cannot be changed. Avoid entering confidential information.

  If you do not specify a name, the Load Balancing service creates one for you.

- **Specify the type of traffic your listener handles:** Required. Specify the protocol to use. Choices are:

  - HTTPS
Load Balancing

- **HTTP**
- **TCP**
- **Specify the port your listener monitors for ingress traffic:** Required. Specify the port. Defaults are:
  - 443 for HTTPS
  - 80 for HTTP
  - 22 for TCP
- **If you chose the HTTPS protocol, or if you chose the TCP protocol and selected the Use SSL check box**
  - **Choose SSL Certificate File:** Required. Drag and drop the certificate file, in PEM format, into the **SSL Certificate** field.
    Alternatively, you can choose the **Paste SSL Certificate** option to paste a certificate directly into this field.
    
    **Important:**
    If you submit a self-signed certificate for backend SSL, you must submit the same certificate in the corresponding CA Certificate field.

- **Specify CA Certificate:** Optional. (Recommended for backend SSL termination configurations.) Select (check) this box if you want to provide a CA certificate. See Working with SSL Certificates on page 2551 for more information.
  - **Choose CA Certificate File:** Drag and drop the CA certificate file, in PEM format, into the **CA Certificate** field.
  
    Alternatively, you can choose the **Paste CA Certificate** option to paste a certificate directly into this field.

- **Specify Private Key:** Optional. (Required for SSL termination.) Select (check) this box if you want to provide a private key for the certificate.
  - **Choose Private Key File:** Drag and drop the private key, in PEM format, into the **Private Key** field.
  
    Alternatively, you can choose the **Paste Private Key** option to paste a private key directly into this field.

- **Use SSL:** Required for HTTPS, optional for TCP, not available for HTTP. Check to apply SSL to the load balancer listener. If you select this option, complete the following:
  - **SSL Certificate:** Select one of these options:
    - **Choose SSL Certificate File:** Drag and drop the certificate file into the **SSL Certificate** field.
  
    Alternatively, click **Select Files** and navigate your system to where you can select the certificate file.
for upload. Certificate files must be in PEM format and must have the .pem, .cer, or .crt file extensions.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you submit a self-signed certificate for backend SSL, you must submit the same certificate in the corresponding CA Certificate field.</td>
</tr>
</tbody>
</table>

- **Paste SSL Certificate:** Copy and paste a certificate directly into this field.
- **Specify CA Certificate:** Optional. (Recommended for backend SSL termination configurations.) Check this box if you want to provide a CA certificate. See Working with SSL Certificates on page 2551 for more information.
- **Specify Private Key:** Optional. (Required for SSL termination.) Check this box if you want to provide a private key for the certificate.
- **Show Advanced Options:** Click this link to access additional options. Select the tab for the corresponding functionality:
  - **Timeout tab:** Specify the maximum idle time in seconds. This setting applies to the time allowed between two successive receive or two successive send network input/output operations during the HTTP request-response phase.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum value is 7200 seconds. For more information, see Connection Management on page 2489.</td>
</tr>
</tbody>
</table>

- **SSL Policy tab:** Specify the type of cipher suite to use:
  - **TLS Version:** Required. Specify the Transport Layer Security (TLS) versions:
    - 1.0
    - 1.1
    - 1.2 (recommended)
  You can select any combination of versions. Choose the ones you want from the list.
  - **Specify the Cipher Suite:** Required. Choose one of the following options:
    - **Select Cipher Suite** - Select a predefined set of cipher suites. (default).
      Pick a choice from the Select Cipher Suite list. All cipher suites listed have at least one cipher from each of the TLS versions you selected.
    - **Create Custom Cipher Suite** - Add ciphers to a new suite.
      Perform the following:
      a. Enter the name of the customer cipher suite in the Suite Name field.
      b. Click Choose Ciphers.
         The Select Ciphers page appears.
      c. Check each cipher that you want to include in the suite.
         The TLS versions associated with each cipher are listed in the Version column. Ensure that any cipher you choose is compatible with the TLS versions you previously chose.
      d. Deselect any ciphers you want to exclude.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign at least one cipher to a cipher suite you create. You cannot create a cipher suite that contains no ciphers.</td>
</tr>
</tbody>
</table>
  e. Click Select. Then select that custom cipher suite (or whatever suite you want to use) from the Select Cipher Suite list.
- **Click Show Cipher Suite Details** to display what ciphers the selected cipher suite contains.
Load Balancing

- **Server Order Preference**: Select Enable to give preference to the server ciphers over the client.

4. Click Create Load Balancer.

After the system provisions the load balancer, details appear in the load balancer list. To view more details, click the load balancer name.

### Note:

The following describes the Dynamic Shapes feature, which is only available to certain legacy customer accounts:

**Dynamic Shapes**: Choose one of the following predefined shape sizes.

- 10 Mbps
- 100 Mbps
- 400 Mbps
- 8000 Mbps

If you are creating the load balancer as a paid account user, you can create various shape options based on your limits and later adjust the bandwidth by changing the shape after the load balancer has been created. You can view your service limits and quotas in the Console by navigating to Governance > Limits, Quotas and Usage. Select "LbaaS" from the Service list. Your bandwidth size options are listed. See Service Limits on page 215 for more information. You can also select the Always Free option if you have not used your one free tier account.

You can adjust the bandwidth shape to a different size after you have completed creating the load balancer. See Changing the Load Balancer Bandwidth on page 2508 for more information.

If you adjust a dynamic size value to a flexible size using the sliders, you cannot revert to a dynamic shape of any size. You can achieve the effect of having a dynamic (fixed) size by setting the minimum and maximum sliders to the same size.

**Editing Load Balancers**

To edit a load balancer

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to edit.
3. Click the load balancer you want to edit under the Name column.
   - The Details page for that load balancer appears.
4. Click the various links under Resources to edit different aspects of the load balancer as wanted.
   - See Creating Load Balancers on page 2497 for details on specific configurations.

**Changing the Load Balancer Bandwidth**

If you are not an Always Free user, you can adjust the size of the bandwidth to one of the other predefined sizes.

### Note:

Always Free users cannot change the bandwidth of a load balancer. Upgrade to a different account if you want to increase your bandwidth size.

**To change a load balancer's bandwidth**

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
   - The Load Balancer page appears listing the load balancers associated with the selected compartment.
2. Choose the **Compartment** that contains the load balancer you want to change.
3. Click the load balancer whose bandwidth you want to change.
   The selected load balancer's Details page appears.
4. Click **Update Shape**.
   The Update Shape dialog box appears. The options displayed vary on what type of existing bandwidth size option you are using.
   - Changing a flexible shape: Enter the values for the **Minimum Bandwidth** and **Maximum Bandwidth** shape sizes you want changed.
     
     **Note:**
     Using flexible bandwidth shapes for Government accounts can result in overages if the pre-paid shape sizes are exceeded.
     
     If you want to specify a dynamic shape size, for example 500 Mbps, set the minimum and maximum sliders to the same value.
   - Changing a dynamic shape: Select the new bandwidth of the load balancer from the **Choose Shape Size** list. The existing bandwidth size of the load balancer is unavailable to select.
     
     You can switch from a dynamic shape size to a flexible shape by checking the **Use a Flexible Load Balancer** option and specifying your shape size using the minimum and maximum sliders (see **Changing a flexible shape**).
     
     **Note:**
     Once you have switched to a flexible shape, you cannot revert to a dynamic shape.

5. Click **Save Changes**.
   Changing the bandwidth size of the load balancer requires resetting all existing sessions of the load balancer.
6. Click **Confirm** to continue.
   The Details page reappears.

**Terminating Load Balancers**

**To terminate a load balancer**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to delete.
3. Find the load balancer you want to terminate.
4. Click the **Actions** icon ( ) associated with the load balancer you want to delete and then click **Terminate**.
   Alternatively, you can click the load balancer link to display the Details page and click **Terminate**.
   You are prompted to confirm you want to terminate the load balancer.
5. Click **Terminate** to confirm the termination.

**Moving a Load Balancer to a Different Compartment**

You can move your load balancer from its current compartment into a different compartment. For information about compartments and access control, see **Managing Compartments** on page 2431.

**To move a load balancer to a different compartment**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Select a compartment under the **List Scope** section.
3. Click the **Actions** icon (ISTRIBUTION) associated with the load balancer you want to move, then click **Move Resource**. The Move Resource dialog box appears.

4. Choose the destination compartment from the list.

5. Click **Move Resource**.

### Managing Tags for a Load Balancer

You can apply tags to your resources, such as load balancers, to help you organize them according to your business needs. You can apply tags at the time you create a load balancer, or you can update the load balancer later with the wanted tags. For general information about applying tags, see [Resource Tags](#) on page 211.

**To manage tags for a load balancer**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to tag, and then click the load balancer's name.
3. Click the **Tags** tab to view or edit existing tags, or click **Apply Tag(s)** to add new ones.

For more information, see [Resource Tags](#) on page 211.

### Logging

You can view logging on a variety of load balancer areas, including access and errors. See [Details for Load Balancer Logs](#) on page 2605 for more information.

### Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see [Monitoring Overview](#) on page 2660 and [Notifications Overview](#) on page 3350.

For information about monitoring the traffic passing through your load balancer, see [Load Balancing Metrics](#) on page 2567.

### Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use these API operations to manage load balancers:

- ChangeLoadBalancerCompartment
- CreateLoadBalancer
- DeleteLoadBalancer
- GetLoadBalancer
- GetLoadBalancerHealth
- ListLoadBalancers
- ListLoadBalancerHealths
- UpdateLoadBalancer: You can update the load balancer's display name.
- UpdateNetworkSecurityGroups
- UpdateLoadBalancerShape

### Managing Backend Sets

This topic describes how to create and delete backend sets for use with a load balancer. For information about managing load balancers, see [Managing Load Balancers](#) on page 2494.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with Backend Sets

A backend set is a logical entity defined by a load balancing policy, a health check policy, and a list of backend servers. To create a backend set, you must specify a load balancing policy and health check script, and then add a list of backend servers (Compute instances). SSL and session persistence configuration is optional. A backend set must be associated with one or more listeners for the load balancer to work.

You cannot delete a backend set used by an active listener.

Changing the load balancing policy of a backend set temporarily interrupts traffic and can drop active connections.

For background information on the Oracle Cloud Infrastructure Load Balancing, see Overview of Load Balancing on page 2480.

Click Backend Sets under Resources in the Load Balancer Details page to display the Backend Sets page. This page contains a button for creating new backend sets.

Health Status

The Load Balancing service provides health status indicators that use your health check policies to report on the general health of your load balancers and their components. You can see health status indicators on the Console List and Details pages for load balancers, backend sets, and backend servers. You also can use the Load Balancing API to retrieve this information.

For general information about health status indicators, see Editing Health Check Policies.

Backend Set Health Summary

The Console list of a load balancer's backend sets provides health status summaries that indicate the overall health of each backend set. Health status indicators have four levels. The meaning of each level is:

- **OK**: All backend servers in the backend set return a status of OK.
- **WARNING**: Both of the following conditions are true:
  - Half or more of the backend set's backend servers return a status of OK.
  - At least one backend server returns a status of WARNING, CRITICAL, or UNKNOWN.
- **CRITICAL**: Fewer than half of the backend set's backend servers return a status of OK.
- **UNKNOWN**: At least one of the following conditions is true:
  - More than half of the backend set's backend servers return a status of UNKNOWN.
  - The system could not retrieve metrics for any reason.
  - The backend set does not have a listener attached.

For guidance on detecting and correcting common issues, see Health Status on page 2559.
**Backend Set Health Details**

The backend set *Details* page provides the same *Overall Health* status indicator found in the load balancer's list of backend sets. It also includes counters for the *Backend Health* status values reported by the backend set's child backend servers.

The health status counter badges indicate the following:

- The number of child entities reporting the indicated health status level.
- If a counter corresponds to the overall health, the badge has a fill color.
- If a counter has a zero value, the badge has a light gray outline and no fill color.

**Creating Backend Sets**

**To create a backend set**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click **Backend Sets** under the **Resources** menu, then click **Create Backend Set**.

   The **Create Backend Set** dialog box appears.
4. Enter the following:
   
   - **Name**: Required. Specify a friendly name for the backend set. It must be unique within the load balancer, and it cannot be changed.
     
     Valid backend set names include only alphanumeric characters, dashes, and underscores. Backend set names cannot contain spaces. Avoid entering confidential information.
   
   - **Traffic Distribution Policy**: Required. Choose the load balancer policy for the backend set. The available options are:
     
     - **IP Hash**
     - **Least Connections**
     - **Weighted Round Robin**
     
     For more information on these policies, see How Load Balancing Policies Work on page 2488.
     
     **Tip:**
     
     You cannot add a backend server marked as **Backup** to a backend set that uses the IP Hash policy.
   
   - **Use SSL**: Optional. Check this box to associate an SSL certificate bundle with the backend set.
     
     If there are no certificate bundles attached to the load balancer, this option is disabled.
     
     **Note:**
     
     If you check **Use SSL**, the **SSL Policies** fields appear at the bottom of the page.
     
     - **Certificate Name**: Required. Select the certificate bundle to use. You can choose any certificate bundle that is attached to the current load balancer. See Managing SSL Certificates on page 2551 for more information.
     
     - **Verify Peer Certificate**: Optional. Select this option to enable peer certificate verification.
     
     - **Verify Depth**: Optional. Specify the maximum depth for certificate chain verification.
     
     - **Session Persistence**: Optional. Specify how the load balancer manages session persistence.
     
     **Important:**
     
     See Session Persistence on page 2491 for important information on configuring these settings.
     
     - **Disable Session Persistence**: Choose this option to disable cookie-based session persistence.
     
     - **Enable Application Cookie Persistence**: Choose this option to enable persistent sessions from a single logical client when the response from a backend application server includes a Set-cookie header with the cookie name you specify.
       
       - **Cookie Name**: The cookie name used to enable session persistence. Specify * to match any cookie name. Avoid entering confidential information.
       
       - **Disable Fallback**: Check this box to disable fallback when the original server is unavailable.
       
       - **Enable Load Balancer Cookie Persistence**: Choose this option to enable persistent sessions based on a cookie inserted by the load balancer.
         
         - **Cookie Name**: Specify the name of the cookie used to enable session persistence. If blank, the default cookie name is X-Oracle-BMC-LBS-Route.
           
           Ensure that any cookie names used at the backend application servers are different from the cookie name used at the load balancer. Avoid entering confidential information.
         
         - **Disable Fallback**: Check this box to disable fallback when the original server is unavailable.
         
         - **Domain Name**: Optional. Specify the domain in which the cookie is valid.
           
           This attribute has no default value. If you do not specify a value, the load balancer does not insert the domain attribute into the Set-cookie header.
• **Path:** Optional. Specify the path in which the cookie is valid. The default value is /.

• **Expiration Period in Seconds:** Optional. Specify the amount of time the cookie remains valid. If blank, the cookie expires at the end of the client session.

• **Attributes**
  - **Secure:** Specify whether the Set-cookie header should contain the Secure attribute. If selected, the client sends the cookie only using a secure protocol.
    
    If you enable this setting, you cannot associate the corresponding backend set with an HTTP listener.
  - **HTTP Only:** Specify whether the Set-cookie header should contain the HttpOnly attribute. If selected, the cookie is limited to HTTP requests. The client omits the cookie when providing access to cookies through non-HTTP APIs such as JavaScript channels.

• **Health Check:** Required. Specify the test parameters to confirm the health of backend servers.

  • **Protocol:** Required. Specify the protocol to use, either HTTP or TCP.

    __Important:__

    Configure your health check protocol to match your application or service.

  • **Port:** Optional. Specify the backend server port against which to run the health check.

    __Tip:__

    You can enter the value '0' to have the health check use the backend server's traffic port.

  • **URL Path (URI):** (HTTP only) Required. Specify a URL endpoint against which to run the health check.

  • **Interval in ms:** Optional. Specify how frequently to run the health check, in milliseconds. The default is 10000 (10 seconds).

  • **Timeout in ms:** Optional. Specify the maximum time in milliseconds to wait for a reply to a health check. A health check is successful only if a reply returns within this timeout period. The default is 3000 (3 seconds).

  • **Number of retries:** Optional. Specify the number of retries to attempt before a backend server is considered "unhealthy". This number also applies when recovering a server to the "healthy" state. The default is '3'.

  • **Status Code:** (HTTP only) Optional. Specify the status code a healthy backend server must return.

  • **Response Body Regexp:** (HTTP only) Optional. Provide a regular expression for parsing the response body from the backend server.

• **SSL Policy:** Optional. Specify the type of cipher suite to use:

  __Note:__

  You must check Use SSL for the SSL Policy features to be displayed.

  • **TLS Version:** Optional. Specify the Transport Layer Security (TLS) version(s):
    - 1.0
    - 1.1
    - 1.2 (recommended)

    You can select any combination of versions. Choose the ones you want from the list. If you do not specify the TLS versions, the default TLS is version 1.2 only.

    • **Select Cipher Suite** - Select a set of cipher suites from the list. (default).

      All choices present in the list have at least one cipher associated with each TLS version you selected.

    • Click Show Cipher Suite Details to display the individual ciphers the selected cipher suite contains.

5. Click Create.
After your backend set is provisioned, you must specify backend servers for the set. See Managing Backend Servers on page 2515 for more information.

**Editing Backend Sets**

**To edit a backend set**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating the backend set temporarily interrupts traffic and can drop active connections.</td>
</tr>
</tbody>
</table>

When you edit a backed set, you can choose a new load balancing policy and modify the SSL configuration.

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click **Backend Sets** under the **Resources** menu, then click the name of the backend set you want to edit.
4. Click **Edit Backend Set**.
5. Edit the backend set configuration changes as wanted.
   
   See Creating Backend Sets on page 2512 for details on specific configurations.
6. Click **Submit**.

If you want to modify the backend set's health check policy, see Editing Health Check Policies on page 2558.

If you want to add or remove backend servers from the backend set, see Managing Backend Servers on page 2515.

**Deleting Backend Sets**

**To delete a backend set**

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot delete a backend set used by an active listener. First, remove any backend sets you want to delete from the associated listeners.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click **Backend Sets** under the **Resources** menu.
4. Click the the Actions icon (three dots) associated with the backend set you want to delete, then click **Delete**.
5. Confirm when prompted.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage load balancer backend sets:

- CreateBackendSet
- DeleteBackendSet
- GetBackendSet
- GetBackendSetHealth
- ListBackendSets
- UpdateBackendSet

**Managing Backend Servers**

This topic describes how to manage backend servers for use with a load balancer. For information about managing load balancers, see Managing Load Balancers on page 2494.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with Backend Servers

When you implement a load balancer, you must specify the backend servers (Compute instances) to include in each backend set. The load balancer routes incoming traffic to these backend servers based on the policies you specified for the backend set. You can use the Console to add and remove backend servers in a backend set.

To route traffic to a backend server, the Load Balancing service requires the IP address of the compute instance and the relevant application port. If the backend server resides within the same VCN as the load balancer, Oracle recommends that you specify the compute instance's private IP address. If the backend server resides within a different VCN, you must specify the public IP address of the compute instance. You also must ensure that the VCN's security rules allow Internet traffic.

Caution:

When you add backend servers to a backend set, you specify either the instance OCID or an IP address for the server to add. An instance with multiple VNICs attached can have multiple IP addresses pointing to it.

- If you identify a backend server by OCID, Load Balancing uses the primary VNIC's primary private IP address.
- If you identify the backend servers to add to a backend set by their IP addresses, it is possible to point to the same instance more than once.

To enable backend traffic, your backend server subnets must have appropriate ingress and egress security rules. When you add backend servers to a backend set, you can specify the applicable network security groups (NSGs). If you prefer to use security lists for your VCN, the Load Balancing service Console can suggest security list rules for you. You also can configure them yourself through the Networking service. See Security Lists on page 2850 for more information.

Tip:

To accommodate high-volume traffic, Oracle strongly recommends that you use stateless security rules for your load balancer subnets.

You can add and remove backend servers without disrupting traffic.

Health Status

The Load Balancing service provides health status indicators that use your health check policies to report on the general health of your load balancers and their components. You can see health status indicators on the Console List and Details pages for load balancers, backend sets, and backend servers. You also can use the Load Balancing API to retrieve this information.

For general information about health status indicators, see Editing Health Check Policies.
**Backend Server Health Summary**

The Console list of a backend set's backend servers provides health status summaries that indicate the overall health of each backend server. The primary and standby load balancers both provide health check results that contribute to the health status. Health status indicators have four levels. The meaning of each level is:

- **OK**: The primary and standby load balancer health checks both return a status of OK.
- **WARNING**: One health check returned a status of OK and one did not.
- **CRITICAL**: Neither health check returned a status of OK.
- **UNKNOWN**: One or both health checks returned a status of UNKNOWN or the system was unable to retrieve metrics.

To view the health status details for a specific backend server, click its **IP Address**.

For guidance on detecting and correcting common issues, see **Health Status** on page 2559.

**Backend Server Health Details**

The **Details** page for a backend set provides the same **Overall Health** status indicator found in the backend set's list of backend servers. It also reports the following data for the two health checks performed against each backend server:

**IP ADDRESS**

The IP address of the health check status report provider, which is a Compute instance managed by the Load Balancing service. This identifier helps you differentiate same-subnet load balancers that report health check status.

The Load Balancing service ensures high availability by providing one primary and one standby load balancer. To diagnose a backend server issue, you must know the source of the health check report. For example, a misconfigured security rule might cause one load balancer instance to report that a backend server is healthy. The other load balancer instance might return an unhealthy status. In this case, one of the two load balancer instances cannot communicate with the backend server. Reconfigure the security rules to restore the backend server's health status.

**STATUS**

The status returned by the health check. Possible values include:
• **OK**
  The backend server's response satisfied the health check policy requirements.
• **INVALID_STATUS_CODE**
  The HTTP response status code did not match the expected status code specified by the health policy.
• **TIMED_OUT**
  The backend server did not respond within the timeout interval specified by the health policy.
• **REGEX_MISMATCH**
  The backend server response did not satisfy the regular expression specified by the health policy.
• **CONNECT_FAILED**
  The health check server could not connect to the backend server.
• **IO_ERROR**
  An input or output communication error occurred while reading or writing a response or request to the backend server.
• **OFFLINE**
  The backend server is set to offline, so health checks are not run.
• **UNKNOWN**
  Health check status is not available.

**LAST CHECKED**

The date and time of the most recent health check.

Health status is updated every three minutes. No finer granularity is available.

**How to debug backend timeout**

Backend timeout or a 504 means that a backend server is either down or not responding to the request forwarded by the load balancer. The client application receives the following response code: HTTP/1.1 504 Gateway Timeout.

**Causes**

• The load balancer failed to establish a connection to the backend server before the connection timeout expired.
• The load balancer established a connection to the backend server but the backend did not respond before the idle timeout period elapsed.
• The security lists/NSGs for the subnet/VNIC did not allow traffic from the backends to the load balancer.
• Backend server/application crash.

**Troubleshooting Steps**

1. Run a curl test directly to the backend from a host in the same network.
   a. `curl -i http://10.0.0.5`
   b. If this test takes longer than one second but the test still responded, then it is likely an application level issue causing latency. We recommend checking any upstream dependency that may cause latency, common components include the following:
      • Network attached storage such as ISCSI or NFS
      • Database latency
      • An off-premise API
      • An application tier
2. Check the application by accessing it directly from the backend and access logs. Can it be addressed? Is it working as intended?
3. If the load balancer and the backend are in different subnets, check the security lists rules to allow traffic else the traffic will be dropped.

4. Check if there are no firewall rules on the backend servers that is blocking the traffic.
   a. `iptables -L` will list all firewall rules enforced by iptables
   b. `sudo firewall-cmd --list-all` will list all firewall rules enforced by firewalld

5. Enable logging on the load balancer that will help determine if the latency is caused due to load balancer or the backend server.

How to test TCP and HTTP backends

The following section describes how to troubleshoot a load balancer connection. The topology used has a public load balancer in a public subnet and the back-ends are in the same subnet.

Oracle recommends using primarily the OCI logging service to troubleshoot in this scenario. Details for Load Balancer Logs on page 2605. However, in addition to using OCI logging you can also use some additional tools to troubleshoot the traffic processed by the load balancer and sent to a backend. To perform these tests we recommend creating an instance in the same network as your load balancer and allowing the traffic in the same network security groups and security lists. Use the following tools to troubleshoot.

• `ping <ip address of backend>`

Using the Console

To add one or more servers to a backend set

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer’s name.
3. In the Resources menu, click Backend Sets, and then click the name of the backend set to which you want to add one or more backend servers.

   Tip:
   If the load balancer has no backend sets, you must create one before you can specify a backend server.

4. In the Resources menu, click Backends, and then click Add Backends.

   Tip:
   You cannot add a backend server marked as Backup to a backend set that uses the IP Hash policy.
5. **Choose how to add backend servers:** Specify how you want to add backend servers to the backend set:

- **Compute Instances:** Choose this option to select from a list of available Compute instances.
- **Instances in <compartment>:** Select (check) the instances you want to include in the backend set.
  
  To select instances from a different compartment, use the Change Compartment link and choose a compartment from the drop-down list.

  **Tip:**

  You can choose instances from one compartment at a time. After you add instances from one compartment, you must repeat the Add Backends process to add instances from another compartment.

Once you select an instance to add to the backend set, you can specify:

- **Port:** Required. The backend server port to which the load balancer must direct traffic.
- **Weight:** The load balancing weight assigned to the server. For more information, see [How Load Balancing Policies Work](#) on page 2488.
- Choose to manually configure subnet security list rules that allow the intended traffic or let the Load Balancing service create security list rules for you. To learn more about these rules, see [Parts of a Security Rule](#) on page 2837.

  - **Manually configure security list rules after the load balancer is created:** When you choose this option, you must create your own rules after adding the backend servers.
  
  - **Automatically add security list rules:** When you choose this option, the Load Balancing service creates security list rules for you.

    The system displays a table for egress rules and a table for ingress rules. Each table lets you choose the security list that applies to the relevant subnet. You can then choose whether to apply the proposed rules for each affected subnet.

- **IP Addresses:** Choose this option to enter the IP addresses of the backend servers (Compute instances) to add.

  - **IP Address:** Required. Specify the IP address of a backend server you want to add to the backend set.
  
  - **Port:** Required. Specify the server port to which the load balancer must direct traffic.
  
  - **Weight:** Required. Specify the load balancing weight to apply to this server. For more information, see [How Load Balancing Policies Work](#) on page 2488.

  You can click the plus + icon to add another server to the list or click the X icon to remove a list item.

6. **Click Add.**

**To edit backend server settings**

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Backend Sets, and then click the name of the backend set that includes the backend servers you want to edit.
4. In the Resources menu, click Backend. A list of servers in the backend set appears.
5. Select (check) the row corresponding to the backend server you want to edit.
6. Choose an action from the **Actions** button drop-down list. The available actions include:

   a. **Edit**: Opens a single dialog box in which you can edit the port, weight, drain, offline, and backup settings.
   b. **Edit Port**: Opens a dialog box in which you can change the application port setting.
   c. **Edit Weight**: Opens a dialog box in which you can change the load balancing weight.
   d. **Edit Drain State**: Opens a dialog box in which you can change the drain state.

   If you set the server's drain status to `true`, the load balancer stops forwarding new TCP connections and new non-sticky HTTP requests to this backend server. This setting allows an administrator to take the server out of rotation for maintenance purposes.
   e. **Edit Offline State**: Opens a dialog box in which you can change the offline status.

   If you set the server's offline status to `true`, the load balance forwards no ingress traffic to this backend server.
   f. **Edit Backup State**: Opens a dialog box in which you can change the backup status.

   If you set the server's backup status to `true`, the load balancer forwards ingress traffic to this backend server only when all other backend servers not marked as backup fail the health check policy. This configuration is useful for handling disaster recovery scenarios.

   **Caution:**
   Backend servers marked as **Backup** are not compatible with a load balancer that uses the IP Hash policy.

   g. **Delete**: Removes the server from the backend set.

   **Tip:**
   You can select multiple servers to apply the same action to each one.

7. Click **Save Changes**.

**To remove a server from a backend set**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the **Resources** menu, click **Backend Sets**, and then click the name of the backend set from which you want to remove a server.
4. In the **Resources** menu, click **Backends**. A list of servers in the backend set appears.
5. Select (check) the row corresponding to the backend server you want to edit.
6. Choose the **Delete** action from the **Actions** button drop-down list.
7. Confirm when prompted.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage the backend servers in a backend set:

- **CreateBackend**
- **DeleteBackend**
- **GetBackend**
- **GetBackendHealth**
- **ListBackends**
- **UpdateBackend**
Managing Listeners

This topic describes how to create and manage listeners. This topic is part of the setup and maintenance of a load balancer. For more Load Balancing information about managing load balancers, see Managing Load Balancers on page 2494.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with *inspect load-balancers* gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with Listeners

A listener is a logical entity that checks for incoming traffic on the load balancer's IP address.

To handle TCP, HTTP, and HTTPS traffic, you must configure at least one listener per traffic type.

When you create a listener, you must ensure that your VCN's *security rules* allow the listener to accept traffic.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To accommodate high-volume traffic, Oracle strongly recommends that you use <em>stateless security rules</em> for your load balancer subnets.</td>
</tr>
</tbody>
</table>

You can have one SSL certificate bundle per listener. You can configure two listeners, one each for ports 443 and 8443, and associate SSL certificate bundles with each listener. For more information about SSL certificates for load balancers, see Managing SSL Certificates on page 2551.

Click **Listeners** under **Resources** in the Load Balancer Details page to display the Listeners page. This page contains a button for creating listeners.

Creating Listeners

To create a listener

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click **Listeners** under the **Resources** menu, then click **Create Listener**.

   The Create Listener dialog box appears.
4. Enter the following:

- **Name**: Required. Specify a friendly name for the listener. The name must be unique, and cannot be changed. Avoid entering confidential information.

- **Hostname**: Optional. Select up to 16 virtual hostnames for this listener.

  **Important:**

  To apply a virtual hostname to a listener, the name must be part of the load balancer's configuration. If the load balancer has no associated hostnames, you can create one on the **Hostnames** page.

- **Protocol**: Required. Specify the protocol to use, either HTTP or TCP.

- **Port**: Required. Specify the port on which to listen for incoming traffic.

- **Use SSL**: Optional. Check this box to associate an SSL certificate bundle with the listener. The following settings are required to enable SSL handling. See Managing SSL Certificates on page 2551 for more information.

  - **Certificate Name**: The friendly name of the SSL certificate bundle to use.
  
  - **Verify Peer Certificate**: Optional. Select this option to enable peer certificate verification.
  
  - **Verify Depth**: Optional. Specify the maximum depth for certificate chain verification.

- **Backend Set**: Required. Specify the default backend set to which the listener routes traffic.

- **Idle Timeout in Seconds**: Optional. Specify the maximum idle time in seconds. This setting applies to the time allowed between two successive receive or two successive send network input/output operations during the HTTP request-response phase.

  **Tip:**

  The maximum value is 7200 seconds. For more information, see Connection Management on page 2489.

- **Path Route Set**: Optional. Specify the name of the set of path-based routing rules that applies to this listener's traffic.

  **Important:**

  - To apply a path route set to a listener, the set must be part of the load balancer's configuration.
  
  - To remove a path route set from an existing listener, choose None as the **Path Route Set** option. The path route set remains available for use by other listeners on this load balancer.

- **Show Advanced Options**: Click to display the following options:

  - **TLS Version**: Specify the Transport Layer Security (TLS) version(s):
    
    - 1.0
    - 1.1
    - 1.2 (recommended)
    
    You can select any combination of versions. Choose the ones you want from the list. If you do not specify the TLS versions, the default TLS is version 1.2 only.

  - **Select Cipher Suite** - Select a set of cipher suites from the list. (default).

    All choices present in the list have at least one cipher associated with each TLS version you selected.

  - **Server Order Preference**: Select Enable to give preference to the server ciphers over the client.

5. Click **Create**.

When you create a listener, you must also update your VCN's security rules to allow traffic to that listener.
Editing Listeners

To edit a listener

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click Listeners under the Resources menu.
4. Click the the Actions icon (three dots) associated with the listener you want to edit, then click Edit.
5. Edit the listener configuration as wanted.

   See Creating Listeners on page 2522 for details on specific configurations.
6. Click Save Changes.

Deleting Listeners

To delete a listener

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click Listeners under the Resources menu.
4. Click the the Actions icon (three dots) associated with the listener you want to delete, then click Delete.
5. Confirm when prompted.

Enabling Listeners to Accept Traffic

To enable a listener to accept traffic, you must update your VCN’s security rules:

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.

   The list of VCNs in the current compartment appears.
2. Click the name of the VCN containing your load balancer, and then click Security Groups or Security Lists.

   A list of the security groups or lists in the cloud network appears.
3. Click the name of the NSG or security list that applies to your load balancer.
4. Add or edit the existing rules to allow access from the appropriate resources.

   An NSG’s security rules appear on the Network Security Group Details page. From there you can add, edit, or remove rules.

   The Security List Details page provides access to separate tables in which you can add or edit Ingress Rules or Egress Rules.

   For details on rule configuration, see Security Rules on page 2833.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage listeners:

- CreateListener
- DeleteListener
- UpdateListener
Managing Cipher Suites

This topic describes how to create and manage cipher suites. Cipher suites are part of the setup and maintenance of a load balancer. For more Load Balancing information about managing load balancers, see Managing Load Balancers on page 2494.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you are new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with Cipher Suites

A cipher suite is a logical entity for a set of algorithms, or ciphers, using Transport Layer Security (TLS) to determine the security, compatibility, and speed of HTTPS traffic. All ciphers are associated with at least one version of Transport Layer Security (TLS) 1.0, 1.1, and 1.2.

Note:

Any cipher suite you use or create must contain individual ciphers that match the TLS version supported in your environment. Some ciphers can work with multiple TLS versions. If your environment supports at least one of the TLS versions associated with a given cipher, you can use it.

When you create or edit a listener, you add or can change the associated cipher suite. See Managing Listeners on page 2522 for more information.

Click Cipher Suites under Resources in the Load Balancer Details page to display the Cipher Suites page. This page contains a button for creating cipher suites.

This page also contains a list of all the currently available cipher suites, both ones that came originally preconfigured from Oracle Cloud Infrastructure (Predefined=Yes), and ones that you created yourself (Predefined=No). You can modify or delete those cipher suites you created yourself (Predefined=No). You cannot modify predefined cipher suites.

Creating Cipher Suites

You can create cipher suites as a resource within the Load Balancer service in the Console. The cipher suites you create are available to use when configuring the load balancer's listener and backend set.

To create a cipher suite

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer for which you want to create cipher suites.
3. Click the load balancer you want from the list.
   The Load Balancer Details page for that load balancer appears.
4. Click Cipher Suites under Resources.
   The Cipher Suites page appears.
5. Click Create Cipher Suite.
   The Create Cipher Suite page appears.
6. Enter a name for the cipher suite you are creating in the **Suite Name** field. Avoid entering confidential information.

7. Check those TLS versions under **Filters** from which you want to select.

   Ciphers associated with the TLS versions you checked (displaying which TLS versions they support) appear. Only select TLS versions that are supported in your environment.

   **Note:**
   
   Assign at least one cipher to a cipher suite you create. You cannot create a cipher suite that contains no ciphers.

8. Check those ciphers that you want to include in your cipher suite.

   The total number of ciphers available can span multiple pages. Use the **Search Ciphers** field to find a specific cipher.

   Uncheck a cipher to deselect it from the cipher suite.

9. Click **Create Suite**.

   **Note:**

   Note the following related to creating cipher suites:

   - Ensure compatibility between specified SSL protocols and configured ciphers in the cipher suite, or else the SSL handshake will not be successful.
   - Ensure compatibility between configured ciphers in the cipher suite and configured certificates (for example, RSA-based ciphers require an RSA certificate whereas ECDSA based ciphers require ECDSA certificates).
   - For all load balancer and listener resources that were created before the cipher suites feature was available, the following apply:
     - When running a GET operation, the cipher suite value returned is by default "oci-default-ssl-cipher-suite-v1" inside the listener's SSL configuration. You can update this value by editing the load balancer or listener.
     - When running a GET operation, the cipher suite value returned is displayed as "oci-customized-ssl-cipher-suite" inside the listener's SSL configuration if the cipher configuration of those load balancers was customized after the load balancer creation via Oracle operations.
   - For all existing load balancer backendsets that were created before the cipher suites feature was available, running a GET operation displays the cipher suite value as "oci-wider-compatible-ssl-cipher-suite-v1" inside the backendset's SSL configuration.
   - If running a GET operation on a load balancer listener displays the cipher suite value as "oci-customized-ssl-cipher-suite", then choose the appropriate cipher suite name (either pre-defined or custom defined cipher suites) when updating these load balancers.
   - The cipher suite name "oci-customized-ssl-cipher-suite" is reserved for use by Oracle and is not acceptable as an available name for a custom cipher suite.

**Viewing Cipher Suite Details**

The Cipher Suite Details page is where you can view the ciphers contained in the cipher suite. When you first create a cipher suite, the Details page appears. After that, you can view the Details page using the following method.

From the Details page, you can also modify or delete custom cipher suites. You cannot modify or delete preconfigured cipher suites.
To view the details of a cipher suite

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer whose cipher suite you want to modify, and then click the load balancer's name.
3. Click Cipher Suites under Resources.

   The Cipher Suites page appears.
4. Click the link under Name for the cipher suite whose details you want to view.

   Alternatively, you can click the Actions icon (three dots), and then click View Details.

   The Details page for that cipher suite appears. The Details page displays those ciphers currently included in the cipher suite.

Editing Cipher Suites

Edit a cipher suite to change the ciphers it contains.

To edit a cipher suite

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer whose cipher suite you want to modify, and then click the load balancer's name.
3. Click Cipher Suites under Resources.

   The Cipher Suites page appears.
4. Click the Actions icon (three dots), and then click Edit for the cipher suite you want to edit.

   Alternatively, you can open the Details page for the cipher suite you want to edit. See Viewing Cipher Suite Details on page 2526 for more information.
5. Modify the ciphers contained in the cipher suite as wanted:

   • To add ciphers, click Manage Cipher(s).

     The Select Ciphers page appears. Check the ciphers that you want to add. The ciphers you add must be compatible with the TLS version you are using. Use the Filters to limit the available ciphers by the TLS versions they support. Click Select Ciphers. You are returned to the Details page.

   • To remove ciphers, check those ciphers listed in the Details page and click Remove. All the check ciphers are removed.

     You can remove individual ciphers by clicking the Actions icon (⋮) for the associated cipher, then click Delete.

     | Note: |
     |-------|
     | You cannot delete all ciphers from a cipher suite. The cipher suite must contain at least one cipher after editing. |

Any updates you make are automatically saved.

Deleting Cipher Suites

You cannot delete a cipher suite that is in use. Ensure all listeners and backend sets using the cipher suite you want to delete are managed to a different suite first. You may not have access to all compartments containing associated resources.

To delete a cipher suite

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can only delete a custom (Predefined=No) cipher suite.</td>
</tr>
</tbody>
</table>
1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Cipher Suites.
   The Cipher Suite page appears.
4. Click the Actions icon (three dots) associated with the cipher suite you want to delete, and then click Delete.
   Alternatively, you can open the Details page for the cipher suite you want to delete. The Details page for that cipher suite appears. Click Delete. See Viewing Cipher Suite Details on page 2526 for more information.
5. Confirm when prompted. The deleted cipher suite disappears from the list.

**Supported Ciphers**

Here is a list of supported ciphers by TLS version.

**TLS version 1.2**

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES128-SHA256
- AES256-GCM-SHA384
- AES256-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DH-DSS-AES256-GCM-SHA384
- DH-DSS-AES256-GCM-SHA384
- DH-RSA-AES256-GCM-SHA384
- DH-DSS-AES256-SHA256
- DH-RSA-AES256-SHA256
- DH-DSS-AES256-SHA256
- ECDH-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- DH-DSS-AES128-GCM-SHA256
- DH-RSA-AES128-GCM-SHA256
- DH-DSS-AES128-SHA256
- DH-RSA-AES128-SHA256
- DH-DSS-AES128-SHA256
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256

**TLS version 1.0/1.1 ciphers supported by TLS version 1.2**

- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- AES128-SHA
- AES256-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-RSA-CAMELLIA128-SHA
- DHE-DSS-CAMELLIA256-SHA
- DHE-DSS-CAMELLIA128-SHA
- DHE-RSA-SEED-SHA
- DHE-DSS-SEED-SHA
- DH-RSA-SEED-SHA
- DH-DSS-SEED-SHA
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- DH-RSA-AES256-SHA
- DH-DSS-AES256-SHA
- DH-RSA-CAMELLIA256-SHA
- DH-DSS-CAMELLIA256-SHA
- ECDH-RSA-AES256-SHA
- ECDH-ECDSA-AES256-SHA
- CAMELLIA256-SHA
- PSK-AES256-CBC-SHA
- DHE-DSS-AES128-SHA
- DH-RSA-AES128-SHA
- DH-DSS-AES128-SHA
- DH-RSA-CAMELLIA128-SHA
- DH-DSS-CAMELLIA128-SHA
- ECDH-RSA-AES128-SHA
- ECDH-ECDSA-AES128-SHA
- SEED-SHA
- CAMELLIA128-SHA
- PSK-AES128-CBC-SHA
- DES-CBC3-SHA
- IDEA-CBC-SHA
- ECDHE-RSA-DES-CBC3-SHA
- ECDHE-ECDSA-DES-CBC3-SHA
- DHE-RSA-DES-CBC3-SHA
- DHE-DSS-DES-CBC3-SHA
- DH-RSA-DES-CBC3-SHA
- DH-DSS-DES-CBC3-SHA
- ECDH-RSA-DES-CBC3-SHA
- ECDHE-ECDSA-DES-CBC3-SHA
- PSK-3DES-EDE-CBC-SHA
- KRB5-IDEA-CBC-SHA
• KRB5-DES-CBC3-SHA
• KRB5-IDEA-CBC-MD5
• KRB5-DES-CBC3-MD5
• ECDHE-RSA-RC4-SHA
• ECDHE-ECDSA-RC4-SHA
• ECDH-RSA-RC4-SHA
• ECDH-ECDSA-RC4-SHA
• RC4-SHA
• RC4-MD5
• PSK-RC4-SHA
• KRB5-RC4-SHA
• KRB5-RC4-MD5

**Predefined Cipher Suites**

Here is a list of the cipher suites that are available for use with Load Balancing, along with the individual ciphers they include.

**oci-default-ssl-cipher-suite-v1**

This cipher suite contains a restricted set of ciphers that are only supported in TLS version 1.2, and meets stricter compliance requirements.

• ECDHE-RSA-AES128-GCM-SHA256
• ECDHE-RSA-AES128-SHA256
• ECDHE-RSA-AES256-GCM-SHA384
• ECDHE-RSA-AES256-SHA384
• DHE-RSA-AES256-GCM-SHA384
• DHE-RSA-AES256-SHA256
• DHE-RSA-AES128-GCM-SHA256
• DHE-RSA-AES128-SHA256

**oci-modern-ssl-cipher-suite-v1**

This cipher suite offers a wider set of ciphers, but still only supported in TLS version 1.2.

• ECDHE-ECDSA-AES128-GCM-SHA256
• ECDHE-RSA-AES128-GCM-SHA256
• ECDHE-ECDSA-AES128-SHA256
• ECDHE-RSA-AES128-SHA256
• ECDHE-ECDSA-AES256-GCM-SHA384
• ECDHE-RSA-AES256-GCM-SHA384
• ECDHE-ECDSA-AES256-SHA384
• ECDHE-RSA-AES256-SHA384
• AES128-GCM-SHA256
• AES128-SHA256
• AES256-GCM-SHA384
• AES256-SHA256
• DHE-RSA-AES256-GCM-SHA384
• DHE-RSA-AES256-SHA256
• DHE-RSA-AES128-GCM-SHA256
• DHE-RSA-AES128-SHA256

**oci-compatible-ssl-cipher-suite-v1**

This cipher suite supports the broadest set of ciphers. It contains ciphers supported by TLS versions 1.1 and 1.2.
Load Balancing

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256

**oci-wider-compatible-ssl-cipher-suite-v1**

This cipher suite contains all supported ciphers.
• TLS version 1.2:
  • ECDHE-ECDSA-AES128-GCM-SHA256
  • ECDHE-RSA-AES128-GCM-SHA256
  • ECDHE-ECDSA-AES128-SHA256
  • ECDHE-RSA-AES128-SHA256
  • ECDHE-ECDSA-AES256-GCM-SHA384
  • ECDHE-RSA-AES256-GCM-SHA384
  • ECDHE-ECDSA-AES256-SHA384
  • ECDHE-RSA-AES256-SHA384
  • AES128-SHA256
  • AES256-GCM-SHA384
  • AES256-SHA256
  • DHE-RSA-AES256-GCM-SHA384
  • DHE-RSA-AES256-SHA256
  • DHE-RSA-AES128-GCM-SHA256
  • DHE-RSA-AES128-SHA256
  • DH-DSS-AES256-GCM-SHA384
  • DH-DSS-AES256-GCM-SHA384
  • DH-RSA-AES256-GCM-SHA384
  • DH-DSS-AES256-SHA256
  • DH-RSA-AES256-SHA256
  • DH-DSS-AES256-SHA256
  • ECDH-RSA-AES256-GCM-SHA384
  • ECDH-ECDSA-AES256-GCM-SHA384
  • ECDH-RSA-AES256-SHA384
  • ECDH-ECDSA-AES256-SHA384
  • DH-DSS-AES128-GCM-SHA256
  • DH-DSS-AES128-GCM-SHA256
  • DH-RSA-AES128-GCM-SHA256
  • DH-DSS-AES128-SHA256
  • DH-RSA-AES128-SHA256
  • DH-DSS-AES128-SHA256
  • ECDH-RSA-AES128-GCM-SHA256
  • ECDH-ECDSA-AES128-GCM-SHA256
  • ECDH-RSA-AES128-SHA256
  • ECDH-ECDSA-AES128-SHA256
- TLS version 1.1:
  - ECDHE-ECDSA-AES128-SHA
  - ECDHE-ECDSA-AES256-SHA
  - ECDHE-RSA-AES128-SHA
  - ECDHE-RSA-AES256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA
  - AES256-SHA
  - DES-CBC3-SHA
  - DHE-RSA-AES256-SHA
  - DHE-RSA-AES128-SHA
  - DHE-RSA-CAMELLIA256-SHA
  - DHE-RSA-CAMELLIA128-SHA
  - DHE-RSA-SEED-SHA
  - DHE-RSA-AES256-SHA
  - DHE-DSS-AES256-SHA
  - DH-RSA-AES256-SHA
  - DH-DSS-AES256-SHA
  - DHE-RSA-CAMELLIA256-SHA
  - DHE-DSS-CAMELLIA256-SHA
  - DH-RSA-CAMELLIA256-SHA
  - DH-DSS-CAMELLIA256-SHA
  - ECDH-RSA-AES256-SHA
  - ECDH-ECDSA-AES256-SHA
  - CAMELLIA256-SHA
  - PSK-AES256-CBC-SHA
  - DHE-RSA-AES128-SHA
  - DHE-DSS-AES128-SHA
  - DH-RSA-AES128-SHA
  - DH-DSS-AES128-SHA
  - DHE-RSA-CAMELLIA128-SHA
  - DHE-DSS-CAMELLIA128-SHA
  - DH-RSA-CAMELLIA128-SHA
  - DH-DSS-CAMELLIA128-SHA
  - ECDH-RSA-AES128-SHA
  - ECDH-ECDSA-AES128-SHA
  - CAMELLIA128-SHA
  - PSK-AES128-CBC-SHA
  - API SPEC

`oci-customized-ssl-cipher-suite`

This cipher suite reflects customized cipher tasks performed by Oracle on a client-specific basis prior to the general release of the cipher suite feature.

**Managing Cipher Suites in Listeners and Backend Sets**

When you create a load balancer, specifying the cipher suite is part of configuring the listener and the backend set. See *Creating Load Balancers* on page 2497 for more information.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage cipher suites:

- CreateSSLCipherSuite
- UpdateSSLCipherSuite
- DeleteSSLCipherSuite
- GetSSLCipherSuite
- ListSSLCipherSuites

Managing Request Routing

This topic describes how to manage your load balancer's request routing. For information about managing load balancers, see Managing Load Balancers on page 2494.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Routing Incoming Requests

The Load Balancing service enables you to route incoming requests to various backend sets. You can:

- Assign virtual hostnames to a listener.
- Create path route rules.
- Combine these techniques.

Virtual Hostnames

When used in concert with A records you create in your DNS system, you can assign virtual hostnames to any listener you create for your load balancer. Each hostname can correspond to a backend set, that backend set can route traffic to specific backends which will host different applications. Some advantages of virtual hostnames include:

- A single associated IP address. Multiple hostnames, backed by DNS entries that you create in your nameservers, can point to the same load balancer IP address.
- A single load balancer. You do not need a separate load balancer for each application.
- A single load balancer shape. Running multiple applications behind a single load balancer helps you manage aggregate bandwidth demands and optimize utilization.
- Simpler backend set management. Managing a set of backend servers under a single resource simplifies network configuration and administration.

You can define exact virtual hostnames, such as "app.example.com", or you can use wildcard names. Wildcard names include an asterisk (*) in place of the first or last part of the name. When searching for a virtual hostname, the service chooses the first matching variant in the following priority order:

1. Exact name match (no asterisk), such as app.example.com.
2. Longest wildcard name that begins with an asterisk, such as *.example.com.

   **Tip:**
   Prefix wildcard names might require a wildcard certificate for HTTPS sites.

3. Longest wildcard name that ends with an asterisk, such as app.example.*.

   **Tip:**
   Suffix wildcard names might require a multi-domain Subject Alternative Name (SAN) certificate for HTTPS sites.

   You do not need to specify the matching pattern to apply. The pattern is inherent in the asterisk position, that is, starting, ending, or none.

The following considerations apply to virtual hostnames:

- You cannot use regular expressions.
- To apply virtual hostnames to a listener, you first create one or more virtual hostnames associated with a load balancer.
- Virtual hostname selection priority is not related to the listener's configuration order.
- You can apply a maximum of 16 virtual hostnames to a listener.
- You can associate a maximum of 16 virtual hostnames with a load balancer.

   **Tip:**
   The virtual hostnames feature supports HTTP and HTTPS listeners only, but does not support TCP listeners.

**Note:**

**Default Listener**

If a listener has no virtual hostname specified, that listener is the default for the assigned port.

If all listeners on a port have virtual hostnames, the first virtual hostname configured for that port serves as the default listener.

**Path Route Rules**

Some applications have multiple endpoints or content types, each distinguished by a unique URI path. For example, /admin/, /data/, /video/, or /cgi/. You can use path route rules to route traffic to the correct backend set without using multiple listeners or load balancers.

A *path route* is a string that the Load Balancing service matches against an incoming URI to determine the appropriate destination backend set.

- You cannot use asterisks in path route strings.
- You cannot use regular expressions.
- Path route string matching is case-insensitive.

   **Important:**
   Browsers often add an ending slash to the path in a request. If you specify a path such as /admin, you might want to configure the path both with and without the trailing slash. For example, /admin and /admin/.

A *path route rule* consists of a path route string and a pattern match type.
Load Balancing

- Pattern match types include:
  - **EXACT_MATCH**
    Looks for a path string that exactly matches the incoming URI path.
    Applies case-insensitive regex:
    ```
    ^<path_string>$
    ```
  - **FORCE_LONGEST_PREFIX_MATCH**
    Looks for the path string with the best, longest match of the beginning portion of the incoming URI path.
    Applies case-insensitive regex:
    ```
    <path_string>.*
    ```
  - **PREFIX_MATCH**
    Looks for a path string that matches the beginning portion of the incoming URI path.
    Applies case-insensitive regex:
    ```
    ^<path_string>.*
    ```
  - **SUFFIX_MATCH**
    Looks for a path string that matches the ending portion of the incoming URI path.
    Applies case-insensitive regex:
    ```
    .*<path_string>$
    ```
- Path route rules apply only to HTTP and HTTPS requests and have no effect on TCP requests.
  - A path route set includes all path route rules that define the data routing for a particular listener.
  - You can specify up to 20 path route rules per path route set.
  - You can have one path route set per listener. The maximum number of listeners limits the number of path route sets you can specify for a load balancer.

**Rule Priority**

The system applies the following priorities, based on match type, to the path route rules within a set:
- For one path route rule that specifies the EXACT_MATCH type, there is no cascade of priorities. The listener looks for an exact match only.
- For two path route rules, one that specifies the EXACT_MATCH type and one that specifies any other match type, the exact match rule is evaluated first. If no match is found, then the system looks for the second match type.
- For multiple path route rules specifying various match types, the system applies the following priority cascade:
  1. EXACT_MATCH
  2. FORCE_LONGEST_PREFIX_MATCH
  3. PREFIX_MATCH or SUFFIX_MATCH
- The order of the rules within the path route set does not matter for EXACT_MATCH and FORCE_LONGEST_PREFIX_MATCH. The system applies the priority cascade no matter where these match types appear in the path route set.
- If matching cascades down to prefix or suffix matching, the order of the rules within the path route set DOES matter. The system chooses the first prefix or suffix rule that matches the incoming URI path.
Virtual Hostname and Path Route Rules Combinations

Virtual hostnames and path route rules route requests to backend sets. Listeners with a virtual hostname receive priority over the default (no hostname) listener. The following example shows the results of a simple routing interaction.

The example system includes three listeners and one path route set:

Listener 1

- Virtual hostname: none
- Default backend set: A
- Path route set: PathRouteSet1

Listener 2

- Virtual hostname: captive.com
- Default backend set: B
- Path route set: PathRouteSet1

Listener 3

- Virtual hostname: wild.com
- Default backend set: C
- Path route set: PathRouteSet1

Path Route Set

- Path route set name: PathRouteSet1
  - Exact match on path string /tame/ routes to backend set B.
  - Exact match on path string /feral/ routes to backend set C.

The example configuration routes incoming URLs as follows:

http://animals.com/ is routed to backend set A

- Virtual hostname animals.com matches Listener 1.
- Path / is not an EXACT_MATCH for any path route string in PathRouteSet1.

http://animals.com/tame/ is routed to backend set B

- Virtual hostname animals.com matches Listener 1.
- Path /tame/ is an EXACT_MATCH for path route string /tame/ in PathRouteSet1.

http://animals.com/feral/ is routed to backend set C

- Virtual hostname animals.com matches Listener 1.
- Path /feral/ is an EXACT_MATCH for path route string /feral/ in PathRouteSet1.

http://captive.com/ is routed to backend set B

- Virtual hostname captive.com matches Listener 2.
- Path / is not an EXACT_MATCH for any path route string in PathRouteSet1.

http://captive.com/tame/ is routed to backend set B

- Virtual hostname captive.com matches Listener 2.
- Path /tame/ is an EXACT_MATCH for path route string /tame/ in PathRouteSet1.

http://captive.com/feral/ is routed to backend set C

- Virtual hostname captive.com matches Listener 2.
- Path /feral/ is an EXACT_MATCH for path route string /feral/ in PathRouteSet1.

http://wild.com/ is routed to backend set C
Load Balancing

- Virtual hostname wild.com matches **Listener 3**.
- Path / is not an EXACT_MATCH for any path route string in PathRouteSet1.

http://wild.com/tame/ is routed to backend set B

- Virtual hostname wild.com matches **Listener 3**.
- Path /tame/ is an EXACT_MATCH for path route string /tame/ in PathRouteSet1.

http://wild.com/feral/ is routed to backend set C

- Virtual hostname wild.com matches **Listener 3**.
- Path /feral/ is an EXACT_MATCH for path route string /feral/ in PathRouteSet1.

**Using the Console**

You can specify virtual hostnames and path route sets when you create or update a listener.

**Creating Virtual Hostnames**

To apply virtual hostnames to a listener, you first create one or more virtual hostnames. The virtual hostnames become a part of the load balancer's configuration. You then specify one or more virtual hostnames to use when you create or update a listener for the load balancer.

**To create a virtual hostname**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the **Resources** menu, click **Hostnames**, and then click **Create Hostname**.
4. In the **Create Hostname** dialog box, enter the following:
   - **Name**: Required. Specify a friendly name for the hostname. The name must be unique, and cannot be changed. Avoid entering confidential information.
   - **Hostname**: Required. Specify the virtual hostname. See **Virtual Hostnames** for a description of valid hostname construction and behavior.
5. Click **Create**. The **Work Request Submitted** dialog box opens.
6. To close the dialog box, click **Close**. To open the **Work Requests** page and view the status of the work request, click **View All Work Requests**.

After you create a virtual hostname, the name becomes available for use with the associated load balance. To apply the hostname, create or update a listener.

**To update a virtual hostname**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the **Resources** menu, click **Hostnames**.
4. For the hostname you want to edit, click the Actions icon (three dots), and then click **Edit**.
5. In the **Edit Hostname** dialog box, enter your updates to the **Hostname** field.
   - You cannot edit the **Name** field of an existing virtual hostname.
6. Click **Update**. The **Work Request Submitted** dialog box opens.
7. To close the dialog box, click **Close**. To open the **Work Requests** page and view the status of the work request, click **View All Work Requests**.

**To delete a virtual hostname**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Hostnames.
4. For the hostname you want to edit, click the Actions icon (three dots), and then click Delete. The Work Request Submitted dialog box opens.
5. To close the dialog box, click Close. To open the Work Requests page and view the status of the work request, click View All Work Requests.

Creating Path Route Sets

To apply path route rules to a listener, you first create a path route set that contains the rules. The path route set becomes a part of the load balancer's configuration. You then specify the path route set to use when you create or update a listener for the load balancer. To remove a path route set from a listener, edit the listener and choose None as the Path Route Set option.

To create a path route set

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Path Route Sets, and then click Create Path Route Set.
4. In the Create Path Route Set dialog box, enter the following:
   - Name: Required. Specify a friendly name for the path route set. The name must be unique, and cannot be changed.
     The path route set name cannot begin with a period and cannot contain the characters ;, ?, #, %, /, \, [, or ]. Avoid entering confidential information.
   - Path Route Rules
     - Order: Optional. If you have multiple path route rules, you can click the up or down arrows to move the corresponding rule.
   - Match Style: Required. The type of matching to apply to incoming URIs.
   - URL String: Required. The path string to match against the incoming URI path, for example /admin/.
   - Backend Set Name: Required. The name of the target backend set for requests where the incoming URI matches the specified path.
5. (Optional) Click + Additional Rule to create another path route rule or click the red box to delete an existing rule. You can have up to 20 path route rules in a set.
6. Click Create.

After you create a path route set, the set becomes available for use with the associated load balance. Create or update a listener to apply the path route set.

To update a path route set

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Path Route Sets.
4. Click the name of the path route set you want to update, and then click Edit Path Route Rules.
5. In the **Edit Path Route Rules** dialog box, edit the following as needed for each rule you want to change:

- **Order**: Optional. If you have multiple path route rules, you can click the up or down arrows to move the corresponding rule.

  Tip:

  The *order of the rules within the path route set* does not matter in most cases. However, if matching cascades down to prefix or suffix matching, the system chooses the first prefix or suffix rule that matches the incoming URI path.

- **Match Style**: Required. The *type of matching* to apply to incoming URIs.

- **URL String**: Required. The path string to match against the incoming URI path, for example `/admin/`.

- **Backend Set Name**: Required. The name of the target backend set for requests where the incoming URI matches the specified path.

6. (Optional) Click **+ Additional Rule** to create another path route rule or click the red box to delete an existing rule. You can have up to 20 path route rules in a set.

7. Click **Save Changes**.

### To update a single path route rule

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.

2. Choose the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.

3. In the **Resources** menu, click **Path Route Sets**, and then click the name of the path route set you want to update.

4. For the path route rule you want to edit, click the Actions icon (three dots), and then click **Edit Path Route**.

5. In the **Edit Path Route Rule** dialog box, edit the following as needed for each rule you want to change:

- **Order**: Optional. If you have multiple path route rules, you can click the up or down arrows to move the corresponding rule.

  Tip:

  The *order of the rules within the path route set* does not matter in most cases. However, if matching cascades down to prefix or suffix matching, the system chooses the first prefix or suffix rule that matches the incoming URI path.

- **Match Style**: Required. The *type of matching* to apply to incoming URIs.

- **URL String**: Required. The path string to match against the incoming URI path, for example `/admin/`.

- **Backend Set Name**: Required. The name of the target backend set for requests where the incoming URI matches the specified path.

6. Click **Save Changes**.

### Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use these API operations to manage request routing:

- `CreateListener`
- `CreatePathRouteSet`
- `DeleteListener`
- `DeletePathRouteSet`
- `GetPathRouteSet`
- `ListPathRouteSets`
- `UpdateListener`
- `UpdatePathRouteSet`
Managing Rule Sets

This topic describes how you can create rule sets composed of actions to apply to traffic at an HTTP listener. For more information about managing load balancer listeners, see Managing Listeners on page 2522.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with Rule Sets

A rule set is a named set of rules associated with a load balancer and applied to one or more listeners on that load balancer. Rules are objects that represent actions applied to traffic at a load balancer listener.

You can include the following types of rules in a rule set:

- Access control rules, which restrict access to application resources based on the source of the request.
- Access method rules, which specify the permitted HTTP methods.
- URL redirect rules, which route incoming HTTP requests to a different destination URL.
- Request and response header rules, which add, alter, or remove HTTP request or response headers.
- HTTP header rules, which specify the size of the HTTP header and whether period and underscore characters are permitted within the headers.

Rule sets apply only to HTTP listeners.

You can apply an existing rule set when you edit a listener. You can apply the same rule set to multiple listeners on the same load balancer.

Rule sets are not shared between load balancers. To use the same set of rules on another load balancer, you must create a new, identical rule set under that load balancer.

You can have up to 20 rules in a rule set. You can associate a maximum of 50 rules with a load balancer.

Access Control Rules

Access control rules permit access to application resources based on user-specified IP address or address range match conditions. If you do not specify any access control rules, the default rule is to allow all traffic. If you add access control rules, the load balancer denies any traffic that does not match the rules.

The service accepts only classless inter-domain routing (CIDR) format (x.x.x.x/y or x:x::x/y) strings for the match condition.

Specify 0.0.0.0/0 or ::/0 to match all incoming traffic.

Note:

Only US Government Cloud regions currently permit IPv6 values.
Access Method Rules

Access method rules specify the HTTP methods allowed at the associated listener. The load balancer does not forward a disallowed request to the backend servers and returns a 405 Method Not Allowed response with a list of the allowed methods. You can associate only one list of allowed methods with a given listener.

By default, you can specify only the standard HTTP methods defined in the HTTP Method Registry. The list of HTTP methods is extensible. If you need to configure custom HTTP methods, contact My Oracle Support to remove the restriction from your tenancy. Your backend application must be able to handle the specified methods.

Default HTTP Methods

ACL
BASELINE-CONTROL
BIND
CHECKIN
CHECKOUT
CONNECT
COPY
DELETE
GET
HEAD
LABEL
LINK
LOCK
MERGE
MKACTIVITY
MKCALENDAR
MKCOL
MKREDIRECTREF
MKWORKSPACE
MOVE
OPTIONS
ORDERPATCH
PATCH
POST
PRI
PROPFIND
ROPPATCH
PUT
REBIND
REPORT
SEARCH
URL Redirect Rules

URL redirect rules specify how to route incoming HTTP requests to a different destination URL. URL redirect rules apply only to HTTP listeners. You configure each redirect rule for a particular listener and a designated path. A listener can have only one redirect rule for a given incoming URL path.

When you create a URL redirect rule, you specify the path string and match condition the service uses to evaluate an incoming URL for redirection. You also define the redirect URL and response code.

Incoming path string evaluation

You specify the path string, or pattern, to evaluate in the incoming URL. For example:

```
/video
```

You also specify the match condition to apply when evaluating the incoming URL for redirection. The available match types are:

- **FORCE_LONGEST_PREFIX_MATCH**
  The system looks for a redirect rule path string with the best, longest match of the beginning portion of the incoming URL path.
- **EXACT_MATCH**
  The incoming URL path must exactly and completely match the specified path string.
- **PREFIX_MATCH**
  The beginning portion of the incoming URL path must exactly match the specified path string.
- **SUFFIX_MATCH**
  The ending portion of the incoming URL path must exactly match the specified path string.

Redirection URL construction

You define the redirect URL applied to the original request. URL redirect rules recognize the following URL components:

```
<protocol>://<host>:<port>/<path>?<query>
```

You can specify a literal string or provide a token for any component. Tokens extract values from the incoming HTTP request URL. Tokens are case-sensitive. For example, `{host}` is a valid token, but `{HOST}` is not.

- **Protocol**
  The HTTP protocol to use in the redirect URL. Valid values are HTTP and HTTPS.
  The `{protocol}` token extracts the protocol from the incoming HTTP request URL. It is the only valid token for this property.
• **Host**
  
The valid domain name or IP address to use in the redirect URL.
  
The `{host}` token extracts the host from the incoming HTTP request URL. All URL Redirect tokens are valid for this property. You can use any token more than once.
  
Curly braces {} are valid in this property only to surround tokens.

• **Port**
  
The communication port to use in the redirect URL. Valid values include integers from 1 to 65535.
  
The `{port}` token extracts the port from the incoming HTTP request URL. It is the only valid token for this property.

• **Path**
  
The HTTP URL path to use in the redirect URL. To omit the path from the redirect URL, set this value to an empty string.
  
The `{path}` token extracts the path string from the incoming HTTP request URL. All URL Redirect tokens are valid for this property. You can use any token more than once.

If the path string does not begin with the `{path}` token, it must begin with a forward slash /.

• **Query**
  
The query string to use in the redirect URL. To omit all incoming query parameters from the redirect URL, set this value to an empty string.
  
The `{query}` token extracts the query string from the incoming HTTP request URL. All URL Redirect tokens are valid for this property. You can use any token more than once.

If the query string does not begin with the `{query}` token, it must begin with a question mark ?.

You can specify multiple query parameters as a single string. Separate each query parameter with an ampersand &.

If the specified query string results in a redirect URL ending with ? or &; the last character is truncated. For example, if the incoming URL is `http://host.com:8080/documents` and the query property value is `?lang=en&{query}`, the redirect URL is `http://host.com:8080/documents?lang=en`. The system truncates the final ampersand & because the incoming URL included no value to replace the `{query}` token.

**Caution:**

Failure to specify a value for at least one URL component field can result in a redirect loop.

---

**Manual Redirect URL construction**

The Console provides text entry fields for each URL component. Alternatively, you can manually specify the full redirect URL.

You can retain the literal characters of a token when you specify values for the path and query properties of the redirect URL. Use a backslash \ as the escape character for the \, \, and } characters. For example, if the incoming HTTP request URL is `/video`, the path property value `/example{path}123\{path\}` appears in the constructed redirect URL as `/example/video123{path}`.

Some path and query string examples:

- `/example/video/123` appears as `/example/video/123` in the redirect URL.
- `/example{path}` appears as `/example/video/123` in the redirect URL when `/video/123` is the path in the incoming HTTP request URL.
- `{path}/123` appears as `/example/video/123` in the redirect URL when `/example/video` is the path in the incoming HTTP request URL.
• {path}123 appears as /example/video123 in the redirect URL when /example/video is the path in the incoming HTTP request URL.

• /{host}/123 appears as /example.com/123 in the redirect URL when example.com is the hostname in the incoming HTTP request URL.

• /{host}/{port} appears as /example.com:123 in the redirect URL when example.com is the hostname and 123 is the port in the incoming HTTP request URL.

• {query} appears as /lang=en in the redirect URL when the query is lang=en in the incoming HTTP request URL.

• lang=en&time_zone=PST appears as lang=en&time_zone=PST in the redirect URL.

• {query} appears as lang=en&time_zone=PST in the redirect URL when lang=en&time_zone=PST is the query string in the incoming HTTP request. If the incoming HTTP request has no query parameters, the {query} token renders as an empty string.

• lang=en&{query}&time_zone=PST appears as lang=en&country=us&time_zone=PST in the redirect URL when country=us is the query string in the incoming HTTP request. If the incoming HTTP request has no query parameters, this value renders as lang=en&time_zone=PST.

• protocol={protocol}&hostname={host} appears as protocol=http&hostname=example.com in the redirect URL when the protocol is http and the hostname is example.com in the incoming HTTP request.

• port={port}&hostname={host} appears as port=8080&hostname=example.com in the redirect URL when the port is 8080 and the hostname is example.com in the incoming HTTP request URL.

**Response Code**

You can specify the HTTP status code to return when the incoming request is redirected. Valid response codes for redirection from the standard HTTP specification are:

- 301 Moved Permanently
- 302 Found
- 303 See Other
- 307 Temporary Redirect
- 308 Permanent Redirect

The default value is 302 Found.

**Request and Response Header Rules**

Request and response header rules add, alter, or remove HTTP request or response headers. These rules can help you pass metadata to your backend servers to do things like:

- Identify which listener sent a request.
- Notify a backend server about SSL termination.

Examples of how rule sets can help you enhance site security include:

- Adding headers to prevent external domains from iframing your site.
- Removing debug headers, such as "Server," sent by backend servers. This action helps you hide the implementation details of your backend.
- Adding the "strict-transport-security" header, with a proper value, to responses. This header helps guarantee that access to your site is HTTPS only.
- Adding the "x-xss-protection" header with a proper value. This header helps you enforce the cross-site scripting (XSS) protection built into modern browsers.
- Adding the "x-content-type" header with a proper value. This header helps you prevent attacks based on content type shifting.

**Note:**

Adding or removing the built-in Host header or one of the X-Headers as described in HTTP "X-" Headers does not remove or override the header
value. Instead, performing these actions can append additional values or duplicate the header.

**Example: Notify WebLogic that the Load Balancer Terminated SSL**

You can configure your load balancer to perform SSL termination. Often, your backend applications require notification of this action. For example, HTTPS WebLogic e-commerce online transaction processing looks for the WL-Proxy-SSL header to confirm that a request came in over SSL. You can use rule sets to add this header at the load balancer listener.

**Tip:**

For security reasons, WebLogic ignores this header unless you check the WebLogic Plugin Enabled box in WebLogic's Administration Console.

1. Follow the instructions to create a rule set and:
   a. Choose the Add Request Header option from the Action drop-down list.
   b. Enter WL-Proxy-SSL as the Header name.
   c. Set the header Value:
      1. If your load balancer is configured to perform SSL termination, set this value to "true."
      2. If the SSL termination point is in the web server where the plug-in operates, set this value to "false."

2. Create a listener, or edit an existing listener, and add the new rule set.

**HTTP Header Rules**

HTTP header rules specify the size of the HTTP header and the kinds of characters that are permitted within the header. Because some applications require a URL header size greater than the default 8k to support their features, HTTP header rules allow you to set header buffers of up to 64k to avoid "414" (large URI requests) errors.

HTTP header rules allow periods ("."), underscores ("_"), providing you more flexibility in your naming structures.

**Creating Rule Sets**

To apply a rule set to a listener, you first create the rule set that contains the rules. The rule set becomes a part of the load balancer's configuration. You can specify the rule set to use when you create or update a listener for the load balancer.

**To create a rule set**

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Rule Sets, and then click Create Rule Set.
4. In the Create Rule Set dialog box, enter the following:
   • **Name**: Required. Specify a friendly name for the rule set. The name must be unique, and cannot be changed. Avoid entering confidential information.
   • **Specify Access Control Rules**: Optional. Check this box to add access control rules.
     • **IP Address CIDR**: Enter the IP address CIDR block from which access is allowed.
     • **+ Another Access Control Rule**: Optional. Click this button to enter another IP address CIDR or click the corresponding X to remove an existing entry.
   • **Specify Access Method Rules**: Optional. Check this box to add access method rules.
     • **Allowed Methods**: From the drop-down list, select the HTTP methods to allow. You can select multiple methods. Click the label's X to remove an existing method.
   • **Specify URL Redirect Rules**: Optional. Check this box to add URL redirect rules.
     • **Source Path**: Specify the incoming path string that triggers the redirect rule. For example, /video.
     • **Match Type**: Choose the match condition to apply when evaluating an incoming path string. The available match types are:
       • **FORCE_LONGEST_PREFIX_MATCH**
         The system looks for a redirect rule path string with the best, longest match of the beginning portion of the incoming URL path.
       • **EXACT_MATCH**
         The incoming URL path must exactly and completely match the specified path string.
       • **PREFIX_MATCH**
         The beginning portion of the incoming URL path must exactly match the specified path string.
       • **SUFFIX_MATCH**
         The ending portion of the incoming URL path must exactly match the specified path string.
     • **Redirect to**: Specify a value for at least one URL component field. Any component fields that you do not modify retain the incoming URL’s values.
       Optionally, click the **Switch to full URL** link to enter the redirect URL manually.

       **Caution:**
       Failure to specify a value for at least one URL component field can result in a redirect loop.

       • **Protocol**: Specify the HTTP protocol to use in the redirect URL. Valid values are:
         • {protocol}
         • HTTPS
         • HTTP
       • **Host**: Specify a valid domain name (hostname) or IP address for the redirect URL. All redirect URL tokens are valid for this property.
       • **Port**: Specify the communication port to use in the redirect URL. Valid values include integers from 1 to 65535.
       • **Path**: The HTTP URL path to use in the redirect URL. All redirect URL tokens are valid for this property.

       **Important:**
       If the path string does not begin with the {path} token, it must begin with the forward slash character /.

       • **Query**: Specify the query string to use in the redirect URL. All redirect URL tokens are valid for this property.
Important:
If the query string does not begin with the \{query\} token, it must begin with the question mark \? character.

- **Response Code**: Specify the HTTP status code to return when the incoming request is redirected. The default response code is **302 Found**.

  Valid response codes for redirection from the standard HTTP specification are:
  - 301 Moved Permanently
  - 302 Found
  - 303 See Other
  - 307 Temporary Redirect
  - 308 Permanent Redirect

- **Another URL Redirect Rule**: Optional. Click this button to create another rule or click the corresponding X to delete an existing rule.

- **Specify Request Header Rules**: Optional. Check this box to add request header rules.

- **Order**: Optional. If you have multiple rules, you can click the up or down arrows to move the corresponding rule.

- **Action**: Select the action that the rule applies. Available actions include:
  - **Add Request Header**
    Adds the specified header and value to the incoming request.
    If the specified header is already present, the system replaces it.
    If more than one header with the same name is present, the system removes all of them and adds one header corresponding to the specified header and value.
  - **Extend Request Header**
    Adds the specified prefix or suffix to the incoming request.
    Provide a prefix value, a suffix value, or both when you choose this action.
    The system does not support this rule for headers with multiple values.
  - **Remove Request Header**
    Removes the specified header.
    If the same header appears more than once in the request, the load balancer removes all occurrences of the specified header.

  **Note**:
  These rules apply only to HTTP or HTTP2 headers.

- **Header**: A header name that conforms to RFC 7230.

  **Caution**:
  The system does not distinguish between underscore and dash characters in headers. That is, it treats example_header_name and example-header-name as identical. Oracle recommends that you do
not rely on underscore or dash characters to uniquely distinguish header names.

- **Value:** (Add rules only.) A header value that conforms to RFC 7230.
- **Prefix:** (Extend rules only.) A character string to add to the beginning of the existing header name. The resulting header must conform to RFC 7230.
- **Suffix:** (Extend rules only.) A character string to add to the end of the existing header name. The resulting header must conform to RFC 7230.
- **+ Another Request Header Rule** Optional. Click this button to create another rule or click the corresponding X to delete an existing rule.
- **Specify Response Header Rules:** Optional. Check this box to add response header rules.
- **Order:** Optional. If you have multiple rules, you can click the up or down arrows to move the corresponding rule.
- **Action:** Select the action that the rule applies. Available actions include:
  - **Add Response Header**
    Adds the specified header and value to the outgoing response.
    If the specified header is already present, the system replaces it.
    If more than one header with the same name is present, the system removes all of them and adds one header corresponding to the specified header and value.
  - **Extend Response Header**
    Adds the specified prefix or suffix to the incoming request.
    Provide a prefix value, a suffix value, or both when you choose this action.
    The system does not support this rule for headers with multiple values.
  - **Remove Response Header**
    Removes the specified header.
    If the same header appears more than once in the response, the load balancer removes all occurrences of the specified header.

**Note:**
These rules apply only to HTTP or HTTP2 headers.

- **Header:** A header name that conforms to RFC 7230.

**Caution:**
The system does not distinguish between underscore and dash characters in headers. That is, it treats example_header_name and example-header-name as identical. Oracle recommends that you do
Load Balancing

not rely on underscore or dash characters to uniquely distinguish header names.

- **Value**: (Add rules only.) A header value that conforms to RFC 7230.
- **Prefix**: (Extend rules only.) A character string to add to the beginning of the existing header name. The resulting header must conform to RFC 7230.
- **Suffix**: (Extend rules only.) A character string to add to the end of the existing header name. The resulting header must conform to RFC 7230.
- **Another Response Header Rule**: Optional. Click this button to create another rule or click the corresponding X to delete an existing rule.
- **Specify HTTP Rules**: Optional. Check this box to specify HTTP header options for a listener.
  - **HTTP Header Buffer Size**: Select one of the following buffer sizes for the HTTP header from the list: None, 8k, 16k, 32k, 64k.
  - **Allow Invalid Characters in HTTP Header**: Check this box to allow periods ("." ) and underscores ("_" ) in the HTTP header.
- **Specify HTTP Header Options**: Optional. Check this box to specify HTTP header options for a listener.
  - **HTTP Header Buffer Size**: Select one of the following buffer sizes for the HTTP header from the list: None, 8k, 16k, 32k, 64k.
  - **Allow Invalid Characters in HTTP Header**: Optional. Check this box to allow invalid characters in the HTTP header.

5. Click Create.

After you create a rule set, the set becomes available for use with the associated load balancer. Update a listener to apply the rule set.

### Editing Rule Sets

**To update a rule set**

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer associated with the rule set you want to modify, and then click the load balancer's name.
3. In the Resources menu, click Rule Sets.
4. Click the name of the rule set you want to edit, and then click Edit Rules.
5. Edit the rules as needed.
   
   You cannot edit the Name field of an existing rule set.
6. Click Save Changes.

### Deleting Rule Sets

**To delete a rule set from a listener**

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer associated with the rule set you want to delete, and then click the load balancer's name.
3. In the Resources menu, click Listeners.
4. For the listener you want to edit, click the the Actions icon (three dots), and then click Edit Listener.
5. In the Rule Sets section of the dialog box, click the corresponding X to remove an existing rule set.

**Tip:**

This action removes the rule set from the current listener, but the rule set remains available for application to other listeners on the load balancer.

6. Click Save Changes.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage rule sets:

- CreateRuleSet
- DeleteRuleSet
- GetRuleSet
- ListRuleSets
- UpdateRuleSet

Use this API to route incoming HTTP requests to a different destination URL:

- RedirectRule

Use this API to allow the setting of HTTP header size and allow or disallow invalid characters in the HTTP headers:

- HttpHeadersRule

Managing SSL Certificates

This topic is part of the setup and maintenance of a load balancer. For more information about managing load balancers, see Managing Load Balancers on page 2494.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with SSL Certificates

To use SSL with your load balancer, you must add one or more certificate bundles to your system. The certificate bundle you upload includes the public certificate, the corresponding private key, and any associated Certificate Authority (CA) certificates. For the easiest workflow, upload the certificate bundles you want to use before you create the listeners or backend sets you want to associate them with.

Load balancers commonly use single domain certificates. However, load balancers with listeners that include request routing configuration might require a subject alternative name (SAN) certificate (also called multi-domain certificate) or a wildcard certificate. The Load Balancing service supports each of these certificate types.

Important:

- The Load Balancing service does not generate SSL certificates. It can only import an existing certificate that you already own. The certificate can be one issued by a vendor, such as Verisign or GoDaddy. You can also use a self-signed certificate that you generate with an open source tool, such as OpenSSL or Let’s Encrypt. Refer to the corresponding tool's documentation for instructions on how to generate a self-signed certificate.
Oracle Cloud Infrastructure accepts x.509 type certificates in PEM format only. The following is an example PEM encoded certificate:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```

Converting to PEM format

If you receive your certificates and keys in formats other than PEM, you must convert them before you can upload them to the system. You can use OpenSSL to convert certificates and keys to PEM format. The following example commands provide guidance.

**Certificate or certificate chain from DER to PEM**

```
openssl x509 -inform DER -in <certificate_name>.der -outform PEM -out <certificate_name>.pem
```

**Private key from DER to PEM**

```
openssl rsa -inform DER -in <private_key_name>.der -outform PEM -out <private_key_name>.pem
```

**Certificate bundle from PKCS#12 (PFX) to PEM**

```
openssl pkcs12 -in <certificate_bundle_name>.p12 -out <certificate_bundle_name>.pem -nodes
```

**Certificate bundle from PKCS#7 to PEM**

```
openssl pkcs7 -in <certificate_bundle_name>.p7b -print_certs -out <certificate_bundle_name>.pem
```

**How to configure and troubleshoot Peer Cert Verify**

The Verify Peer Certificate is used for client authentication. Peer Cert Verify Depth is the number of certificates in the chain that need to be verified for client authentication.

The following are expected values to be set:

- One Intermediate Cert, Client Cert, Root Cert - 2
- Client Cert, Root Cert - 1

To determine if your Peer Cert Verification is misconfigured, note the following:

- Your Client will indicate that it is unable to verify the certificate and will result in a Client SSL handshake failure. This error message will vary based on the client type.
- In your Load Balancer Logs, you will witness the error: `Client %s has SSL certificate verify error`
• Using the OpenSSL tool, run the following command: `openssl verify -verbose -CAfile RootCert.pem Intermediate.pem`

  You will see an error that shows you at what depth the validation failure is occurring: `error 20 at 0 depth lookup:unable to get local issuer certificate`

• To resolve this situation, you will need to provide the correct certificate depth, and confirm the client certificate and CA certificate match and are provided in the correct order.

### Uploading Certificate Chains

If you have multiple certificates that form a single certification chain (for example, any Intermediate CA certificates), include all relevant certificates in one file in the correct order before you upload them to the system. The correct order begins with the certificate directly signed by the Trusted Root CA at the bottom. Any additional certificates are pasted directly on top of the authority who signed it.

You need to combine the Server certificate (`SSL_Certificate.crt`) and the Intermediate CA certificate (`intermediateCA.crt`) files into a single concatenated file.

To get a single concatenated file out of the Intermediate CA and the SSL Certificate, open a command prompt and run the following command:

```
cat ssl_certificate.crt IntermediateCA.crt >> certbundle.pem
```

The following example of a concatenated certificate chain file includes four certificates:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```

### Submitting Private Keys

**Tip:**

Oracle recommends a minimum length of 2048 bits for your RSA private key.

If your private key submission returns an error, the three most common reasons are:

• You provided an incorrect passphrase.
• Your private key is malformed.
• The system does not recognize the encryption method used for your key.

### Key Pair Mismatch

If you receive an error related to the private key and public key being mismatched, prior to uploading use these OpenSSL commands to confirm they are part of the same pair.

```
openssl x509 -in <certificate_name>.crt -noout -modulus | openssl sha1
openssl rsa -in <private_key>.key -noout -modulus | openssl sha1
```
Confirm that the returned sha1 hash values match exactly. If they are different the Private Key provided is not used to sign the public certificate and can not be used.

**Private key consistency**

If you receive an error related to the private key, you can use OpenSSL to check its consistency:

```bash
openssl rsa -check -in <private_key>.pem
```

This command verifies that the key is intact, the passphrase is correct, and the file contains a valid RSA private key.

**Decrypting a private key**

If the system does not recognize the encryption technology used for your private key, decrypt the key. Upload the unencrypted version of the key with your certificate bundle. You can use OpenSSL to decrypt a private key:

```bash
openssl rsa -in <private_key>.pem -out <decrypted_private_key>.pem
```

**Updating an Expiring Certificate**

To ensure consistent service, you must update (rotate) expiring certificates:

1. Update your client or backend server to work with a new certificate bundle.

   **Note:**
   The steps to update your client or backend server are unique to your system.
2. Upload the new SSL certificate bundle to the load balancer
   
   a. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
   
   b. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
   
   c. Click the load balancer you want to configure.
   
   d. In the **Resources** menu, click **Certificates**, and then click **Add Certificate**.
   
   e. In the **Add Certificate** dialog box, enter the following:
      
      • **Certificate Name**: Required. Specify a friendly name for the certificate bundle. It must be unique within the load balancer, and it cannot be changed in the Console. (It can be changed using the API.) Avoid entering confidential information.
      
      • **Choose SSL Certificate File**: Required. Drag and drop the certificate file, in PEM format, into the **SSL Certificate** field.

      Alternatively, you can choose the **Paste SSL Certificate** option to paste a certificate directly into this field.
3. **Edit listeners or backend sets (as needed) so they use the new certificate bundle**

**Editing a listener:**

a. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.

b. Choose the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.

c. In the **Resources** menu, click **Listeners**.

d. For the listener you want to edit, click the Actions icon (three dots), and then click **Edit Listener**.

e. In the **Certificate Name** drop-down list, choose the new certificate bundle.

f. Click **Submit**.

**Editing a backend set:**

> **Caution:**
> Updating the backend set temporarily interrupts traffic and can drop active connections.

a. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.

b. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.

c. In the **Resources** menu, click **Backend Sets**, and then click the name of the backend set you want to edit.

d. Click **Edit Backend Set**.

e. In the **Edit Backend Set** dialog box, select (check) **Use SSL**.

f. In the **Certificate Name** drop-down list, choose the new certificate bundle.

g. Click **Save Changes**.

4. **(Optional) Remove the expiring SSL certificate bundle**

> **Important:**
> You cannot delete an SSL certificate bundle that is associated with a listener or backend set. Remove the bundle from any additional listeners or backend sets before deleting.

a. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.

b. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.

c. Click the load balancer you want to configure.

d. In the **Resources** menu, click **Certificates**.

e. For the certificate you want to delete, click the Actions icon (three dots), and then click **Delete**.

f. Confirm when prompted.

**Configuring SSL Handling**

With Oracle Cloud Infrastructure Load Balancing, you can:

- Terminate SSL at the load balancer. This configuration is **frontend SSL**. Your load balancer can accept encrypted traffic from a client. There is no encryption of traffic between the load balancer and the backend servers.

- Implement SSL between the load balancer and your backend servers. This configuration is **backend SSL**. Your load balancer does not accept encrypted traffic from client servers. Traffic between the load balancer and the backend servers is encrypted.

- Implement end to end SSL. Your load balancer can accept SSL encrypted traffic from clients and encrypts traffic to the backend servers.
**Terminating SSL at the Load Balancer**

To terminate SSL at the load balancer, you must create a listener at a port such as 443, and then associate an uploaded certificate bundle with the listener.

**Implementing Backend SSL**

To implement SSL between the load balancer and your backend servers, you must associate an uploaded certificate bundle with the backend set.

***Tip:***

- If you want to have more than one backend server in the backend set, sign your backend servers with an intermediate CA certificate. The intermediate CA certificate must be included as part of the certificate bundle.
- Your backend services must be able to accept and terminate SSL.

**Implementing End to End SSL**

To implement end to end SSL, you must associate uploaded certificate bundles with both the listener and the backend set.

**Using the Console**

To upload an SSL certificate bundle to your load balancing system

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer’s name.
3. Click the load balancer you want to configure.
4. In the Resources menu, click Certificates, and then click Add Certificate.
5. In the Add Certificate dialog box, enter the following:

   - **Certificate Name:** Required. Specify a friendly name for the certificate bundle. It must be unique within the load balancer, and it cannot be changed in the Console. (It can be changed using the API.) Avoid entering confidential information.
   - **Choose SSL Certificate File:** Required. Drag and drop the certificate file, in PEM format, into the SSL Certificate field.
     Alternatively, you can choose the Paste SSL Certificate option to paste a certificate directly into this field.

     **Important:**
     
     If you submit a self-signed certificate for backend SSL, you must submit the same certificate in the corresponding CA Certificate field.

   - **Specify CA Certificate:** Optional. (Recommended for backend SSL termination configurations.) Select (check) this box if you want to provide a CA certificate.
     - **Choose CA Certificate File:** Drag and drop the CA certificate file, in PEM format, into the CA Certificate field.
       Alternatively, you can choose the Paste CA Certificate option to paste a certificate directly into this field.

   - **Specify Private Key:** Optional. (Required for SSL termination.) Select (check) this box if you want to provide a private key for the certificate.
     - **Choose Private Key File:** Drag and drop the private key, in PEM format, into the Private Key field.
     - **Enter Private Key Passphrase:** Optional. Specify the private key passphrase.

6. Click Add Certificate.
To delete an SSL certificate bundle from your load balancing system

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot delete an SSL certificate bundle that is associated with a listener or backend set. Remove the bundle from any listeners or backend sets before deleting.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click the load balancer you want to configure.
4. In the Resources menu, click Certificates.
5. For the certificate you want to delete, click the Actions icon (three dots), and then click Delete.
6. Confirm when prompted.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage load balancer certificates:

- CreateCertificate
- DeleteCertificate
- ListCertificates

Editing Health Check Policies

This topic describes how to modify health check policies for a backend set.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Working with Health Check Policies

A health check is a test to confirm the availability of backend servers. A health check can be a request or a connection attempt. Based on a time interval you specify, the load balancer applies the health check policy to continuously monitor backend servers. If a server fails the health check, the load balancer takes the server temporarily out of rotation. If the server subsequently passes the health check, the load balancer returns it to the rotation.

You configure your health check policy when you create a backend set. You can configure TCP-level or HTTP-level health checks for your backend servers.

- TCP-level health checks attempt to make a TCP connection with the backend servers and validate the response based on the connection status.
• HTTP-level health checks send requests to the backend servers at a specific URI and validate the response based on the status code or entity data (body) returned.

The service provides application-specific health check capabilities to help you increase availability and reduce your application maintenance window.

**Important:**

Configure your health check protocol to match your application or service.

If you run an HTTP service, be sure to configure an HTTP-level health check. If you run a TCP-level health check against an HTTP service, you might not get an accurate response. The TCP handshake can succeed and indicate that the service is up even when the HTTP service is incorrectly configured or having other issues. Although the health check appears good, customers might experience transaction failures. For example:

- The backend HTTP service has issues when talking to the health check URL and the health check URL returns 5XX messages. An HTTP health check catches the message from the health check URL and marks the service as down. In this case, a TCP health check handshake succeeds and marks the service as healthy, even though the HTTP service is may not be usable.
- The backend HTTP service responds with 4XX messages because of authorization issues or no configured content. A TCP health check does not catch these errors.

**Health Status**

The Load Balancing service provides health status indicators that use your health check policies to report on the general health of your load balancers and their components. You can see health status indicators on the Console List and Details pages for load balancers, backend sets, and backend servers. You also can use the Load Balancing API to retrieve this information.

Health status indicators have four levels. The following table provides the general meaning of each level:

<table>
<thead>
<tr>
<th>Level</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Green</td>
<td>No attention required. The resource is functioning as expected.</td>
</tr>
<tr>
<td>Warning</td>
<td>Yellow</td>
<td>Some reporting entities require attention. The resource is not functioning at peak efficiency or the resource is incomplete and requires further work.</td>
</tr>
<tr>
<td>Critical</td>
<td>Red</td>
<td>Some or all reporting entities require immediate attention. The resource is not functioning or unexpected failure is imminent.</td>
</tr>
<tr>
<td>Level</td>
<td>Color</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unknown</td>
<td>Gray</td>
<td>Health status cannot be determined. The resource is not responding or is in transition and might resolve to another status over time.</td>
</tr>
</tbody>
</table>

The precise meaning of each level differs among the following components:

- **Load balancers**
- **Backend sets**
- **Backend servers**

### Using Health Status

At the highest level, load balancer health reflects the health of its components. The health status indicators provide information you might need to drill down and investigate an existing issue. Some common issues that the health status indicators can help you detect and correct include:

**A health check is misconfigured.**

In this case, all the backend servers for one or more of the affected listeners report as unhealthy. If your investigation finds that the backend servers do not have problems, then a backend set probably includes a misconfigured health check.

**A listener is misconfigured.**

All the backend server health status indicators report **OK**, but the load balancer does not pass traffic on a listener.

The listener might be configured to:

- Listen on the wrong port.
- Use the wrong protocol.
- Use the wrong policy.

If your investigation shows that the listener is not at fault, check the security list configuration.

**A security rule is misconfigured.**

Health status indicators help you diagnose two cases of misconfigured security rules:

- All entity health status indicators report **OK**, but traffic does not flow (as with misconfigured listeners). If the listener is not at fault, check the security rule configuration.
- All entity health statuses report as unhealthy. You have checked your health check configuration and your services run properly on your backend servers.

In this case, your security rules might not include the IP range for the source of the health check requests. You can find the health check source IP on the **Details** page for each backend server. You can also use the API to find the IP in the **sourceIpAddress** field of the **HealthCheckResult** object.

**Note:**

Source IP

The source IP for health check requests comes from a Compute instance managed by the Load Balancing service.

**One or more of the backend servers reports as unhealthy.**

A backend server might be unhealthy or the health check might be misconfigured. To see the corresponding error code, check the **status** field on the backend server's **Details** page. You can also use the API to find the error code in the **healthCheckStatus** field of the **HealthCheckResult** object.
Other cases in which health status might prove helpful include:

- VCN network security groups or security lists block traffic.
- Compute instances have misconfigured route tables.

Health status is updated every three minutes. No finer granularity is available.

Health status does not provide historical health data.

**Health Check Best Practices**

Configure your health check protocol to match your application or service. If you run an HTTP service, be sure to configure an HTTP-level health check. If you run a TCP-level health check against an HTTP service, you might not get an accurate response. The TCP handshake can succeed and indicate that the service is up even when the HTTP service is incorrectly configured or having other issues. Although the health check appears good, customers might experience transaction failures. For example:

- The backend HTTP service has issues when talking to the health check URL and the health check URL returns 5XX messages. An HTTP health check catches the message from the health check URL and marks the service as down. In this case, a TCP health check handshake succeeds and marks the service as healthy, even though the HTTP service may not be usable.
- The backend HTTP service responds with 4XX messages because of authorization issues or no configured content. A TCP health check does not catch these errors.

**Configure the Health Check**

To configure the health check, use the following procedure.

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. In the Resources menu, click **Backend Sets** and then click the name of the backend set you want to modify.
4. Click **Update Health Check**.
5. In the Health Check section, specify the test parameters to confirm the health of backend servers. All parameters are required when updating an existing health check policy.

- **Protocol**: Required. Specify the protocol to use, either HTTP or TCP.

  **Note:**
  Configure your health check protocol to match your application or service.

- **Port**: Required. Specify the backend server port against which to run the health check.

  **Note:**
  You can enter the value '0' to have the health check use the backend server's traffic port.

- **URL Path (URI)**: (HTTP only) Required. Specify a URL endpoint against which to run the health check. Example:

  /health
  (This is a commonly used path for a health check application).

- **Interval in ms**: Required. Specify how frequently to run the health check, in milliseconds. Default is 10000 (10 seconds).

- **Timeout in ms**: Required. Specify the maximum time in milliseconds to wait for a reply to a health check. A health check is successful only if a reply returns within this timeout period. Default is 3000 (3 seconds).

  **Note:**
  Enter a timeout value that is smaller than the interval value to ensure the health check works correctly.

- **Number of retries**: Required. Specify the number of retries to attempt before a backend server is considered "unhealthy." This number also applies when recovering a server to the "healthy" state. The default is 3.

- **Status Code**: (HTTP only) Required. Specify the status code a healthy backend server must return.

- **Response Body Regex**: (HTTP only) Optional. Provide a regular expression for parsing the response body from the backend server. The system treats a blank entry here as the value ".*".

  **Note:**
  Health checks require all fields to match. Your status code and response body both must match, as specified.

6. Click **Save**.

**Common Side effects of health check misconfiguration**

The following are common side effects of health check misconfiguration, and can be used to troubleshoot issues.

- **Wrong Port**
  In this scenario, all of the backend servers report as unhealthy. If the backend servers do not have any problems, you may have made a mistake setting the port it needs to be a port that matches a port that is listening and has allowed traffic on the backend.

  OCI Logging Error: \texttt{errno}="EHOSTUNREACH", \texttt{syscall}="connect".

- **Wrong Path**
  In this scenario, all of the backend servers report as unhealthy. If the backend servers do not have any problems, you may have made a mistake setting the path for the HTTP health check it needs to match a an actual application
on the backend. In this scenario you can use a curl test from a system in the same network. ex: $ curl -i http://10.0.0.5/health

You will receive the configured status code in the response OCI Logging Error: "msg":"invalid statusCode","statusCode":404,"expected":"200".

• Wrong Protocol

In this scenario, all of the backend servers report as unhealthy. If the backend servers do not have any problems, you may have made a mistake setting the protocol it needs to match the protocol that is listening on the backend. For example: We only support TCP and HTTP health checks. If your backend is using HTTPS then you would need to use TCP as the protocol.

OCI Logging Error: "code":"EPROTO","errno":"EPROTO".

• Wrong Status Code

In this scenario, all of the backend servers report as unhealthy. If the backend servers do not have any problems, for a HTTP health check you may have made a mistake setting the status code to match the actual status code being returned from the backend. A common scenario is when a backend is returning a 302 and you are expecting a 200. This is likely the backend sending you to a login page or another location on the server. In this scenario you can either fix the backend to return the expected code or use 302 in your health check config.

OCI Logging Error: "msg":"invalid statusCode","statusCode":XX,"expected":"200" where XX to be the status code that is returned.

• Wrong Regex Pattern

All the backend servers report as unhealthy. If the backend servers do not have any problems, you may have made a mistake setting an incorrect regex pattern consistent with the body, or the backend is not returning the expected body. In this scenario you can either change the backend to match the pattern or correct the pattern to match the backend. The following are some specific pattern examples.

• Any Content - ".*"
• A page returning the value "Status:OK:" - "Status:OK:.*"
• OCI Logging Error: "response match result: failed"

• Misconfigured Network Security Groups, Security Lists or Local Firewall

All or some of the backend servers report as unhealthy. If the backend servers do not have any problems, you may have made a mistake configuring either the NSGs, Security Lists, or local firewalls such as firewalld, iptables, or SELinux. In this scenario you can use a curl or netcat test from a system that belongs to the same subnet and NSG as your LBaaS instance HTTP: ex: $ curl -i http://10.0.0.5/health TCP: ex: nc -zvw3 10.0.05 443.

You can check your local firewall by using the following command: firewall-cmd --list-all --zone=public. If your firewall is missing the expected rules you can use a command set like this to add the service: (this example is for HTTP port 80):

• firewall-cmd --zone=public --add-service=http
• firewall-cmd --zone=public --permanent --add-service=http

Creating a custom health check page

In many scenarios you may want to expose your own custom health check page to do a more thorough check. One example scenario is to use the flask application as in the example below rather than relying on your existing application.https://pypi.org/project/py-healthcheck/

import tornado.web
from healthcheck import TornadoHandler, HealthCheck, EnvironmentDump

# add your own check function to the healthcheck

def redis_available():
  client = _redis_client()
info = client.info()
return True, "Redis Test Pass"

health = HealthCheck(checkers=[redis_available])
app = tornado.web.Application([
    ("/healthcheck", TornadoHandler, dict(checker=health)),
])

In the above example the test page is doing more than just making sure the HTTP application is listening. This example checks for a redis client and waits for a response to make sure the full application is healthy before returning a 200 OK. Some other command examples would be to check for disk space or the availability of an upstream dependency. In your health check configuration you would specify the following:

- /healthcheck as your path
- flask default 5000 as port
- 200 as status code

**Editing Health Check Policies**

You create your health check tests when you [create a backend set](#).

**To edit an existing health check policy**

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer’s name.
3. In the **Resources** menu, click **Backend Sets**, and then click the name of the backend set you want to modify.
4. Click **Update Health Check**.
5. In the **Health Check** section, specify the test parameters to confirm the health of backend servers.

   **Tip:**
   
   All parameters are required when updating an existing health check policy.

   - **Protocol:** Required. Specify the protocol to use, either HTTP or TCP.

     **Important:**
     
     Configure your health check protocol to match your application or service.

   - **Port:** Required. Specify the backend server port against which to run the health check.

     **Tip:**
     
     You can enter the value '0' to have the health check use the backend server's traffic port.

   - **URL Path (URI):** (HTTP only) Required. Specify a URL endpoint against which to run the health check.

     **Important:**
     
     Enter a timeout value that is smaller than the interval value to ensure the health check works correctly.

   - **Interval in ms:** Required. Specify how frequently to run the health check, in milliseconds. Default is 10000 (10 seconds).

   - **Timeout in ms:** Required. Specify the maximum time in milliseconds to wait for a reply to a health check. A health check is successful only if a reply returns within this timeout period. Default is 3000 (3 seconds).

   **Important:**
   
   Enter a timeout value that is smaller than the interval value to ensure the health check works correctly.

   - **Number of retries:** Required. Specify the number of retries to attempt before a backend server is considered "unhealthy." This number also applies when recovering a server to the "healthy" state. Default is 3.

   - **Status Code:** (HTTP only) Required. Specify the status code a healthy backend server must return.

   - **Response Body Regex:** (HTTP only) Optional. Provide a regular expression for parsing the response body from the backend server. The system treats a blank entry here as the value ".*".

   **Tip:**
   
   Health checks require all fields to match. Your status code and response body both must match, as specified.

6. Click **Save**.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use this API operation to edit a backend set's health check policy:

   UpdateBackendSet

Use these API operations to retrieve health status information:

- GetBackendHealth
- GetBackendSetHealth
- GetLoadBalancerHealth
- ListLoadBalancerHealths

**Viewing the State of a Work Request**

This topic describes how to view the state of work requests associated with a given load balancer.
Load Balancing

**Note:**

The Load Balancing service does not use the common Work Requests API to support work request operations. Instead, Load Balancing work requests are supported by the Load Balancing API. See Using the Console to View Work Requests on page 260 for information on viewing work requests for other services.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: For a typical policy that gives access to load balancers and their components, see Let network admins manage load balancers on page 2143.

Also, be aware that a policy statement with inspect load-balancers gives the specified group the ability to see all information about the load balancers. For more information, see Details for Load Balancing on page 2292.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Monitoring Work Requests**

Many of the Oracle Cloud Infrastructure Load Balancing service requests do not take effect immediately. In these cases, the request spawns an asynchronous workflow for fulfillment. To provide visibility for in-progress workflows, the Load Balancing service creates a work request object. Because some operations depend on the completion of other operations, you must monitor each operation’s work request and confirm it has succeeded before proceeding to the next operation. For example, if you want to create a backend set and add a backend server to the new set, you first must create the backend set. After that operation completes, you can add the backend server. If you try to add a backend server before the backend set creation completes, the system cannot ensure that the request to add the server succeeds. You can monitor the request to add a backend set to determine when that workflow is complete, and then add the backend server.

The work request states are:

- **ACCEPTED**
  
  The request is in the work request queue to be processed.

- **IN PROGRESS**
  
  A work request record exists for the specified request, but there is no associated WORK_COMPLETED record.

- **SUCCEEDED**
  
  A work request record exists for this request and an associated WORK_COMPLETED record has the state SUCCEEDED.

- **FAILED**
  
  A work request record exists for this request and an associated WORK_COMPLETED record has the state FAILED.

**Using the Console**

The Oracle Cloud Infrastructure Console consumes the REST API and is subject to the same considerations as any Oracle Cloud Infrastructure client. You can view the state of a load balancing work request in the Console:

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Click the name of the **Compartment** that contains the load balancer you want to review, and then click the load balancer's name.

3. In the **Resources** menu, click **Work Requests**. The status of all work requests appears on the page.

**Using the API**

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use these operations to monitor the state of work requests:

- **ListWorkRequests**
- **GetWorkRequest**

**Load Balancing Metrics**

You can monitor the health, capacity, and performance of your load balancers by using **metrics**, **alarms**, and **notifications**.

This topic describes the metrics emitted by the Load Balancing service in the **oci_lbaas** metric namespace.

Resources: Load balancers, listeners, and backend sets.

**Overview of the Load Balancing Service Metrics**

Your load balancer acts as an intermediary for data traffic between clients and your application servers. Clients send requests to your load balancer and the load balancer distributes the requests to your backend servers according to rules you establish. See the diagram in **Overview of Load Balancing** on page 2480 for a high-level view of a simple public load balancing system configuration.

The Load Balancing service metrics help you measure the number and type of connections, and quantity of data managed by your load balancer. You can use metrics data to diagnose and troubleshoot load balancer and client issues. The metrics also help you analyze the HTTP responses returned by the servers in your backend set.

To view a default set of metrics charts in the Console, navigate to the load balancer or backend set you're interested in, and then click **Metrics**. You also can use the Monitoring service to create **custom queries**.

**Prerequisites**

- **IAM policies**: To monitor resources, you must be given the required type of access in a **policy** written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which **compartment** you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or **Notifications**.
- The metrics listed on this page are automatically available for any load balancer, listener, and backend set you create. You do not need to enable monitoring on the resource to get these metrics.

**Available Metrics: oci_lbaas**

Load Balancing service metrics include the following **dimensions**:

**AVAILABILITYDOMAIN**

The **availability domain** in which the load balancer resides.

**BACKENDSETNAME**

The name of the backend set to which the metrics apply.
**LBCOMPONENT**

The load balancer component to which the metrics apply.

Valid metrics for the Load Balancing service vary among the three `lbComponent` dimension values:

- **Backendset**
- **Listener**
- **Loadbalancer**

The tables on this page describe which data is valid for each of these dimension values. If you choose a metric that does not apply to the specified dimension value, the metric returns no data.

**LBHOSTID**

A unique ID that represents the current load balancer host. This ID is subject to change.

**LISTENERNAME**

The name of the listener to which the metrics apply.

**REGION**

The `region` in which the load balancer resides.

**RESOURCEID**

The `OCID` of the resource to which the metrics apply.

### Metrics for the `lbComponent` Dimension Value "Backendset"

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveConnections</td>
<td>Active Connections</td>
<td>count</td>
<td>The number of active connections from the load balancer to all backend servers.</td>
<td>availabilityDomain backendSetName lbComponent lbHostId region resourceId</td>
</tr>
<tr>
<td>BackendServers</td>
<td>Backend Servers</td>
<td>count</td>
<td>The number of backend servers in the backend set.</td>
<td></td>
</tr>
<tr>
<td>BackendTimeouts</td>
<td>Backend Timeouts</td>
<td>count</td>
<td>The number of timeouts across all backend servers.</td>
<td></td>
</tr>
<tr>
<td>BytesReceived</td>
<td>Bytes Received</td>
<td>bytes</td>
<td>The number of bytes received across all backend servers.</td>
<td></td>
</tr>
<tr>
<td>BytesSent</td>
<td>Bytes Sent</td>
<td>bytes</td>
<td>The number of bytes sent across all backend servers.</td>
<td></td>
</tr>
<tr>
<td>ClosedConnections</td>
<td>Closed Connections</td>
<td>count</td>
<td>The number of connections closed between the load balancer and backend servers.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>HttpRequests</td>
<td>Inbound Requests</td>
<td>count</td>
<td>The number of incoming client requests to the backend set.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses</td>
<td>Responses</td>
<td>count</td>
<td>The number of HTTP responses across all backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses200 Responses</td>
<td>HTTP 200 Responses</td>
<td>count</td>
<td>The number of HTTP 200 responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses2xx Responses</td>
<td>HTTP 2xx Responses</td>
<td>count</td>
<td>The number of HTTP 2xx responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses3xx Responses</td>
<td>HTTP 3xx Responses</td>
<td>count</td>
<td>The number of HTTP 3xx responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses4xx Responses</td>
<td>HTTP 4xx Responses</td>
<td>count</td>
<td>The number of HTTP 4xx responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses502 Responses</td>
<td>HTTP 502 Responses</td>
<td>count</td>
<td>The number of HTTP 502 responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses504 Responses</td>
<td>HTTP 504 Responses</td>
<td>count</td>
<td>The number of HTTP 504 responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses5xx Responses</td>
<td>HTTP 5xx Responses</td>
<td>count</td>
<td>The number of HTTP 5xx responses received from backend servers.</td>
<td></td>
</tr>
<tr>
<td>InvalidHeaderResponses</td>
<td>Invalid Header</td>
<td>count</td>
<td>The number of invalid header responses across all backend servers.</td>
<td></td>
</tr>
<tr>
<td>KeepAliveConnections</td>
<td>Keep alive Connections</td>
<td>count</td>
<td>The number of keep-alive connections.</td>
<td></td>
</tr>
</tbody>
</table>
### Load Balancing

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResponseTimeFirstByte</td>
<td>Average Response Time (TCP only)</td>
<td>ms</td>
<td>Average time to the first byte of response from backend servers. TCP only.</td>
<td></td>
</tr>
<tr>
<td>ResponseTimeHttpHeader</td>
<td>Average Response Time (HTTP only)</td>
<td>ms</td>
<td>Average response time of backend servers. HTTP only.</td>
<td></td>
</tr>
<tr>
<td>UnhealthyBackendServers</td>
<td>Unhealthy Backend Servers</td>
<td>count</td>
<td>The number of unhealthy backend servers in the backend set.</td>
<td></td>
</tr>
</tbody>
</table>

### Metrics for the `lbComponent` Dimension Value "Loadbalancer"

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcceptedConnections</td>
<td>Accepted Connections</td>
<td>count</td>
<td>The number of connections accepted by the load balancer.</td>
<td>availabilityDomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>lbComponent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>lbHostId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceId</td>
</tr>
<tr>
<td>ActiveConnections</td>
<td>Active Connections</td>
<td>count</td>
<td>The number of active connections from clients to the load balancer.</td>
<td></td>
</tr>
<tr>
<td>ActiveSSLConnections</td>
<td>Active SSL Connections</td>
<td>count</td>
<td>The number of active SSL connections.</td>
<td></td>
</tr>
<tr>
<td>BytesReceived</td>
<td>Bytes Received</td>
<td>bytes</td>
<td>The number of bytes received by the load balancer.</td>
<td></td>
</tr>
<tr>
<td>BytesSent</td>
<td>Bytes Sent</td>
<td>bytes</td>
<td>The number of bytes sent by the load balancer.</td>
<td></td>
</tr>
<tr>
<td>FailedSSLClientCertVerifications</td>
<td>Failed Client SSL Cert Verifications</td>
<td>count</td>
<td>The number of failed client SSL certificate verifications.</td>
<td></td>
</tr>
<tr>
<td>FailedSSLHandshakes</td>
<td>Failed SSL Handshakes</td>
<td>count</td>
<td>The number of failed SSL handshakes.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------</td>
<td>------</td>
<td>-----------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>HandledConnections</td>
<td>count</td>
<td></td>
<td>The number of connections handled by the load balancer.</td>
<td></td>
</tr>
<tr>
<td>HttpRequests</td>
<td>Inbound Requests</td>
<td>count</td>
<td>The number of incoming client requests to the load balancer.</td>
<td></td>
</tr>
</tbody>
</table>

**Metrics for the lbComponent Dimension Value "Listener"**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>HttpResponses200</td>
<td>HTTP 200 Responses</td>
<td>count</td>
<td>The number of HTTP 200 responses received from backend sets.</td>
<td>availabilityDomain lbComponent lbHostId</td>
</tr>
<tr>
<td>HttpResponses2xx</td>
<td>HTTP 2xx Responses</td>
<td>count</td>
<td>The number of HTTP 2xx responses received from backend sets.</td>
<td>listenerName region resourceId</td>
</tr>
<tr>
<td>HttpResponses3xx</td>
<td>HTTP 3xx Responses</td>
<td>count</td>
<td>The number of HTTP 3xx responses received from backend sets.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses4xx</td>
<td>HTTP 4xx Responses</td>
<td>count</td>
<td>The number of HTTP 4xx responses received from backend sets.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses502</td>
<td>HTTP 502 Responses</td>
<td>count</td>
<td>The number of HTTP 502 responses received from backend sets.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses504</td>
<td>HTTP 504 Responses</td>
<td>count</td>
<td>The number of HTTP 504 responses received from backend sets.</td>
<td></td>
</tr>
<tr>
<td>HttpResponses5xx</td>
<td>HTTP 5xx Responses</td>
<td>count</td>
<td>The number of HTTP 5xx responses received from backend sets.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>HttpResponses</td>
<td>Responses</td>
<td>count</td>
<td>The number of incoming responses received from backend sets.</td>
<td></td>
</tr>
</tbody>
</table>

Using the Console

To view default metric charts for a single load balancer

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Choose the **Compartment** that contains the load balancer you want to view, and then click the load balancer's name.
3. In the **Resources** menu, click **Metrics** (if necessary).

   The **Metrics** page displays a default set of charts for the current load balancer.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

To view default metric charts for multiple load balancers

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. For **Metric Namespace**, select **oci_lbaas**.

   The **Service Metrics** page displays a default set of charts for the selected metric namespace. For more information about the emitted metrics, see the foregoing table. You can also use the **Monitoring service** to create **custom queries**.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

Using the API

Use the following APIs for monitoring:

- **Monitoring API** for metrics and alarms
- **Notifications API** for notifications (used with alarms)
Chapter 23

Logging

This chapter explains how to use Oracle Cloud Infrastructure Logging.

Logging Overview

The Oracle Cloud Infrastructure Logging service is a highly scalable and fully managed single pane of glass for all the logs in your tenancy. Logging provides access to logs from Oracle Cloud Infrastructure resources. These logs include critical diagnostic information that describes how resources are performing and being accessed.

How Logging Works

Use Logging to enable, manage, and search logs. The three kinds of logs are the following:

- **Audit logs**: Logs related to events emitted by the Oracle Cloud Infrastructure Audit service. These logs are available from the Logging Audit page, or are searchable on the Search page alongside the rest of your logs.
- **Service logs**: Emitted by OCI native services, such as API Gateway, Events, Functions, Load Balancing, Object Storage, and VCN Flow Logs. Each of these supported services has pre-defined logging categories that you can enable or disable on your respective resources.
- **Custom logs**: Logs that contain diagnostic information from custom applications, other cloud providers, or an on-premise environment. Custom logs can be ingested through the API, or by configuring the Unified Monitoring Agent. You can configure an OCI Compute instance/resource to directly upload Custom Logs through the Unified Monitoring Agent. Custom logs are supported in both a virtual machine and bare metal scenario.

A log is a first-class Oracle Cloud Infrastructure resource that stores and captures log events collected in a given context. For example, if you enable Flow Logs on a subnet, it has its own dedicated log. Each log has an OCID and is stored in a log group. A log group is a collection of logs stored in a compartment. Logs and log groups are searchable, actionable, and transportable.

To get started, enable a log for a resource. Services provide log categories for the different types of logs available for resources. For example, the Object Storage service supports the following log categories for storage buckets: read and write access events. Read access events capture download events, while write access events capture write events. Each service can have different log categories for resources. The log categories for one service have no relationship to the log categories of another service. As a result, the Functions service uses different log categories than the Object Storage service.

When you enable a log, you must add it to a log group that you create. Log groups are logical containers for logs. Use log groups to organize and streamline management of logs by applying IAM policy or grouping logs for analysis. For more information, see Managing Logs and Log Groups on page 2577.

Logs are indexed in the system, and searchable through the Console, API, and CLI. You can view and search logs on the Logging Search page. When searching logs, you can correlate across many logs simultaneously. For example, you can view results from multiple logs, multiple log groups, or even an entire compartment with one query. You can filter, aggregate, and visualize your logs. For more information, see Searching Logs on page 2634.
Note:
Logs are encrypted in the OCI system during storage, but they are not encrypted when returned to the customer.

After you enable a log, log entries begin to appear on the detail page for the log (see Enabling Logging for a Resource on page 2591 for more information). If you need more archiving support, you can use Service Connector Hub (archiving to object storage, write to stream, and so on). For more information on service logs, see Service Log Reference on page 2593, and Service Connector Hub Overview on page 3750.

Note:
You can view usage report detail for Logging by accessing Cost and Usage Reports.

Logging APIs

Oracle Cloud Infrastructure Logging has the following APIs available:

- Logging Management API
- Logging Ingestion API
- Logging Search API

Also see Using the (Logging Management) API, Using the (Logging Ingestion) API for custom logs, and Using the (Logging Search) API for more information on logging operations specific to each API.

Logging Concepts

The following concepts are essential to working with Logging.

Service Logs

Critical diagnostic information from supported Oracle Cloud Infrastructure services. See Supported Services on page 2591.

Custom Logs

Diagnostic information from custom applications, other cloud providers, or an on-premise environment. To ingest custom logs, call the API directly or configure the unified monitoring agent.

Audit Logs

Read-only logs from the Audit service, provided for you to analyze and search. Audit logs capture the information about API calls made to public endpoints throughout your tenancy. These include API calls made by the Console, Command Line Interface (CLI), Software Development Kits (SDK), your own custom clients, or other Oracle Cloud Infrastructure services.

Log Groups

Log groups are logical containers for logs. Use log groups to streamline log management, including applying IAM policy or searching sets of logs. You can move log groups from one compartment to another and all the logs contained in the log group moves with it.

Service Log Category

Services provide log categories for the different types of logs available for resources. For example, the Object Storage service supports the following log categories for storage buckets: read and write access events. Read access events capture download events, while write access events capture write events. Each service can have different log categories for resources. The log categories for one service have no relationship to the log categories of another service.
**Service Connector Hub**

Service Connector Hub moves logging data to other services in Oracle Cloud Infrastructure. For example, use Service Connector Hub to alarm on log data, send log data to databases, and archive log data to Object Storage. For more information, see Service Connector Hub Overview on page 3750.

**Unified Monitoring Agent**

The fluentd-based agent that runs on customer machines (OCI instances), to help customers ingest custom logs.

**Agent Configuration**

A configuration of the Unified Monitoring Agent that specifies how custom logs are ingested.

**Limits on Logging**

In your tenancy, you can create a maximum of:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs</td>
<td>500 logs per tenancy</td>
</tr>
<tr>
<td>Log groups</td>
<td>100 log groups per tenancy</td>
</tr>
</tbody>
</table>

For more information on extra Logging resource limits, see Logging Limits on page 226. See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For administrators: Use the following topics to find examples of IAM policy for Logging:
Managing Logs and Log Groups

This topic describes how to manage logs and log groups.

Overview of Logs and Log Groups

Logs contain critical diagnostic information that tells you how your resources are performing and being accessed. You can enable logging on supported resources. To see a list of supported resources grouped by service, see Supported Services on page 2591.

Log groups are logical containers for organizing logs. Logs must always be inside log groups. You must create a log group to enable a log.

Use log groups to limit access to sensitive logs with IAM policy. With log groups, you don't have to rely on complex compartment hierarchies to secure your logs. For example, say the default log group in a single compartment is where you store logs for the entire tenancy. You grant access to the compartment for log administrators with IAM policy as you normally would. However, let's say some projects contain personally identifiable information (PII) and those logs can only be viewed by a select group of log administrators. Log groups allow you to put logs that contain PII into a separate log group, and then use IAM policy to restrict access to all but a few log administrators.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

Administrators: for policy samples specific to logs and log groups, see Required Permissions for Working with Logs and Log Groups on page 2577.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to know more about writing policies for Logging, see Details for Logging on page 2294.

Required Permissions for Working with Logs and Log Groups

To enable service logs in a resource, a user must be granted manage access on the log group and access to the resource. In general, inspect access on the resource is enough, but check for specific resources. Inspect access provides permission to update the resource and permission for the log group that contains the log.

Logs and log groups use the log-group resource-type, but to search the contents of logs you must use a different resource-type.
Managing log groups and log objects

To manage groups or objects, use verbs for log-groups:

- Allow group A to use log-groups in compartment C
- Allow group B to manage log-groups in compartment C
- Allow group D to read log-groups in compartment C

This allows users in group A to create, update, or delete log groups and log objects in compartment C.

To provision agent configurations

Three different types of access are needed:

1. Access to operate on configurations.
2. Access to operate on log groups.
3. Inspect capabilities on dynamic groups or groups.

To have access to configurations, the policy must be:

- Allow group B to use unified-configuration in compartment X

To create, update, or delete custom logs used as a destination in a configuration

This policy allows users in compartment B to create, update, or delete configurations in compartment X.

To provide a destination for the logs incoming from the configuration, you need log-groups access:

- Allow group B to use log-groups in compartment X

To assign a configuration to a set of instances

To assign a configuration to a set of instances, you need inspect access to the dynamic group or group that identifies the instances:

- Allow group B (IDENTITY_DYNAMIC_GROUP_INSPECT) in tenancy
- Allow group B (IDENTITY_GROUP_INSPECT) in tenancy

Enable instances to push logs into the Logging service

To allow instances to push logs, the instances need to have access to get a configuration and push the logs. log-content controls this permission (where X is the compartment where the configurations are located):

- Allow dynamic-group production-fleet to use log-content in compartment X

To view logs

To view logs in the Console (Search), the following is required:

- Allow group Searchers to read log-content in compartment X

Example log search policy

To allow a group to read the contents of indexed logs:

- allow group GroupA to read log-groups in tenancy
- allow group GroupA to read log-content in tenancy

Example policies for logs and log groups

In these examples, policy statements use GroupA as the name of the group.
Logging

To allow a group to view the log groups in the tenancy (or in a compartment), requires `inspect` access:

```
allow group GroupA to inspect log-groups in tenancy
```

To allow a group to read metadata for logs or log groups, requires `read` access:

```
allow group GroupA to read log-groups in tenancy
```

To allow a group to update log groups, or the logs in them, requires `use` access:

```
allow group GroupA to use log-groups in tenancy
```

To enable a log on a resource (or to create and delete log groups and the logs in them), requires `manage` access:

```
allow group GroupA to manage log-groups in tenancy
```

To allow usage of a specific log group or groups, use a `where` clause with the `target.loggroup.id` variable. For example:

```
Allow group GroupA to manage loggroups in tenancy where target.loggroup.id='ocid1.loggroup.oc1.phx.<uniqueID>'
```

To specify multiple log groups:

```
Allow group GroupA to manage log-groups in tenancy where any {target.loggroup.id='ocid1.loggroup'}
```

**Custom logs**

For **custom logs** the following is required. This policy is needed to allow the user to search logs through the Console **Search** page:

```
allow group userGroup1 to read log-content in compartment c
```

**Note:**

Even though this policy is described for usage with custom logs, the policy is also true for all logs. `LOG_CONTENT_READ` allows reading logs from both custom and OCI service logs. It is identical in behavior to this policy:

```
allow group GroupA to read log-content in tenancy
```

The following is needed for the agent that uses the instance principal on the virtual machine to send logs:

```
allow dynamicGroup1 to use log-content in compartment c
```

**Note:**

If a user group is being used instead of a dynamic group for pushing custom logs, replace the dynamic group name with the user group name in these policies.

For custom logs, if you use `allow group dynamicGroup1 to use log-content in compartment c`, the instances in that dynamic group get permission to download the configuration, send logs, and can search logs.

**IAM Policy Requirements for Resources**

In addition to the permissions to work with the log group, to add service logs to a resource you must have the `update` permission for the resource. For many resources, the update permission is granted with the `use` verb. For example, users who can `use` buckets in CompartmentA, can also enable logging on a bucket in CompartmentA.
However, some resources don’t include permission to update a resource with the `use` verb. For example, to update a rule for the Events service, you must have the full `manage` permission. To enable a log on an Events rule (or any other resource that doesn't include the update permission with the `use` verb), you must have the `manage` permission.

To allow a group to enable logging for these resources, without granting the full permissions of `manage`, you can add a policy statement to grant only the `<RESOURCE>_UPDATE` permission (or, in the case of the Events service, `<RESOURCE>_MODIFY`) from the `manage` verb. For example, to allow a group EventUsers to enable logs on Events rules in CompartmentA, you could write a policy like the following:

```
Allow group EventUsers to read cloudevents-rules in compartment CompartmentA
Allow group EventUsers to manage cloudevents-rules in compartment CompartmentA
  where request.permission='EVENTRULE_MODIFY'
```

For information about resource permissions, see Policy Reference on page 2167.

**VCN Flow Logs IAM Policy**

In addition to Required Permissions for Working with Logs and Log Groups on page 2577, subnet read and update permissions are required for managing VCN Flow Logs.

To provide subnet permissions, use one of the following policies, listed in order from broader to narrowed privileges:

```
Allow group FlowLogsEnablers to manage virtual-network-family in tenancy
```

Or:

```
Allow group FlowLogsEnablers to manage subnets in tenancy
```

Or:

```
Allow group FlowLogsEnablers to {SUBNET_READ, SUBNET_UPDATE} in tenancy
```

This group is similar to what is described for EventUsers in IAM Policy Requirements for Resources on page 2579.

**Example Scenario**

Your company has an Operations department. Within the Operations department are several costs centers. You want to be able to tag resources that belong to the Operations department with the appropriate cost center.

1. Create a log group called "confidential". Avoid entering confidential information.
2. Add logs with sensitive data to the "confidential" log group.

An employee named Alice already belongs to the group BucketManagers. Alice can manage buckets in CompartmentA. You want Alice and other members of BucketManagers group to be able to enable logs on buckets in CompartmentA.

To grant the BucketManagers group access to the sensitive data log group (and only the sensitive data log group), add the following statements to the BucketManagers policy:

```
Allow group BucketManagers to manage log-groups in compartment CompartmentA
  where target.loggroups.id='ocid1.lumloggroup.oc1.phx.<uniqueID>'
```

Alice can now enable logs to bucket resources in CompartmentA.

**Move Log Groups to a Different Compartment**

You can move log groups from one compartment to another. When you move a log group to a new compartment, all the logs in the log group move with the log group to the new compartment. After you move the log group to the new compartment, the policies in the new compartment apply immediately, and affect access to the log group and any logs the log group contains.
Logging

For more information, see Moving Resources to a Different Compartment on page 2433.

Log and Log Group Names

For log group names, the first character must start with a letter. Otherwise, the following guidelines apply to both log and log group names:

• Use from 1 to 256 characters.
• Valid characters are letters (upper or lower case), numbers, hyphens, underscores, and periods.
• Log and log group names are case-sensitive. Logging handles write-log and WRITE-log as separate logs.
• Avoid entering confidential information.

Legacy Archival

Legacy automatic log archival was previously available before general release. This is a toggle configurable for every log. If enabled, it automatically creates a bucket in your compartment, and places a copy of your log there. New and improved functionality is now available in Service Connector Hub.

Using the Console

The Logs table lists both custom logs and service logs (indicated by the Log type field). The table is organized in terms of the following fields:

• Log name
• Log type
• Status
• Details
• Created

From this page you can click the Log name entry to go to the Log details page, or click the linked resource in Details to go directly to the resource. For example, if the log is for the Load Balancer service, clicking the link opens the Load Balancer Details page. From the action menu, you can edit the log, disable logging, change the log group, view tags, or delete the log.

To view the contents of logs

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Logs.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. Under **Log name**, click the name of the log you want to view. The log detail page opens. This page displays the following on the **Log Information** tab:

- **OCID**
- **Compartment**
- **Log Group** (click to view the log group contents)
- **Created** date and time in UTC format
- **Retention Period**

  **Note:**
  
  Retention period can be set in 30-day increments, up to a maximum of 180 days.

- **Legacy Archival** mode
- **Status** (Creating, Active, Updating, Inactive, Deleting, Deleted)
- The **Tags** tab shows associated tags for this log.
- Under **Log Details**, following is displayed: the **Log Type** (whether Service or Custom), **Service** (for service logs), **Log Category**, and **Resource** (click to view the linked resource).

  In the Explore Log resource, log data is displayed in a similar manner as the **Log Data** on the **Search** page. You can apply some simple filters, such as sorting by newest or oldest from the **Sort** field, or filtering by time from the corresponding **Filter by Time** field.

4. Click **Explore with Log Search**, which allows you to view this log on the **Search** page directly. After clicking this link, the Search page opens with the **Select Logs to Search** field populated with the log in the filter settings. At this point, you can perform more analysis and investigation related to this log directly on the **Search** page. For more information, see Searching Logs on page 2634.

  In addition to these functions in the Explore Log resource, you can also click the Metrics resource to view interactive charts for either a chosen time period (**Start Time** and **End Time**), or pre-selected ranges from **Quick Selects**. The charts display the **Bytes Ingested** (total bytes of log entries ingested) and the **Search Success** (number of successful search queries issued by the user).

  Clicking anywhere in a chart displays a larger version of the chart. You can perform several chart actions from the Options menu (both in the Metrics resource and in the zoomed-in view):

  - **View Query in Metrics Explorer**: Opens the chart in the Monitoring Metrics Explorer. See Metrics Explorer page on page 2684 for more information.
  - **Copy Chart URL**
  - **Copy Query (MQL)**
  - **Create an Alarm on this Query**: Opens the Monitoring Create Alarm page. See To create an alarm on page 2719 for more information.
  - **Table View**: Displays a tabular summary of the chart data. Select **Chart View** to switch back to the chart.

**To edit the name of a log**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Logs**.
2. Under **List Scope, Compartment**, choose a compartment you have permission to work in.
3. Under **Log name**, click the name of the log you want to view. The log detail page opens.
4. Click **Edit**. The **Edit Log** panel is displayed. This panel indicates the resource, and allows you to change the log name in the associated field under **Configure Log**. You can also enable or disable the **Enable Legacy Archival Logs** setting (see Legacy Archival on page 2581). Avoid entering confidential information.

  From the main **Logs** page, for the log you want to edit, you can also click the the Actions icon (three dots), and then click **Edit** to access the **Edit Log** panel.
5. Make your changes and click **Save Changes**.
To delete a log

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Logs.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. Under Log name, click the name of the log you want to view. The log detail page opens.
4. Click Delete. A confirmation dialog is displayed regarding the delete operation.
5. Confirm by clicking Delete.

From the main Logs page, for the log you want to delete, you can also click the the Actions icon (three dots), and then click Delete.

To move a log to a new log group

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Logs.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. Under Log name, click the name of the log you want to view. The log detail page opens.
4. Click Change Log Group. The Move to a Different Log Group dialog is displayed.
5. From the Choose New Group list, select the new group from the list, and click Change Log Group. The new log group membership is reflected on the Log Information tab's Log Group field.

From the main Logs page, for the log you want to move to a new group, you can also click the the Actions icon (three dots), and then click Change Log Group.

To enable or disable an existing log

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Logs.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. Under Log name, click the name of the log you want to view. The log detail page opens.
4. Click Disable Log/Enable Log. A confirmation dialog is displayed regarding the disabling or enabling of the log.
5. Confirm by clicking Disable Log/Enable Log. The log detail page changes its status and displays Inactive (for a disabled log) or Active (for an enabled log) in the status field, both on the log detail page and the Logs page.

From the main Logs page, for the log you want to enable or disable, you can also click the the Actions icon (three dots), and then click Disable Logging/Enable Logging.

To create a log group

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Log Groups.
2. Choose a compartment you have permission to work in and click Create Log Group. The Create Log Group panel is displayed.
3. Enter the following:
   - Compartment: The compartment in which you want to create the log group. This field is pre-filled based on your compartment choice.
   - Name: A name for this log group. The first character of a log group name must be a letter. For more, see Log and Log Group Names on page 2581. Avoid entering confidential information.
   - Description: A friendly description.
   - Optionally, enter tagging information.
4. Click **Create**. The log group detail page is then displayed. From this page you can:

- Edit the group
- Move resources
- Add tags
- Delete the log group
- View log group information and tags
- View log group resources (explore the log group, view the logs included in the log group, create custom or service logs, and view metrics)

The **Metrics** resource in a log group detail page functions the same as in a log detail page. See **To view the contents of logs** on page 2581 for more information.

**To edit a log group**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Log Groups**.
2. Choose a compartment you have permission to work in and click the linked log group name under **Log Group** in the table. The log group detail page is displayed.
3. Click **Edit**. The **Edit Log Group** panel is displayed. From here, you can change the log group name and its description in the associated fields. Avoid entering confidential information. See **Log and Log Group Names** on page 2581 for more information on naming.

   From the main **Log Groups** page, for the log group you want to edit, you can also click the the Actions icon (three dots), and then click **Edit**.

4. Make your changes and click **Update**.

   **Note:**

   You cannot move, edit, or delete the default log group.

**To delete a log group**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Log Groups**.
2. Choose a compartment you have permission to work in and click the linked log group name under **Log Group** in the table. The log group detail page is displayed.

   **Tip:**

   You cannot delete a log group that contains logs.

3. Click **Delete**. A confirmation dialog is displayed regarding the delete operation.
4. Confirm by clicking **Delete**. The log group is removed from the **Log Groups** page.

   From the main **Log Groups** page, for the log group you want to delete, you can also click the the Actions icon (three dots), and then click **Delete**.

   **Note:**

   You cannot move, edit, or delete the default log group.

**To move a log group to a different compartment**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Log Groups**.
2. Choose a compartment you have permission to work in and click the linked log group name under **Log Group** in the table. The log group detail page is displayed.

3. Click **Move Resource**. The **Move Resource to a Different Compartment** dialog is displayed.
4. Choose the new compartment and then click **Move Resource**.

   From the main **Log Groups** page, for the log group you want to move to a new compartment, you can also click the the Actions icon (three dots), and then click **Move Resource**.
To list the logs in a log group

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Log Groups.
2. Choose a compartment you have permission to work in.
3. For the log group you want to inspect for logs, click the name of the log group under Log Group in the table. The log group detail page is displayed.
4. In Resources, click Logs to display a list of all the logs contained in the log group. This resource table of logs functions in the same manner as the main Logs page.

Create a log group and configure LBaaS access and error logs

This procedure describes how to create a log group and how to configure LBaaS access and error logs.

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Log Groups.
2. Click Create Log Group. Choose the compartment where you want to create the log group. Choose a Name and Description that can properly identify your log group.
3. Click Create.
4. Next, click Logs. The Logs page is displayed.
5. Click Enable Service Log. The Enable Resource Log panel is displayed.
6. Next, enable access logs. Under Select Resource, Resource Compartment, choose a compartment you have permission to work in.
7. Select a service from the Service - Select Load Balancers.
8. Select a resource: in Resource, select a load balancer that you need to troubleshoot.
9. Configure the log: in Log Category, select a log category to specify the type of log to create. For this procedure, select Access Logs In Log Name, and then type a name for the log. In this procedural example, we will name it loadbalancer-access.
10. Click Enable Log.
11. Click Enable Service Log. The Enable Resource Log panel is displayed. Next, we will enable error logs.
12. Under Select Resource, Resource Compartment, choose a compartment you have permission to work in.
13. Select a service from the Service - Select Load Balancers.
14. Select a resource: in Resource, select the load balancer that you need to troubleshoot.
15. Configure the log: in Log Category, select a log category to specify the type of log to create. For this example, select Error Logs In Log Name, and then type a name for the log. For this example, we will name it loadbalancer-error.
16. Click Enable Log.

Using the Command Line Interface (CLI)

For more information on installing the CLI, see Quickstart on page 4195, and logging-ingestion, logging, and logging-search for command documentation.

Agent Configuration Commands

The following are agent configuration-related commands:

To create a unified agent configuration registration

Open a command prompt and run:

```
oci logging agent-configuration create --compartment-id | --compartment_OCID>, --is-enabled <boolean>, --service-configuration <service_configure>
```
To create a unified agent log configuration registration
Open a command prompt and run:

```
oci logging agent-configuration create-log-configuration --compartment-id | -c <compartment_OCID>, --is-enabled <boolean>
```

To get a unified agent configuration for an ID
Open a command prompt and run:

```
oci logging agent-configuration get --config-id <agent_configuration_OCID>
```

To list all agent configurations in the specified compartment
Open a command prompt and run:

```
oci logging agent-configuration list --compartment-id | -c <compartment_OCID>
```

To update an existing unified agent configuration
Open a command prompt and run:

```
oci logging agent-configuration update --config-id <agent_configuration_OCI>, --display-name <configuration_name>, --is-enabled <Boolean>, --service-configuration <service_configure>
```

This call fails if the log group does not exist.

To update an existing unified agent log configuration
Open a command prompt and run:

```
oci logging agent-configuration update-log-configuration --config-id <agent_configuration_OCI>, --display-name <configuration_name>, --is-enabled <Boolean>
```

This call fails if the log group does not exist.

To move a unified agent configuration into a different compartment within the same tenancy
Open a command prompt and run:

```
oci logging agent-configuration change-compartment --config-id <agent_configuration_OCID>
```

When provided, the If-Match is checked against the ETag values of the resource. For information about moving resources between compartments, see Moving Resources to a Different Compartment on page 2433.

To delete a unified agent configuration
Open a command prompt and run:

```
oci logging agent-configuration delete --config-id <agent_configuration_OCID>
```

Log Commands
The following are log commands:
Create a log within a specified log group

Open a command prompt and run:

```
oci logging log create --display-name <log_name>, --log-group-id <log_group_OCID>, --log-type <SERVICE_or_CUSTOM>
```

This call fails if the log group has already been created with the same displayName or (service, resource, category) triplet.

Get the log object configuration for the log object OCID

Open a command prompt and run:

```
oci logging log get --log-group-id <log_group_OCID>, --log-id <log_OCID>
```

List the specified log group’s log objects

Open a command prompt and run:

```
oci logging log list --log-group-id <log_group_OCID>
```

Move a log into a different log group within the same tenancy

Open a command prompt and run:

```
oci logging log change-log-group --log-group-id <log_group_OCID>, --log-id <log_OCID>
```

When provided, the If-Match is checked against the ETag values of the resource.

To delete a log object in a log group

If you have an issue with deleting a log object, open a command prompt and run the following command to delete it:

```
oci logging log delete --log-group-id <log_group_OCID>, --log-id <log_OCID>
```

To ingest logs associated with a logId

Open a command prompt and run:

```
oci logging-ingestion put-logs --log-entry-batches, --log-id, --specversion
```

List all services supporting logging

Open a command prompt and run:

```
oci logging service list
```

Update an existing log object with the associated configuration

Open a command prompt and run:

```
oci logging log update --log-group-id <log_group_OCID>, --log-id <log_OCID>
```

This call fails if the log object does not exist.

**Log Group Commands**

The following are log group-related commands:

Create a new log group with a unique display name
Logging

Open a command prompt and run:

```
oci logging log-group create --compartment-id | -c <compartment_OCID>, --display-name <log_group_name>
```

This call fails if the log group is already created with same displayName in the compartment.

**Get a specified log group's information**

Open a command prompt and run:

```
oci logging log-group get --log-group-id <log_group_OCID>
```

**List all log groups for the specified compartment or tenancy**

Open a command prompt and run:

```
oci logging log-group list --compartment-id | -c <compartment_OCID>
```

**Updates an existing log group with the associated configuration**

Open a command prompt and run:

```
oci logging log-group update --log-group-id <log_group_OCID>
```

This call fails if the log group does not exist.

**Move a log group into a different compartment within the same tenancy**

Open a command prompt and run:

```
oci logging log-group change-compartment --log-group-id <log_group_OCID>
```

When provided, the If-Match is checked against the ETag values of the resource. For information about moving resources between compartments, see Moving Resources to a Different Compartment on page 2433.

**To delete a specified log group**

Open a command prompt and run:

```
oci logging log-group delete --log-group-id <log_group_OCID>
```

**Work Request Commands**

The following are work request-related commands:

**Get the details of a work request with a given ID**

Open a command prompt and run:

```
oci logging work-request get --work-request-id <work_request_OCID>
```

**List the work requests in a compartment**

Open a command prompt and run:

```
oci logging work-request list --compartment-id | -c <compartment_OCID>
```

**List the errors for a given work request**
Open a command prompt and run:

```
oci logging work-request-error list --work-request-id <work_request_OCID>
```

**List the logs for a given work request**

Open a command prompt and run:

```
oci logging work-request-log list --work-request-id <work_request_OCID>
```

**Delete a work request that has not yet started**

Open a command prompt and run:

```
oci logging work-request delete --work-request-id <work_request_OCID>
```

---

**Object Storage Example**

The following is an Object Storage example:

**To create a log group and create a log in Object Storage**

Open a command prompt and run:

```
oci logging log-group create --compartment-id <compartment_OCID> --display-name CLITestLogGroup
oci logging log create --display-name object_log_write --log-group-id <log_group_OCID> --log-type SERVICE --is-enabled true --configuration file://~/.oci/objectstorage_configuration.json
```

`objectstorage_configuration.json`:

```json
{
  "archiving": {
    "isEnabled": true
  },
  "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
  "source": [
    {
      "category": "write",
      "parameters": null,
      "resource": "bucket-cli-sample",
      "service": "objectstorage",
      "sourceType": "OCISERVICE"
    }
  ]
}
```

**VCN Flow Logs Example**

The following are sample commands related to VCN Flow Logs:

**To create a log group**

Open a command prompt and run:

```
oci logging log-group create --compartment-id <compartment_OCID> --display-name <log_group_name> --description <description>
```

**To create a flowlogs log object (enable Flow Logs)**
Open a command prompt and run:

```
oci logging log create --display-name <log_display_name> --log-group-id <log_group_OCID>
--description <description> --log-type SERVICE --is-enabled <Boolean>
--configuration file://input.json
```

Sample configuration file:

```json
{
   "compartment-id":"...", # CompartmentId of where the subnet resource is present.
   "source": {
      "resource": "ocid1.subnet.....", # OCID of subnet for which flowlogs is enabled.
      "service": "flowlogs", # "flowlogs" is the official service name and it should be all lowercase.
      "source-type": "OCISERVICE", # OCISERVICE is the name of the Logging source-type.
      "category": "all"
   }
}
```

To disable a flowlogs log object (disable Flow Logs)

Open a command prompt and run:

```
oci logging log update --log-group-id <log_group_OCID> --log-id <log_OCID>
--is-enabled false
```

To delete the log object

Open a command prompt and run:

```
oci logging log delete --log-id <log_OCID>
```

Functions Example

To enable Functions logging

To enable Functions logging, open a command prompt and run:

```
oci logging log create --display-name cli_test --log-group-id ocid1.loggroup.oc1.phx.<log_group_OCID>
--log-type SERVICE --is-enabled true --configuration file://fnconfig.json
```

Sample fnconfig.json configuration file:

```json
{
   "compartment-id":"ocid1.compartment.oc1..<compartment_OCID>" # OCID of the compartment
   "source": {
      "resource": "ocid1.fnapp.oc1.phx.<unique_ID>", # OCID of the function
      "service": "functions",
      "source-type": "OCISERVICE",
      "category": "invoke"
   }
}
```
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage logs:

- ListLogs
- GetLog
- CreateLog
- UpdateLog
- ChangeLogLogGroup
- DeleteLog

Use the following operations to manage log groups:

- ListLogGroups
- GetLogGroup
- CreateLogGroup
- UpdateLogGroup
- ChangeLogGroupCompartment
- DeleteLogGroup

Service Logs

Oracle Cloud Infrastructure services, such as API Gateway, Events, Functions, Load Balancing, Object Storage, and VCN Flow Logs emit service logs. Each of these supported services has a Logs resource that allows you to enable or disable logging for that service.

Supported Services

You can enable service logs for the following Oracle Cloud Infrastructure services:

- API Gateway
- Events
- Functions
- Load Balancers
- Object Storage
- VCN Flow Logs
- VPN Connect

**Note:**

VPN Connect logs are only supported with v2 VPN connections. v1 connections are not supported.

**Note:**

This list of Oracle Cloud Infrastructure services is updated as supported services are added.

Enabling Logging for a Resource

Logs can be enabled in two places: directly on the resource itself, or on the central Logs page. When you enable a log on a specific resource, you specify the category. Different resources can have different categories. For example, rules in the Events Service have the Logs resource available for logging management. The rule can issue a log according to the category listed in the corresponding Category field. On this page, the logs are listed that the resource can create.
Enabling Logging from the Resource page

For Oracle Cloud Infrastructure services that are compatible with Logging, the Logs resource allows you to manage the logs issued by the resource. You can view the following information:

- Category
- Status
- Log name
- Log group

In addition, you can enable or disable logging, edit the log, or delete it (the last two options are available in the action menu). When enabling logging, you also create the log object itself.

For a newly created resource, logging is automatically enabled. For a resource you want to enable logging on, under Resources click Logs, and then toggle Enable Logging. The Create Log panel is displayed, and the entry fields are pre-populated:

- **Compartment** (the same as your resource)
- **Log Group**: The first log group in your compartment. You can select another log group, or create a new group by clicking Create New Group.
- **Log Name**: Pre-populated as the name of your resource and the category, which are combined with an underscore (\<resource\>_\<category\>). For example, if the resource is named "resource" and the category is "ruleexecutionlog", the log name is "resource_ruleexecutionlog".

After logging is enabled, you can click the link under Log name or Log group to view the log details or log group details pages, respectively.

To disable logging, toggle the Enable log control, which displays a disable logging confirmation dialog. Click Disable Log to confirm. The Status field is set to INACTIVE to indicate the inactive status.

When creating a log, a log object is established. To delete the log, select Delete from the action menu. A confirmation is displayed confirming whether you want to delete the log. After clicking Delete, this removes the log object, as opposed to disabling it (which means the log object still exists but does not record new data into it).

Enabling Logging on the Logs page

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Logs. The Logs page is displayed.
2. Click Enable Service Log. The Enable Resource Log panel is displayed.
3. Under Select Resource, Resource Compartment, choose a compartment you have permission to work in.
4. Select a service from the Service list (see Supported Services on page 2591 for the available services).
5. Select a resource:
   - In **Service**, select the service of the resource for which you want to enable the log.
   - In **Resource Compartment**, select the compartment of the resource.

   **Tip:**
   You can type in the list box to perform a filtered search of all compartments in the tenancy.
   - In **Resource** select a resource.

6. Configure the log:
   - In **Log Category** select a log category to specify the type of log to create. For example, Object Storage buckets have categories for read and write. Select read to enable a log with only read events. Select write for a log with only write events.

   You can only have one log for any combination of service, resource, and log category. For example, Object Storage buckets have two categories: read and write. Therefore:
   - You can enable a single read log and a single write log for every bucket in your tenancy.
   - You cannot enable more than two logs (one read and one write) for any one bucket.
   - In **Log Name**, type a name for the log. See Log and Log Group Names on page 2581 for more information. Avoid entering confidential information. Select **Enable Legacy Archival Logs** to automatically create a bucket in your compartment, and place a copy of your log there. See Legacy Archival on page 2581 for more information.

7. To specify the log location (click **Show Advanced Options** if necessary):
   - In **Compartment**, select the compartment for the log.

   **Tip:**
   You can type in the list box to perform a filtered search of all compartments in the tenancy.
   - In **Log Group**, select a log group for the log.

8. In **Log Retention**, select a value from the list:
   - 1 month (the default)
   - 2 months
   - 3 months
   - 4 months
   - 5 months
   - 6 months

9. Apply any tagging-related information in the **Tag Namespace**, **Tag Key**, and **Value** fields.

10. Click **Enable Log**.

    The Log detail page is displayed, and the log is in the process of being created (a "Creating log" message is displayed). See Using the Console on page 2581 for more information on viewing and using this page.

**Service Log Reference**

The overarching logging schema is described in Logging Format Overview on page 2594, while each service that enables logging has its own specific logging details. This reference includes:

- Details for API Gateway on page 2597
- Details for Events
- Details for Functions
Logging Format Overview

Every log line is normalized into a common event format for ease of correlation. This format is based on the JSON implementation of CloudEvents v1.0 specification. A log line has three key sections:

- Unified envelope
- Oracle-specific metadata (oracle.*)
- Contents of the log line (data)

Outer Envelope Format

All messages sent to the ingestion front end use the outer envelope format, and only change the message body based on the log type. The outer envelope format conforms to the CloudEvents v1.0 spec, with extension fields defined for logging purposes. The following table describes this format.

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Position</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification Version</td>
<td>Yes</td>
<td>Body: specversion</td>
<td>String</td>
<td>The version of the CloudEvents specification this message conforms to.</td>
</tr>
<tr>
<td>Id</td>
<td>Yes</td>
<td>Body: id</td>
<td>String</td>
<td>A source-unique identifier for this message. Duplicate messages can have the same ID. Consumers can assume events with the same IDs are unique.</td>
</tr>
</tbody>
</table>
| Type             | Yes      | Body: type     | String  | The type of the message. Consumers use the type and specversion to determine how to interpret the body. Pattern: com.oraclecloud. 
{service}. 
{resource-type}. 
{category}. For example: com.oraclecloud.compute.instance.terminated.  |
<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Position</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Yes</td>
<td>Body: source</td>
<td>URI-reference</td>
<td>The message source. When emitted by a service, refers to the name of the resource that generated the message, for example, the Object Storage bucket name, Instance Name. When emitted by an agent, based on the source/input used to read events. For example, the instance name (not the OCID) or the hostname of the asset in an on-premise environment.</td>
</tr>
<tr>
<td>Subject</td>
<td>No</td>
<td>Body: subject</td>
<td>String</td>
<td>A specific subresource that generated the event, if applicable to the source. This is useful for sources with subresources. Examples:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Object Storage example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Source: my-bucket</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Subject: image.png</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Custom Logging example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Source: hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Subject: /var/log/some.log</td>
</tr>
<tr>
<td>Name</td>
<td>Required</td>
<td>Position</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Time</td>
<td>No</td>
<td>Body: time</td>
<td>Timestamp</td>
<td>The time the message was generated. If present, must adhere to the format specified in RFC 3339. If not provided, the wall clock of the ingestion host that receives the request is used.</td>
</tr>
<tr>
<td>Data Schema</td>
<td>No</td>
<td>Body: dataschema</td>
<td>String</td>
<td>The schema version for the data field. This is not required, and if not provided, is assumed to be the initial version.</td>
</tr>
<tr>
<td>Data Content Type</td>
<td>No</td>
<td>Body: datacontenttype</td>
<td>String</td>
<td>The format in which the message body is encoded. If not provided, the default is JSON (equivalent to datacontenttype: application/json).</td>
</tr>
<tr>
<td>Message Body</td>
<td>Yes</td>
<td>Body: data</td>
<td>Object</td>
<td>The message body encoded in the format defined by datacontenttype. If datacontenttype is not specified, this is expected to be JSON (equivalent to datacontenttype: application/json).</td>
</tr>
<tr>
<td>Oracle Cloud Metadata</td>
<td>Yes</td>
<td>Body: oracle</td>
<td>Object</td>
<td>More Oracle-specific metadata is provided in a map of attributes at the top level of the envelope. This conforms to CloudEvents v1 Attribute Extensions specification. See the following table for supported Oracle Cloud Infrastructure metadata attributes.</td>
</tr>
</tbody>
</table>
Oracle Metadata Attributes

The following attributes are supported in the **oci** extension field of the message format. Naming for these attributes conforms to the CloudEvents v1 Attribute Naming Convention, that is, they are lowercase alpha-numeric identifiers fewer than 20 characters long.

<table>
<thead>
<tr>
<th>Name</th>
<th>Required for Ingestion</th>
<th>Enriched for Retrieval</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logid</td>
<td>Yes</td>
<td>-</td>
<td>String</td>
<td>The OCID of the log object the message was sent to.</td>
</tr>
<tr>
<td>loggroupid</td>
<td>No</td>
<td>Yes</td>
<td>String</td>
<td>The OCID of the log group the object resides in.</td>
</tr>
<tr>
<td>tenantid</td>
<td>No</td>
<td>Yes</td>
<td>String</td>
<td>The OCID of the tenant that owns the log object.</td>
</tr>
<tr>
<td>compartmentid</td>
<td>No</td>
<td>Yes</td>
<td>String</td>
<td>The OCID of the compartment the log object resided in at the time the message was ingested.</td>
</tr>
</tbody>
</table>

Details for API Gateway

This topic provides details for API Gateway logs.

Resources

- API deployment

Log Categories

<table>
<thead>
<tr>
<th>API value (ID):</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Access Logs</td>
<td>Access logs for an API deployment.</td>
</tr>
<tr>
<td>Execution</td>
<td>Execution Logs</td>
<td>Execution logs for an API deployment.</td>
</tr>
</tbody>
</table>

Availability

API Gateway Access/Execution logging is available in all the regions of the commercial realm.

API Deployment Access Log

API deployment access logs record a summary of every request and response that goes through the API gateway, matching a route on the API deployment. Each access log entry contains information about the request and response (time the request was received, server protocol, response status, and so on). For the complete list of fields, see Contents of an Access Log on page 2597.

Contents of an Access Log

Access logs appear as a value in the **Log Data** field. This value is JSON-formatted data with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpMethod</td>
<td>GET</td>
<td>HTTP method derived from the request line.</td>
</tr>
<tr>
<td>requestUri</td>
<td>/example/</td>
<td>Request URI derived from the request line.</td>
</tr>
<tr>
<td>serverProtocol</td>
<td>HTTP/1.1</td>
<td>HTTP protocol derived from the request line.</td>
</tr>
</tbody>
</table>
### Field | Example | Description
--- | --- | ---
bodyBytesSent | 45 | Total size of the response (in bytes) sent to the client.
gatewayId | ocid1.apigateway.oc1.iad.<unique_ID> | OCID of the API Gateway for the API deployment servicing the request.
httpUserAgent | Apache-HttpClient/4.5.9 (Java/1.8.0_252) | HTTP user agent for the request.
message | GET /example/ HTTP/1.1 | Request line received from the client.
opcRequestId | FF7F0B8A32246FC7526AE45A2FA8D5CE/A408784281BF81B0EE23596CE57CA93C/C06F7DDDFC7C505FAA0566D8F2FE0BB2 | Value of the opc-request-id HTTP header, or an internally generated request ID if none was specified in the request.
remoteAddr | 138.1.55.172 | IP address of the requesting client.
httpReferrer | https://www.example.com | The URL of the referral, if present.
requestDuration | 0.016 | Total time taken (in seconds, with millisecond precision), from when the gateway starts receiving request from the client, until it completes sending a response to the client.
status | 404 | Status code of the response from the gateway.

### Sample Access Log

```json
{
    "httpMethod": "GET",
    "requestUri": "/example/",
    "serverProtocol": "HTTP/1.1",
    "bodyBytesSent": 45,
    "gatewayId": "ocid1.apigateway.oc1.iad.<unique_ID>",
    "httpUserAgent": "Apache-HttpClient/4.5.9 (Java/1.8.0_252)",
    "message": "GET /example/ HTTP/1.1",
    "opcRequestId": "FF7F0B8A32246FC7526AE45A2FA8D5CE/A408784281BF81B0EE23596CE57CA93C/C06F7DDDFC7C505FAA0566D8F2FE0BB2",
    "remoteAddr": "138.2.05.172",
    "requestDuration": 0.016,
    "status": 404
}
```

### API Deployment Execution Log

API deployment execution logs record information about processing within the API gateway for an individual route, to help with troubleshooting and monitoring. Each execution log entry contains information (time the request was received, level to denote the severity of the log message, a message code, and so on). For the complete list of fields, see Contents of an Execution Log on page 2598.

### Contents of an Execution Log

By default Log Level info is enabled. This value is JSON-formatted data with the following fields:
<table>
<thead>
<tr>
<th>Field</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>request.loopDetected</td>
<td>Short code for the logging event encountered while running the request. For the complete list of message codes, see the &quot;Log Codes&quot; table Log Codes on page 2599.</td>
</tr>
<tr>
<td>gatewayId</td>
<td>ocid1.apigateway.oc1.iad. <code>&lt;unique_ID&gt;</code></td>
<td>API gateway OCID for the API deployment servicing the request.</td>
</tr>
<tr>
<td>functionId</td>
<td>ocid1.fnfunc.oc1.iad. <code>&lt;unique_ID&gt;</code></td>
<td>OCID of function that the API gateway invoked. This field is only present for function backends.</td>
</tr>
<tr>
<td>level</td>
<td>WARN</td>
<td>Log level for the execution log entry, whether INFO, WARN, or ERROR.</td>
</tr>
<tr>
<td>message</td>
<td>A request loop has been detected - requests for this gateway are being directed back to this gateway.</td>
<td>Execution message emitted while processing the request.</td>
</tr>
<tr>
<td>opcRequestId</td>
<td>FF7F0B8A32246FC7526AE45A2FA8A408784281BF81B0EE23596CE57C02CF/ A408784281BF81B0EE23596CE57C02CF/ C06F7DDDFC7C505FAA0566D8F2F8B83</td>
<td>Value of the opc-request-id HTTP header, or an internally generated request ID if none was specified in the request.</td>
</tr>
</tbody>
</table>

**Log Codes**

<table>
<thead>
<tr>
<th>Log Code</th>
<th>Description</th>
<th>Related Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpBackend.timeout</td>
<td>Request to the HTTP backend timed out.</td>
<td>HTTP Backend</td>
</tr>
<tr>
<td>httpBackend.dnsResolutionFailed</td>
<td>Failed to resolve the HTTP backend URL.</td>
<td></td>
</tr>
<tr>
<td>httpBackend.sslHandshakeFailed</td>
<td>SSL Handshake failed with the HTTP backend.</td>
<td></td>
</tr>
<tr>
<td>httpBackend.successfulRequest</td>
<td>Successful request to the HTTP backend.</td>
<td></td>
</tr>
<tr>
<td>httpBackend.responseReceived</td>
<td>Response received from the HTTP backend.</td>
<td></td>
</tr>
<tr>
<td>httpBackend.requestSent</td>
<td>Request sent to the HTTP backend.</td>
<td></td>
</tr>
<tr>
<td>functionBackend.successfulRequest</td>
<td>Successful invocation of the Oracle Function.</td>
<td>Oracle Functions Backend</td>
</tr>
<tr>
<td>functionBackend.notFoundOrNotAuthorized</td>
<td>Failed to invoke the Oracle Function due to 404 from Oracle Functions service.</td>
<td></td>
</tr>
<tr>
<td>functionBackend.rateLimited</td>
<td>Rate limited when invoking the Oracle Function.</td>
<td></td>
</tr>
<tr>
<td>functionBackend.serviceUnavailable</td>
<td>Oracle Functions service unavailable.</td>
<td></td>
</tr>
<tr>
<td>Log Code</td>
<td>Description</td>
<td>Related Feature</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>functionBackend.badGateway</td>
<td>Received &quot;Bad Gateway&quot; when invoking the Oracle Function.</td>
<td></td>
</tr>
<tr>
<td>functionBackend.timeout</td>
<td>Oracle Function invocation timed out.</td>
<td></td>
</tr>
<tr>
<td>functionBackend.internalServiceError</td>
<td>Internal service error when invoking the Oracle Function.</td>
<td></td>
</tr>
<tr>
<td>specification.badVariableReference</td>
<td>The context variable couldn't be resolved.</td>
<td>Incorrect Specification at run-time</td>
</tr>
<tr>
<td>specification.invalidAuthenticationPolicy</td>
<td>Invalid authentication policy.</td>
<td></td>
</tr>
<tr>
<td>specification.badTransformationPolicy</td>
<td>Bad transformation policy.</td>
<td></td>
</tr>
<tr>
<td>specification.badHeaderTransformationPolicy</td>
<td>Bad Header Transformation policy.</td>
<td></td>
</tr>
<tr>
<td>specification.badQueryParameterTransformationPolicy</td>
<td>Bad Query Parameter Transformation policy.</td>
<td></td>
</tr>
<tr>
<td>request.internalServiceError</td>
<td>Internal service error.</td>
<td>Request processing</td>
</tr>
<tr>
<td>request.loopDetected</td>
<td>A request loop condition has been detected, whereby requests for the gateway are being redirected to itself creating a cycle.</td>
<td></td>
</tr>
<tr>
<td>request.possibleLoopDetected</td>
<td>A possible request loop condition has been detected, whereby requests for the gateway are being redirected to itself creating a cycle.</td>
<td></td>
</tr>
<tr>
<td>request.headersTruncated</td>
<td>Request headers were truncated.</td>
<td></td>
</tr>
<tr>
<td>request.queryParametersTruncated</td>
<td>Request query parameters were truncated.</td>
<td></td>
</tr>
<tr>
<td>authorization.unauthorizedRequest</td>
<td>Authorization failed for the request.</td>
<td>Request Authorization</td>
</tr>
<tr>
<td>authorization.scopeCheckFailed</td>
<td>Failed to check the scope for the request.</td>
<td></td>
</tr>
<tr>
<td>customAuthentication.successfulFunctionInvocation</td>
<td>Successfully invoked the Oracle Function.</td>
<td>Custom Authentication</td>
</tr>
<tr>
<td>customAuthentication.failedFunctionInvocation</td>
<td>Failed to invoke the Oracle Function.</td>
<td></td>
</tr>
<tr>
<td>customAuthentication.successfulAuthenticationSuccessful</td>
<td>Authentication successful.</td>
<td></td>
</tr>
<tr>
<td>customAuthentication.authenticationFailed</td>
<td>Custom Authentication failed.</td>
<td></td>
</tr>
<tr>
<td>customAuthentication.unexpectedResponse</td>
<td>Unexpected response from the Oracle Function.</td>
<td></td>
</tr>
<tr>
<td>jwtAuthentication.successfulAuthenticationSuccessful</td>
<td>Authentication successful.</td>
<td>JWT Authentication</td>
</tr>
<tr>
<td>jwtAuthentication.authenticationFailed</td>
<td>JWT Authentication failed.</td>
<td></td>
</tr>
<tr>
<td>jwtAuthentication.badJsonWebKeySet</td>
<td>JSON Web Key Set is not valid.</td>
<td></td>
</tr>
<tr>
<td>jwtAuthentication.loadingJsonWebKeySet</td>
<td>Loading the JSON Web Key Set.</td>
<td></td>
</tr>
<tr>
<td>headerTransformation.badHeaderValue</td>
<td>Bad value for request header.</td>
<td>Header Transformation</td>
</tr>
</tbody>
</table>
Logging

<table>
<thead>
<tr>
<th>Log Code</th>
<th>Description</th>
<th>Related Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>headerTransformation.protectedHeaderTransformed</td>
<td>The policy tried to transform a protected header.</td>
<td></td>
</tr>
<tr>
<td>headerTransformation.protectedElementTransformed</td>
<td>The policy tried to transform a protected element.</td>
<td></td>
</tr>
<tr>
<td>headerTransformation.missingSetValue</td>
<td>Missing value for the set transform policy.</td>
<td></td>
</tr>
<tr>
<td>queryParameterTransformation.badParameterValue</td>
<td>Bad value for request query parameter.</td>
<td>Query Parameter Transformation</td>
</tr>
<tr>
<td>queryParameterTransformation.protectedElementTransformed</td>
<td>The policy tried to transform a protected element.</td>
<td></td>
</tr>
<tr>
<td>queryParameterTransformation.missingSetValue</td>
<td>Missing value for the set transform policy.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Execution Logs

- Type: Request
- Scenario: Request Loop Detected
- Description: A request loop condition has been detected, whereby requests for the gateway are being redirected to itself creating a cycle.
- Example:

```json
{  "code": "request.loopDetected",  "gatewayId": "ocid1.apigateway.oc1.iad.<unique_ID>",  "level": "WARN",  "message": "A request loop has been detected - requests for this gateway are being directed back to this gateway.",  "opcRequestId": "FF7F0B8A32246FC7526AE45A2FA8D5CE/A408784281BF81B0EE23596CE57CA93C/C06F7DDDFC7C505FAA0566D8F2FE0BB2",}
```

Details for Events

This topic provides details for Events logs.

Resources

- rules

Log Categories

<table>
<thead>
<tr>
<th>API value (ID):</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleexecutionlog</td>
<td>Rule Execution Logs</td>
<td>Describes how rules were evaluated against events emitted from resources.</td>
</tr>
</tbody>
</table>

Availability

Events logging is available in all the regions of the commercial realm. Events logging is not available in regions within the Government Cloud realm.
## Contents of an Events Log

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logTime</td>
<td>The time of the event, expressed in RFC 3339 timestamp format.</td>
</tr>
<tr>
<td>ruleId</td>
<td>The events rule ID.</td>
</tr>
<tr>
<td>eventId</td>
<td>The UUID of the event. This identifier is not an OCID, but just a unique ID for the event.</td>
</tr>
<tr>
<td>message</td>
<td>The event message.</td>
</tr>
</tbody>
</table>
| target   | The rule action. For example:  
  - For streaming, it means that the event was delivered to the stream.  
  - For a notification, it means it was delivered to the email subscribed to the topic.  
  - For a function, it means it triggered the function with the event data. |

### An Example Events Log

For events there are two types of messages:

```json
{
  "specversion": "1.0",
  "type": "com.oraclecloud.eventsservice.eventrule.ruleexecutionlog",
  "source": "Flowlogs",
  "id": "6e6dbfd3-4bce-4484-848d-af53f19bd6c9",
  "time": "2020-08-24T23:31:44Z",
  "oracle": {
    "logid": "ocid1.log.oc1.iad.<unique_ID>",
    "loggroupid": "ocid1.loggroup.oc1.iad.<unique_ID>",
    "compartmentid": "ocid1.compartment.oc1..<unique_ID>",
    "tenantid": "ocid1.tenancy.oc1..<unique_ID>",
    "ingestedtime": "2020-08-19T15:33:30.832Z"
  },
  "data": {
    "ruleId": "ocid1.eventrule.oc1.iad.<unique_ID>",
    "eventId": "24bc7219-efec-4ccd-350b-be2d833439d2",
    "message": "Event failed to deliver to FAAS. Exception from FAAS endpoint  
      https://ptktjbkp22a.us-ashburn-1.functions.oci.oraclecloud.com,  
      exception message:  
      (502, FunctionInvokeImageNotAvailable, false) Failed to pull function image (opc-request-id:  
      AA3D3CEE50107C103AA662B8646A0EEE/01EGHCZXNW1BT0750ZJ0058HCQ/01EGHCZXNW1BT0750ZJ0058HCQ,  
      opc-request-id  
      AA3D3CEE50107C103AA662B8646A0EEE/01EGHCZXNW1BT0750ZJ0058HCQ/01EGHCZXNW1BT0750ZJ0058HCQ,  
      statuscode 502", "target": "ocid1.fnfunc.oc1.iad.<unique_ID>"
  }
}
```

```
{
  "specversion": "1.0",
  "type": "com.oraclecloud.eventsservice.eventrule.ruleexecutionlog",
  "source": "cmi-push-vcn-splunk-phoenix",
  "id": "52007b4c-225e-4d6c-9dea-077b884a94e9",
  "time": "2020-08-24T23:35:16Z",
  "oracle": {
    "logid": "ocid1.log.oc1.iad.<unique_ID>",
    "loggroupid": "ocid1.loggroup.oc1.iad.<unique_ID>",
    "compartmentid": "ocid1.compartment.oc1..<unique_ID>"
  },
  "data": {
    "ruleId": "ocid1.eventrule.oc1.iad.<unique_ID>",
    "eventId": "c50a08b9-8e5d-4000-bb84-077b884a94e9",
    "message": "Exception from Splunk Realtime Streaming Processor  
      instance "0000" for topic "f1"
      (502, FunctionInvokeImageNotAvailable, false) Failed to pull function image (opc-request-id:  
      AA3D3CEE50107C103AA662B8646A0EEE/01EGHCZXNW1BT0750ZJ0058HCQ/01EGHCZXNW1BT0750ZJ0058HCQ,  
      opc-request-id  
      AA3D3CEE50107C103AA662B8646A0EEE/01EGHCZXNW1BT0750ZJ0058HCQ/01EGHCZXNW1BT0750ZJ0058HCQ,  
      statuscode 502", "target": "ocid1.fnfunc.oc1.iad.<unique_ID>"
  }
}
```
Logging

```
"tenantid": "ocid1.tenancy.oc1..<unique_ID>",
"ingestedtime": "2020-08-19T15:33:30.832Z"
},
"data": {
  "ruleId": "ocid1.eventrule.oc1.phx.<unique_ID>",
  "eventId": "30bde0fa-af8a-f50c-aa01-4fc42f28acb9",
  "message": "Rule has matched event"
}
```

**Events Log Object Name**

Objects that store Events log data use the following naming format:

```
Rule_Execution_Log/<event_rule_OCID>/<YYYY-MM-DDTHH_MMZ>[_<seqNum>].log.gz
```

For example:

```
Rule_Execution_Log/
ocid1.eventrule.oc1.phx.<unique_ID>/2019-03-21T00_00Z.log.gz
Rule_Execution_Log/
ocid1.eventrule.oc1.phx.<unique_ID>/2019-03-21T00_00Z_2.log.gz
```

**Details for Functions**

This topic provides details for Functions logs.

**Resources**

- applications

**Log Categories**

<table>
<thead>
<tr>
<th>API value (ID)</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>invoke</td>
<td>Function Invocation Logs</td>
<td>Logs entries each time a function in an application is invoked.</td>
</tr>
</tbody>
</table>

**Availability**

Functions logging is available in all the regions of the [commercial realm](#).

**Comments**

To use Functions logging, you must add a print statement to your function.

**Examples:**

For node js:

```javascript
console.log('Entering Hello Node.js function');
```

For java:

```java
System.out.println("Entering Java Hello World Function");
```

For go:

```go
fmt.Println("Entering Hello Go function")
```
Contents of a Functions Log

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>specversion</td>
<td>Oracle Cloud Infrastructure logging schema version of the log.</td>
</tr>
<tr>
<td>type</td>
<td>Category of log, following convention <code>com.oraclecloud.{service}.{resource-type}.{log-category}</code>. Currently only: <code>com.oraclecloud.functions.application.functioninvoke</code></td>
</tr>
<tr>
<td>source</td>
<td>Display name of the application the log is associated with.</td>
</tr>
<tr>
<td>subject</td>
<td>Display name of the function the log is associated with.</td>
</tr>
<tr>
<td>id</td>
<td>Random UUID, unique to each log entry.</td>
</tr>
<tr>
<td>time</td>
<td>Time the function output was generated, in RFC 3339 timestamp format.</td>
</tr>
<tr>
<td>oracle.logid</td>
<td>OCID of the Oracle Cloud Infrastructure Logging log object.</td>
</tr>
<tr>
<td>oracle.loggroupid</td>
<td>OCID of the Oracle Cloud Infrastructure Logging log group.</td>
</tr>
<tr>
<td>oracle.compartmentid</td>
<td>OCID of the compartment the function/application is in.</td>
</tr>
<tr>
<td>oracle.tenantid</td>
<td>OCID of the tenancy the function/application is in.</td>
</tr>
<tr>
<td>oracle.ingestedtime</td>
<td>Time the log line was ingested by Oracle Cloud Infrastructure logging, in RFC 3339 timestamp format.</td>
</tr>
<tr>
<td>data.applicationId</td>
<td>OCID of the application the log line is associated with.</td>
</tr>
<tr>
<td>data.containerId</td>
<td>FaaS service-specific ID of the function's container.</td>
</tr>
<tr>
<td>data.functionId</td>
<td>OCID of the function the log line is associated with.</td>
</tr>
<tr>
<td>data.requestId</td>
<td>Oracle RID of the function invocation the log line is associated with.</td>
</tr>
<tr>
<td>data.src</td>
<td>I/O stream origin of data.message. Either STDOUT or STDERR.</td>
</tr>
<tr>
<td>data.message</td>
<td>User-generated line of output from the function.</td>
</tr>
</tbody>
</table>

An Example Functions Log

```json
{
  "specversion": "1.0",
  "type": "com.oraclecloud.functions.application.functioninvoke",
  "source": "Application display name",
  "subject": "Function display name",
  "id": "487c8669-f384-4c79-950a-d6df47246093",
  "time": "2020-08-19T15:33:29.000Z",
  "oracle": {
    "logid": "ocid1.log.oc1.iad.<unique_ID>",
    "loggroupid": "ocid1.loggroup.oc1.iad.<unique_ID>",
    "compartmentid": "ocid1.compartment.oc1..<unique_ID>",
    "tenantid": "ocid1.tenancy.oc1..<unique_ID>",
    "ingestedtime": "2020-08-19T15:33:30.832Z"
  },
  "data": {
    "applicationId": "ocid1.fnapp.oc1.iad.<unique_ID>",
    "containerId": "01EG3NMHG60000000000000022S",
    "functionId": "ocid1.fnfunc.oc1.iad.<unique_ID>",
    "requestId": "/01EG3NN3C11BT19PGZJ00000VZ/01EG3NN3C11BT19PGZJ00000W0",
    "src": "STDOUT"
  }
}```
Functions Log Object Name

Objects that store Functions log data use the following naming format:

\[ \text{log/}<\text{function-OCID}>/\text{<YYYY-MM-DDTHH_MMZ>[_<seqNum>].log.gz} \]

For example:

\[ \text{log/ocid1.function.oc1.phx.<unique_ID>/2019-03-21T00_00Z.log.gz} \]
\[ \text{log/ocid1.function.oc1.phx.<unique_ID>/2019-03-21T00_00Z_2.log.gz} \]

Using the Command Line Interface (CLI)

See Functions Example on page 2590 for an example command to enable Functions logging.

Details for Load Balancer Logs

This topic provides details for load balancer access logs. See these instructions to create a log group and configure LBaaS access and error logs.

Resources

- load balancer

Log Categories

<table>
<thead>
<tr>
<th>API value (ID):</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Access Logs</td>
<td>Load balancer access logs.</td>
</tr>
<tr>
<td>Error</td>
<td>Error Logs</td>
<td>Load balancer error logs.</td>
</tr>
</tbody>
</table>

Availability

LBaaS access logs are available in all the regions of the commercial realm.

Load Balancer Access Log

Load balancer access logs capture detailed information about requests sent to the load balancer. Each access log entry contains:

- The time the request was received.
- Client and intermediate HTTP proxy IP addresses.
- Time taken at the load balancer and backend to process the request.

Limitations and Considerations

Some traffic might not be logged during a capture window because of capacity issues or system errors. In such cases, the following error log message is logged.

\[ \{ "timestamp": "2020-08-05T00:12:39+00:00", "errorLog": \{ "type": "General", "errorDetails": "Missed 100 access logs" \} \} \]

For traffic destined to the public IP of a load balancer, access logs record the corresponding private IP.
Contents of an Access Log

Access logs appear as a value in the Log Data field. This value is a JSON-formatted data with the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>2020-04-20T00:56:18+00:00</td>
<td>Log entry generation time in ISO-8601 format.</td>
</tr>
<tr>
<td>clientAdd</td>
<td>192.168.0.33:7870</td>
<td>IP address and port number of the requesting client.</td>
</tr>
<tr>
<td>forwardedForAddr</td>
<td>192.168.0.33</td>
<td>IP address of the client and http proxies between client and load balancer.</td>
</tr>
<tr>
<td>host</td>
<td>a.com</td>
<td>Domain name which resolves to VIP address assigned to the load balancer.</td>
</tr>
<tr>
<td>backendAddr</td>
<td>192.168.0.34:8080</td>
<td>IP address and port number of the backend server, which processed the client request.</td>
</tr>
<tr>
<td>requestProcessingTime</td>
<td>0.003</td>
<td>Total time taken (in seconds, with millisecond precision), from when the load balancer starts receiving request from the client, until it completes sending responses to the client.</td>
</tr>
<tr>
<td>backendConnectTime</td>
<td>0.00</td>
<td>Time spent (in seconds, with millisecond precision), to establish backend server connection.</td>
</tr>
<tr>
<td>backendProcessingTime</td>
<td>0.002</td>
<td>Total time taken from the load balancer establishing a connection to a backend, until it completes receiving the response from the backend.</td>
</tr>
<tr>
<td>lbStatusCode</td>
<td>200</td>
<td>Status code of the response from the load balancer.</td>
</tr>
<tr>
<td>backendStatusCode</td>
<td>200</td>
<td>Status code of the response from the target.</td>
</tr>
<tr>
<td>receivedBytes</td>
<td>150</td>
<td>Total size of the request (in bytes), received from the client.</td>
</tr>
<tr>
<td>sentBytes</td>
<td>450</td>
<td>Total size of the response (in bytes), sent to the client from the load balancer.</td>
</tr>
<tr>
<td>request</td>
<td>&quot;GET / HTTP/1.1&quot;</td>
<td>Request line received from the client.</td>
</tr>
<tr>
<td>sslCipher</td>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
<td>Negotiated SSL cipher between the client and the load balancer.</td>
</tr>
<tr>
<td>sslProtocol</td>
<td>TLSv1.2</td>
<td>Negotiated SSL protocol between the client and the load balancer.</td>
</tr>
<tr>
<td>userAgent</td>
<td>curl/7.29.0</td>
<td>User Agent, which sent the request to the load balancer.</td>
</tr>
</tbody>
</table>

Load Balancer Error Log

Load balancer error logs capture detailed information about requests related to troubleshooting and monitoring. Each Error Log entry contains information such as the time the request was received, error type, and extra details related to the specific error.

Contents of an Error Log

This value is JSON-formatted data with the following fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>2020-08-04T21:25:27+00:00</td>
<td>Log entry generation time in ISO-8601 format.</td>
</tr>
<tr>
<td>type</td>
<td>frontDoor</td>
<td>Error log Category.</td>
</tr>
<tr>
<td>errorDetails</td>
<td>Access for client 160.34.88.6 forbidden by ACL rule</td>
<td>Detailed description of the error message.</td>
</tr>
</tbody>
</table>

Sample Error Logs

**Type: healthChecker**

timestamp: 2020-08-05T00:12:39+00:00, "errorLog": {"type": "healthChecker", "errorDetails":

- check failure because of connection timeout.

**Type: healthChecker**

timestamp: 2020-08-04T23:28:52+00:00, "errorLog": {"type": "healthChecker", "errorDetails":

- check failure because of RegEx mismatch.

**Type: healthChecker**

timestamp: 2020-08-04T19:53:29+00:00, "errorLog": {"type": "healthChecker", "errorDetails":

- check failure because of connection RST.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HealthChecker</td>
<td>Example:</td>
</tr>
<tr>
<td>healthChecker</td>
<td>Unreachable host. Back-end health check failure because of unreachable host.</td>
</tr>
<tr>
<td>healthChecker</td>
<td>Success (Unhealthy to healthy). Unhealthy backend became healthy.</td>
</tr>
<tr>
<td>healthChecker</td>
<td>SSL Backend, with some SSL error.</td>
</tr>
<tr>
<td>frontDoor</td>
<td>Drop (TCP) Client connection drop to ACL rules.</td>
</tr>
<tr>
<td>sslClient</td>
<td>SSL error as client did not send certificate.</td>
</tr>
<tr>
<td>backEnd</td>
<td>Connection failure when all backends are unhealthy.</td>
</tr>
</tbody>
</table>
Details for Object Storage

This topic provides details for Object Storage logs.

Resources

- buckets

Log Categories

<table>
<thead>
<tr>
<th>API value (ID):</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write</td>
<td>Write Access Events</td>
<td>Includes logs for write events.</td>
</tr>
<tr>
<td>read</td>
<td>Read Access Events</td>
<td>Includes logs for read events.</td>
</tr>
</tbody>
</table>

Availability

Object Storage logging is available in all the regions of the commercial realm.

Comments

Choose the log category for the type of information that you want to log. For example, if you enable a write log, the requestAction property would contain values of PUT, POST, or DELETE. If you enable a read log, requestAction would contain values of GET, LIST, or HEAD.

Contents of an Object Storage Log

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>additionalDetails</td>
<td>Includes the following fields when applicable to the particular log:</td>
</tr>
<tr>
<td></td>
<td>- versionId: From PutObject and DeleteObject responses</td>
</tr>
<tr>
<td></td>
<td>- isDeleteMarker: From the DeleteObjectVersion response</td>
</tr>
<tr>
<td></td>
<td>- retentionRuleName</td>
</tr>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>apiType</td>
<td>Originating Object Storage API:</td>
</tr>
<tr>
<td></td>
<td>• native</td>
</tr>
<tr>
<td></td>
<td>• s3-compatible</td>
</tr>
<tr>
<td></td>
<td>• swift</td>
</tr>
<tr>
<td>authenticationType</td>
<td>Request authentication type:</td>
</tr>
<tr>
<td></td>
<td>• user</td>
</tr>
<tr>
<td></td>
<td>• service</td>
</tr>
<tr>
<td></td>
<td>• resource</td>
</tr>
<tr>
<td></td>
<td>• instance</td>
</tr>
<tr>
<td>bucketCreator</td>
<td>OCID of the bucket creator</td>
</tr>
<tr>
<td>bucketId</td>
<td>OCID of the bucket</td>
</tr>
<tr>
<td>bucketName</td>
<td>Name of the bucket</td>
</tr>
<tr>
<td>clientId</td>
<td>IP address of the requesting client</td>
</tr>
<tr>
<td>compartmentId</td>
<td>OCID of the compartment</td>
</tr>
<tr>
<td>compartmentName</td>
<td>Name of the compartment</td>
</tr>
<tr>
<td>credentials</td>
<td>Request security credentials</td>
</tr>
<tr>
<td>endTime</td>
<td>Request end timestamp</td>
</tr>
<tr>
<td>errorCode</td>
<td>If present, a short error code meant for programmatic parsing that defines the error</td>
</tr>
<tr>
<td>eTag</td>
<td>Entity tag (ETag) for the resource</td>
</tr>
<tr>
<td>isPar</td>
<td>Boolean describing whether this is a pre-authenticated request:</td>
</tr>
<tr>
<td></td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td>• false</td>
</tr>
<tr>
<td>message</td>
<td>Human-readable string describing the request</td>
</tr>
<tr>
<td>namespace</td>
<td>Object Storage namespace used for the request</td>
</tr>
<tr>
<td>objectName</td>
<td>Name of the object</td>
</tr>
<tr>
<td>opcRequestId</td>
<td>Client request ID for tracing</td>
</tr>
<tr>
<td>principalId</td>
<td>OCID of the requestor</td>
</tr>
<tr>
<td>principalName</td>
<td>Name of the requestor</td>
</tr>
<tr>
<td>region</td>
<td>Region identifier</td>
</tr>
<tr>
<td>requestAction</td>
<td>HTTP method of the request (DELETE/GET/HEAD/POST/PUT)</td>
</tr>
<tr>
<td>requestResourcePath</td>
<td>Resource path of the request</td>
</tr>
<tr>
<td>startTime</td>
<td>Request start timestamp</td>
</tr>
<tr>
<td>statusCode</td>
<td>Response status code</td>
</tr>
<tr>
<td>tenantId</td>
<td>OCID of the tenant</td>
</tr>
<tr>
<td>tenantName</td>
<td>OCID of the tenant</td>
</tr>
<tr>
<td>userAgent</td>
<td>User Agent that sent the request to Object Storage</td>
</tr>
</tbody>
</table>
An Example Object Storage Log

```json
{
    "time": "2020-09-10T19:04:11.324Z",
    "specversion": "1.0",
    "id": "2901893c-2140-491e-b23d-9cc6649f6e67",
    "source": "MyBucket",
    "subject": "MyObject",
    "type": "com.oraclecloud.objectstorage.putobject",
    "data": {
        "additionalDetails": {
            "versionId": "7dec129d-ec60-470f-a153-f44af0ac15a6"
        },
        "apiType": "native",
        "authenticationType": "user",
        "bucketCreator": "ocid1.user.oc1..<unique_ID>",
        "bucketId": "ocid1.bucket.oc1.phx.<unique_ID>",
        "bucketName": "MyBucket",
        "clientIpAddress": "203.0.113.4",
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "MyObjectStore",
        "credentials": "<credentials>",
        "endTime": "2020-09-10T19:04:11.324Z",
        "isPar": false,
        "message": "Object uploaded.",
        "namespaceName": "MyNamespace",
        "objectName": "MyObject",
        "opcRequestId": "phx-1:7Tx5eJoAX01cWk5F-1Wjz_W2zF8aLqW8PepN5gsK7HlqKm3Mrot9JIAuZbQxBEI",
        "principalId": "ocid1.user.oc1..<unique_ID>",
        "principalName": "jane.smith@example.com",
        "requestAction": "PUT",
        "requestResourcePath": "/n/MyNamespace/b/MyBucket/o/MyObject",
        "startTime": "2020-09-10T19:04:10.679Z",
        "statusCode": 200,
        "tenantId": "ocid1.tenancy.oc1..<unique_ID>",
        "tenantName": "MyTenancy",
        "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36"
    },
    "oracle": {
        "logid": "ocid1.log.oc1.phx.<unique_ID>"
    }
}
```

Object Storage Log Object Name

Objects that store Object Storage data use the following naming format:

```
public_log/<bucket_name>/YYYY-MM-DDTHH_MMZ[<seqNum>].log.gz
```

For example:

```
public_log/example_bucket/2019-03-21T00_00Z.log.gz
public_log/example_bucket/2019-03-21T00_00Z_2.log.gz
```

Using the Command Line Interface (CLI)

See Object Storage Example on page 2589 for example commands.
Details for VCN Flow Logs

This topic provides details for VCN Flow logs.

Resources

• subnet

Log Categories

<table>
<thead>
<tr>
<th>API value (ID):</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Flow Logs (All records)</td>
<td>Includes both accept and reject records in VCN flow logs.</td>
</tr>
</tbody>
</table>

Availability

VCN Flow Logs are available in all the regions of the commercial realm.

Comments

Each instance in a VCN has one or more virtual network interface cards (VNICs). The Networking service uses security rules to determine what traffic is allowed through a given VNIC. Security rules can be defined using Security lists or Network security groups.

To help troubleshoot the traffic in and out of your VNICs, you can set up VCN flow logs. Flow logs record details about traffic that has been accepted or rejected based on the security rules set up for your VCN.

You can enable flow logs for a given subnet, which means traffic is logged for all existing and future VNICs in that subnet. Each flow log contains information about traffic for a single VNIC.

Note:

Certain traffic to core Oracle infrastructure services hosted on link-local (169.254.0.0/16) IP addresses do not appear in flow logs. This includes items such as VCN DNS, DHCP, and block storage. Also excluded is network management traffic, such as ARP.

Contents of a VCN Flow Log

A flow log record contains the following fields:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.action</td>
<td>Type of record. Possible values:</td>
<td>ACCEPT</td>
</tr>
<tr>
<td></td>
<td>• ACCEPT: This record's traffic was accepted by the security lists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REJECT: This record's traffic was rejected by the security lists.</td>
<td></td>
</tr>
<tr>
<td>data.bytesOut</td>
<td>Number of bytes recorded in the capture window.</td>
<td>17114</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Sample Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>data.destinationAddress</td>
<td>IP address of the destination, either in IPv4 dot, or IPv6 colon notation.</td>
<td>10.0.99.4 8222:91f5:88bb:2bf0:94a:e71b:65d3:4bd7</td>
</tr>
<tr>
<td></td>
<td>Note:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When IPv6 traffic is encountered in a customer’s virtual cloud network, a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flow log entry with IPv6 address values is generated, in place of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>current location of IPv4 values. The source and destination addresses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>could be either IPv4 or IPv6, based on the configuration and traffic present</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in the customer’s VCN. This data is only available in regions where</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv6 support is generally available, and configured by the customer.</td>
<td></td>
</tr>
<tr>
<td>data.destinationPort</td>
<td>IANA port number of the destination.</td>
<td>36266</td>
</tr>
<tr>
<td>data.endTime</td>
<td>End time of the capture window in UNIX epoch seconds.</td>
<td>1598917970</td>
</tr>
<tr>
<td>data.flowid</td>
<td>Hash of key fields (source and destination addresses, ports, and protocol).</td>
<td>a6a737770</td>
</tr>
<tr>
<td>data.packets</td>
<td>Number of packets recorded in the capture window.</td>
<td>250</td>
</tr>
<tr>
<td>data.protocol</td>
<td>IANA protocol number.</td>
<td>6</td>
</tr>
<tr>
<td>data.protocolName</td>
<td>IANA name for protocol.</td>
<td>TCP</td>
</tr>
<tr>
<td>data.sourceAddress</td>
<td>IP address of the source, either in IPv4 dot, or IPv6 colon notation.</td>
<td>123.0.0.1 1fde:9f1c:2433:4038:68fc:e0b:73f3:32f5</td>
</tr>
<tr>
<td>data.sourcePort</td>
<td>IANA port number of the source.</td>
<td>443</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Sample Value</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>data.startTime</td>
<td>Start time of the capture window in Unix epoch seconds.</td>
<td>1598917969</td>
</tr>
<tr>
<td></td>
<td>UNIX epoch time uses a fixed point in the past to reference the current time. That means that every second of the current time can be expressed as a number, such as 1576090259 (which is Wednesday, December 11, 2019 6:50:59 PM GMT). Each flow log record records a one-minute interval (0 to 59 seconds) of data flow, using epoch start and end times to indicate the time that data appears during the 60-second interval for that record. Let's consider the epoch time entries that would appear for data flow during a fixed interval of 140 seconds. At five seconds past a particular minute, you open a connection to your host and begin to continuously send data over that connection for the next 140 seconds (&lt; three minutes, three records). Epoch start and end times would appear in the log according to the following: • The first record would show an epoch start time at the five seconds past the minute mark and an epoch end time at the end of that minute (54 seconds later). • The next record would show an epoch start time at the zero-seconds mark, and epoch end time at the end of that minute (59 seconds later). This assumes you sent the data continuously. If your transmission had been intermittent, the epoch times would reflect the first and last second data flow that occurred during that 60-second interval (the absolute time). • The final record would show an epoch start time at the zero-seconds mark, and an epoch end time for 20 seconds later (since the total flow life was only 140 seconds, or 20 seconds into the third one-minute logging interval recorded by each record).</td>
<td></td>
</tr>
<tr>
<td>data.status</td>
<td>Status of data capture window. Possible values:</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>• OK: Normal packet log.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NODATA: No traffic was recorded during the capture window, in which case, only the following data fields are set: endTime, startTime, status, and version. The remaining data fields are set to null: action, bytesOut, destinationAddress, destinationPort, flowid, packets, protocol, protocolName, sourceAddress, and sourcePort. • SKIPDATA: Some traffic was not logged during the capture window because of system errors or capacity issues, in which case, only data fields endTime, startTime, status, and version are set, and the remaining data fields are set to null. The flow log can contain other records for accepted or rejected traffic in the capture window.</td>
<td></td>
</tr>
<tr>
<td>data.version</td>
<td>Version of the flow log record schema.</td>
<td>2</td>
</tr>
<tr>
<td>datatime</td>
<td>Timestamp in milliseconds. Same as the oracle.ingestedtime field but in milliseconds.</td>
<td>1598917955000</td>
</tr>
<tr>
<td>id</td>
<td>Random UUID, unique to each log entry.</td>
<td>abcdabcd-abed-abedabcdabcdabcd</td>
</tr>
</tbody>
</table>
### Logging

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.compartmentid</td>
<td>OCID of the compartment the log group is in.</td>
<td>ocid1.compartment.oc1..&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>oracle.ingestedtime</td>
<td>Time the log was ingested by OCI Logging.</td>
<td>2020-08-31T23:53:54Z</td>
</tr>
<tr>
<td>oracle.loggroupid</td>
<td>OCID of the log group.</td>
<td>ocid1.loggroup.oc1.&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>oracle.logid</td>
<td>OCID of the log.</td>
<td>ocid1.log.oc1.&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>oracle.tenantid</td>
<td>OCID of the tenant.</td>
<td>ocid1.tenancy.oc1.&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>oracle.vniccompartmentocid</td>
<td>OCID of the compartment to which the VNIC belongs.</td>
<td>ocid1.compartment.oc1..&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>oracle.vnicocid</td>
<td>OCID of the VNIC.</td>
<td>ocid1.vnic.oc1.&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>oracle.vnicsubnetocid</td>
<td>OCID of the subnet to which the VNIC belongs.</td>
<td>ocid1.subnet.oc1.&lt;region-id&gt;..&lt;unique-id&gt;</td>
</tr>
<tr>
<td>specversion</td>
<td>OCI logging schema version.</td>
<td>1.0</td>
</tr>
<tr>
<td>time</td>
<td>Same as start time.</td>
<td>2020-08-31T23:52:35Z</td>
</tr>
<tr>
<td>type</td>
<td>Category of log: DataEvent, QualityEvent.NoData, or QualityEvent.SkipData.</td>
<td>com.oraclecloud.vcn.flownlogs.DataEvent</td>
</tr>
</tbody>
</table>

### Limitations and Considerations

- Some traffic might not be logged during a capture window because of capacity issues or system errors. In such cases, NODATA, or SKIPDATA log status is recorded.
- Some services manage VNICS. For example, the Load Balancing service manages VNICS attached to load balancers. Flow logs for managed VNICS are captured, and identified by VNIC ID. Flow logs, however, currently do not include a field to indicate what service such VNICS belong to.
- For traffic over the public IP of a Compute instance, flow logs records the corresponding private IP.

### Using the Command Line Interface (CLI)

See VCN Flow Logs Example on page 2589 for example commands.

### Details for VPN Connect

This topic provides details for VPN Connect logs.

### Resources

- IPSecConnection

### Log Categories

<table>
<thead>
<tr>
<th>API value (ID):</th>
<th>Console (Display Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>IPSec Logs</td>
<td>Includes VPN Connect logs for read access.</td>
</tr>
</tbody>
</table>
Availability
See VPN Connect v2 availability on page 3156 for up-to-date information on VPN Connect logging availability.

Comments
VPN Connect logs contain all status-related information of the IPSec tunnels associated with the site-to-site type of IPSec connections. This includes bringing of tunnels up or down, and accompanying negotiation information. Each IPSec connection has two IPSec tunnels created, thus the VPN Connect logs will contain status on both tunnels. Amongst other types of filtering, IPSec tunnels can be distinguished and thus filtered on their data.TunnelId (see Contents of a VPN Connect Log on page 2616 below for details).

Most VPN Connect log messages begin with a connection name. The connection name is unique for each IPSec tunnel. Its base form is comprised of ten numeric digits (see the sample value for the data.message property in the table below). In total, a connection name has three additional variants, and which variant(s) are used is based on the following:

1. Each IPSec tunnel has a unique ten-digit key assigned to (for example, 9123456789) which is contained in the beginning of many of the IPSec log messages. This is the form for IPv4 tunnels.
2. If the given IPSec tunnel is also configured for IPv6, IPSec log messages can also contain the same ten-digit key with a _v6 appended to it (for example, 9123456789_v6).
3. If the tunnel is policy-based (that is, MED is enabled) there can be multiple SAs depending on the configuration. The form of the ten-digit key for IPv4 tunnels with multiple SAs is a sequence of _1, _2, _3, and accordingly depending on the number of SAs (for example, 9123456789_1, 9123456789_2, 9123456789_3).
4. If the given policy-based tunnel is also configured for IPv6, IPSec log messages can also contain the same ten-digit key and SA index, along with v6 (for example, 9123456789_v6_1).

Contents of a VPN Connect Log
A VPN Connect log contains the following fields:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.message</td>
<td>The VPN Connect log message.</td>
<td>&quot;2062988354&quot;: terminating SAs using this connection</td>
</tr>
<tr>
<td>data.tunneld</td>
<td>The IPSec tunnel OCID of one of the IPSec connection's IPSec tunnels.</td>
<td>ocid1.ipsectunnel.region1.sea.&lt;uniqueId&gt;</td>
</tr>
<tr>
<td>id</td>
<td>Random UUID, unique to each log entry.</td>
<td>e3002eaa-d717-472e-8474-d024943a0f27</td>
</tr>
<tr>
<td>oracle.compartmentid</td>
<td>OCID of the compartment that the log group belongs to.</td>
<td>ocid1.tenancy.region1..&lt;uniqueId&gt;</td>
</tr>
<tr>
<td>oracle.ingestedtime</td>
<td>Time the log was ingested by Oracle Cloud Infrastructure Logging.</td>
<td>2021-02-18T18:22:01.453Z</td>
</tr>
<tr>
<td>oracle.loggroupid</td>
<td>OCID of the log group.</td>
<td>ocid1.loggroup.region1.sea.&lt;uniqueId&gt;</td>
</tr>
<tr>
<td>oracle.logid</td>
<td>OCID of the log.</td>
<td>ocid1.log.region1.sea.&lt;uniqueId&gt;</td>
</tr>
<tr>
<td>oracle.tenantid</td>
<td>OCID of the tenant.</td>
<td>ocid1.tenancy.region1..&lt;uniqueId&gt;</td>
</tr>
<tr>
<td>source</td>
<td>OCID of the IPSec connection, which is comprised of two IPSec tunnels.</td>
<td>ocid1.ipsecconnection.region1.sea.&lt;uniqueId&gt;</td>
</tr>
<tr>
<td>specversion</td>
<td>OCI logging schema version.</td>
<td>1.0</td>
</tr>
<tr>
<td>time</td>
<td>Time the log was generated in the IPSec tunnel.</td>
<td>2021-02-18T18:21:52.024Z</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Sample Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>type</td>
<td>Category of the log. Set of possible values: read</td>
<td>com.oraclecloud.vpn.ipseclog.read</td>
</tr>
</tbody>
</table>

An Example VPN Connect Log

```json
{
  "data": {
    "message": "2062988354": terminating SAs using this connection",
    "tunnelId": "ocid1.ipsectunnel.region1.sea.uniqueId"
  },
  "id": "e3002eaa-d717-472e-8474-d024943a0f27",
  "oracle": {
    "compartmentId": "ocid1.tenancy.region1..uniqueId",
    "ingestedTime": "2021-02-18T18:22:01.453Z",
    "logGroupId": "ocid1.loggroup.region1.sea.uniqueId",
    "logId": "ocid1.log.region1.sea.uniqueId",
    "tenantId": "ocid1.tenancy.region1..uniqueId"
  },
  "source": "ocid1.ipsecconnection.region1.sea.uniqueId",
  "specversion": "1.0",
  "time": "2021-02-18T18:21:52.024Z",
  "type": "com.oraclecloud.vpn.ipseclog.read"
}
```

Troubleshooting

An error is displayed on the log details page if you attempt to enable logs for a v1 VPN connection. Only v2 connections are supported.

Audit Logs

On the Audit page, you can explore audit logs. Audit logs are also searchable on the Search page, and you can view Audit logs in every compartment by selecting the `_Audit` log group on the Search page. For an overview of Audit, see Overview of Audit on page 488.

Note:

This page replaces the classic Audit page features found in the Governance and Administration portion of the Console, which will eventually be deprecated. As a result, a new and improved Audit experience is now part of Oracle Cloud Infrastructure Logging, and we recommend you use this latest version of Audit instead.

Required Permissions for Audit Logs

To view and search Audit logs, you must have the corresponding Audit-related permissions. See Details for the Audit Service on page 2177 and Required Permissions for Searching Logs on page 2635 for more information.

Filtering Audit Logs

To filter Audit logs:

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Audit. The list of audit logs in the current compartment is displayed.
2. Choose a compartment you have permission to work in.
3. In **User**, add user filters. Multiple users can be added.
4. In **Resource**, add resource filters. Multiple resources can be filtered on.
5. In **Request Action Types**, select an action operation:
   - GET
   - POST
   - PUT
   - PATCH
   - DELETE
   Multiple request action types can be filtered on.
6. In **Event Type**, add event filters. Multiple event filters can be added.
7. In **Custom Filters**, start typing to automatically display filter settings, along with operators. For example, entering `d` displays filters starting with that letter. Use the up or down arrow keys to select from the list, or continue typing to enter what you want to filter on. This functions the same as this field on the Logging **Search** page.

   **Note:**
   If you want to find log events with a specific status code, include quotes ("') around the code to avoid results that have those numbers embedded in a longer string.

8. In **Filter by Time**, select from one of the preset time periods:
   - Past 5 Minutes (the default)
   - Past 15 Minutes
   - Past Hour
   - Past 3 Hours
   - Today
   - Custom (choose your own using the **Start Date** and **End Date** fields)
9. After entering your search text or filters, click **Apply**.

   **Note:**
   Since the **Audit** page automatically refreshes after applying filters, you do not need to click the **Apply** button as you select different filters. You will, however, need to click **Apply** again after some time has passed and new logs have appeared.

The **Convert to search** option allows viewing your Audit Log results in the **Search** page, to further search and perform analysis across other logs in the system. When you use this option, the **Advanced Search** version of the **Search** page is filled with the chosen filter parameters (available in the **Query** field).

Click **View query syntax** to view the actual syntax query statement(s) associated with your filter settings. If you have applied multiple filters for a field, you can view how the query is constructed in terms of the combined OR and AND statements.

**Exploring the Details of Events**

On the **Explore Events** tab, each log entry is organized in terms of the **Event Time**, **User**, **Resource**, **Type**, **Action**, and **Status**. Click and expand an audit log entry. Each entry displays the log data in a JSON field view, similar to the **Search** page, where you can collapse and expand nodes, or click the copy icon to copy the log entry to the clipboard.

**To export log data**

At the top right portion of **Explore Events**, click **Export Log Data (JSON)**. This feature allows you to export the log data to a JSON file that you can save to your system.
Viewing the Activity Stream

Click the **Activity Stream** tab to view the audit logs as a visual sequential list (by date, from newest to oldest log event). You click and expand an event to display the event in JSON format, and you can click the copy icon to copy the audit event to the clipboard.

Exporting Audit Events

Audit events can be exported using Service Connector Hub.

Audit Schema

See [Version 2 Audit Log Schema](#) on page 488 for more information on the audit logging schema.

Custom Logs

Custom logs are logs that contain diagnostic information from custom applications, other cloud providers, or an on-premise environment. Custom logs can be ingested in the following ways:

- By using PutLogs to ingest custom logs directly. See the Logging Ingestion API and REST APIs on page 4368 for more information. Also see [Using the API](#) on page 2634 for an example log entry payload that can be used with PutLogs.
- By configuring the Unified Monitoring Agent. See [Installing the Agent](#) on page 2621 for instructions.

**Note:**

When managing Oracle Cloud Agent plugins, the Unified Monitoring Agent is referred to as "Custom Logs Monitoring".

Custom logs can be viewed in the Oracle Cloud Infrastructure Compute instance page, and have an associated **Logs** resource. They can also be viewed on the Logging **Search** page, **Logs** page, or within an associated **Log Groups** detail page. Custom logs are also supported in bare metal instances.

The agent can be installed on many machines, and it pulls logs from local directories, where your apps or systems emit logs. The agent can also parse your logs for you. All of this is configured in **Agent Configurations**. You can create an agent configuration separately, and then associate a custom log with it, or create a custom log and then later create its agent configuration.

An agent configuration is the central mechanism for defining:

- What hosts you want logs from.
- What specific logs you want from the hosts.
- Additional parsers.
- The custom log destination.

Creating a custom log is a two-step process, in that you create the custom log object first, and then second, create its associated agent configuration. See [Creating Custom Logs](#) on page 2619 for more information on creating custom logs and agent configurations, and **Agent Management** on page 2621 for more information on setting up and managing the agent.

**Note:**

For the agent to run correctly, ensure that your firewall settings allow the following URI endpoints:

- https://auth.<your region>.oraclecloud.com

Creating Custom Logs

To create custom logs:
1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Logs.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. In Custom Log Name, enter a name for the custom log. Avoid entering confidential information.
4. From Compartment, choose a compartment you have permission to work in.
5. From Log Group, select a log group to place the custom log into.
6. Optionally, select a log retention value from Log Retention, and add any applicable tags in Add Tags.
7. Click Create Log Object. The Create Agent Configuration panel is displayed. You can next create a new configuration, to define the parameters for the associated log data (the default), or add it later.
8. In Name and compartment, enter a Configuration Name in the corresponding field, and select a Compartment you have permissions to work in.
9. In Choose Host Groups, which allows you to define which VMs apply to this configuration, select a Group Type from the list, whether Dynamic Group or User Group.

For the Dynamic Group case, Dynamic Group refers to a group of instances, which you can create in the IAM feature of the Console. See About Dynamic Groups on page 2422 for more information. These Dynamic Groups can be selected from the Groups field when setting up Dynamic Group settings.

For the User Group case, select the group from the Groups field. User Groups also refer to the IAM Groups feature of the Console. See Managing Groups on page 2419 for more information.

Click Add Host Group to add more groups. You can add a combination of Group Types for the agent configuration, that is, both Dynamic Groups and User Groups can be set up in the configuration.

Note:
A maximum of five groups per configuration are allowed, and a host can be in a maximum of five different groups.

10. Next, in the configuration, you need to define the format of the logs (that is, what logs do you want to watch for) in Configure Log Inputs. Select an Input Type from the list, whether Windows Event Log or Log Directory.

- For Windows Event Log, enter an Input Name and select an Event Channels option from the list.
- For Log Directory, enter an Input Name and a Path in the corresponding fields. For example, /<log_path>/<log_name>. Multiple paths can be entered.

Click Advanced Parser Options, which opens the Advanced Parser Options panel. This allows you to specify how to parse the log, according to the following parsers. Some of the parsers require further input and have more options, depending on the type chosen.

- AUDITD
- JSON
- TSV
- CSV
- NONE (the default)
- SYSLOG
- APACHE2
- APACHE_ERROR
- MSGPACK
- REGEXP
- multiline

For example for JSON, you must select a Time Type value from the list, while optionally, you can specify event time and null field settings. Meanwhile for REGEXP, you specify the regular expression for matching logs, along with the time format. See Log Inputs and Parsers on page 2626 for more information.

11. After configuring the log inputs and the parser, you can optionally specify any tag settings. Click Submit to save your changes, and create the custom log and its associated agent configuration.

In summary, the agent configuration defines what instances the configuration applies to (Choose Host Groups), which log files are obtained and what parser (if any) is used (Configure Log Inputs), and to what log object in the
Oracle Cloud Infrastructure system that the records are pushed to (Select log destination). The latter is already set up since this was set during the custom log creation step.

The custom log object is now created, as well as the agent configuration, which pulls data from instances, and pushes into the custom log object.

Agent Management

To ingest events from your applications into your custom log, you can install the Oracle fluentd-based agent. This agent allows you to control exactly which logs you want to collect, how to parse them, and more.

Note:
The Unified Monitoring Agent is a fully managed agent, and custom client configuration is not officially supported. For example, gathering logs from remote sources is not recommended, since doing so can have serious security implications (because the log source cannot be verified).

Oracle Cloud Infrastructure Logging provides an easy mechanism (Agent Configurations) to enable and manage the agent for a set of supported operating systems. Agent Configurations give you a central experience to easily configure what custom logs you want to ingest across your fleet of hosts. The following are the supported operating systems for agent configurations:

- Oracle Linux 7, Oracle Linux 8
- CentOS 7, CentOS 8

Note:
For Linux, only register Linux-specific input types, such as "Log Path", for a dynamic group that includes only a Linux instance. For Windows, only register Windows-specific input types, such as "Windows event log", for a dynamic group that includes only a Windows instance. Otherwise, the Unified Monitoring Agent malfunctions if you register a Windows input type for a Linux instance, and vice versa.

Installing the Agent

New Oracle Cloud Infrastructure Instances

For supported operating systems, you can enable the agent directly during creation time. The Custom Logs Monitoring plugin must be enabled, and all plugins must be running. See Managing Plugins with Oracle Cloud Agent on page 740 for more information.

Existing Oracle Cloud Infrastructure Instances

For existing instances with supported operating systems, the Custom Logs Monitoring plugin must be enabled, and all plugins must be running. See Managing Plugins with Oracle Cloud Agent on page 740 for more information.

If you already have the monitoring plugin enabled, then your instance will be automatically patched to install the agent by September 18, 2020. Otherwise, you can follow the manual installation instructions:

Linux:
1. Connect to the instance.
2. You can obtain the agent by using this script, and then run the script to download the agent. For example:

   ```bash
   ./downloadAgent.sh centos7
   ./downloadAgent.sh centos8
   ./downloadAgent.sh oel7
   ./downloadAgent.sh oel8
   ```
Logging

./downloadAgent.sh windows

Otherwise, you can download the agent for the following individual operating systems:

- Oracle Linux 7 RPM: https://objectstorage.us-phoenix-1.oraclecloud.com/n/axmjwnk4dzjv/b/unified-monitoring-agent-ol7-repo/o/unified-monitoring-agent-0.0.5.rpm
- Oracle Linux 8 RPM: https://objectstorage.us-phoenix-1.oraclecloud.com/n/axmjwnk4dzjv/b/unified-monitoring-agent-ol8-repo/o/unified-monitoring-agent-0.0.5.rpm
- CentOS 7 RPM: https://objectstorage.us-phoenix-1.oraclecloud.com/n/axmjwnk4dzjv/b/unified-monitoring-agent-centos7-repo/o/unified-monitoring-agent-0.0.5.rpm
- CentOS 8 RPM: https://objectstorage.us-phoenix-1.oraclecloud.com/n/axmjwnk4dzjv/b/unified-monitoring-agent-centos8-repo/o/unified-monitoring-agent-0.0.5.rpm

For the FIPS-enabled agent:

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance is impacted when using the FIPS-enabled agent.</td>
</tr>
</tbody>
</table>


3. Run the following command to install the RPM:

```
yum install -y <rpm-name>
```

Windows:

1. Connect to the instance.
2. Download the agent from: https://objectstorage.us-phoenix-1.oraclecloud.com/n/axmjwnk4dzjv/b/unified-monitoring-agent-windows-repo/o/unified-monitoring-agent-0.0.5.msi
3. Open an elevated command prompt (running as Administrator), and run the MSI command (installation can take up to five minutes to complete):

```
C:\path\to\file\unified-monitoring-agent-0.0.2.msi
```
4. For a more advanced version of the preceding command (to debug MSI installation issues), run:

```
msiexec /i "C:\path\to\file\unified-monitoring-agent-0.0.2.msi" /l*v "C:\unified-monitoring-agent_msi.log"
```

Instances Created from Custom Images and Non-Oracle Cloud Infrastructure Instances

1. Install the agent according to the same steps in Existing Oracle Cloud Infrastructure Instances on page 2621.
2. Configure User API keys for the instance you are running on. To generate the user API key, follow the instructions described in How to Generate an API Signing Key on page 4180.
   - (Linux) Step 2a. Place the ".oci" directory and its contents under /etc/unified-monitoring-agent.
   - (Windows) Step 2a. For Windows, there are a few steps that differ, so ensure to follow the appropriate steps. Create the ".oci" folder and its contents in the directory C:\oracle_unified_agent.
3. Follow the instructions described in 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049, to create the configuration file with the modifications in the next step.
4. After following the steps in 2. Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File on page 2049, ensure to name the profile (<profile-name>) for this section as "UNIFIED_MONITORING_AGENT".

The following is an example of what the configuration looks like for the Unified Monitoring Agent to use for authentication with the service:

```
[UNIFIED_MONITORING_AGENT]
user=ocid1.user.region..aaa...
fingerprint=<cert fingerprint>
key_file=/path/to/ocifolder/.oci/private.pem
tenancy=ocid1.tenancy.region..aaa...
region=<instances region>
pass_phrase="pashphrase1234"
```

Verify Agent Installation

**Windows:**

1. Connect to the instance.
2. Open Services.msc (Start menu and type services.msc). Scroll until you see the "Oracle Unified Monitoring Agent" and that the agent is in a "Running" state.
3. In the Task Scheduler under Task Scheduler Library, verify that the UnifiedAgentConfigUpdater exists, and has (or will) run successfully. After the initial install, it can take up to 20 minutes for the first run. If preferred, this can be run manually.
4. After the UnifiedAgentConfigUpdater task has run, verify that a "unified-monitoring-agent.conf" file in exists in C:\oracle_unified_agent.
5. After a few minutes, supervisor (unified-monitoring-agent-supervisor-0.log) logs and worker (unified-monitoring-agent-0.log) logs appear in the C:\oracle_unified_agent directory.
6. The preceding logs contain the Fluentd parser and plugin output.

**Oracle Linux 7, Oracle Linux 8, CentOS 7, and CentOS 8:**

1. Connect to the instance.
2. Check that the agent is running by running the following command:

   ```
   systemctl status unified-monitoring-agent
   ```
3. The status looks like the following:

   ```
   Loaded: loaded (/usr/lib/systemd/system/unified-monitoring-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2020-09-10 18:11:45 GMT; 2h 14min ago
   Docs: https://docs.cloud.oracle.com/
   ```

Managing Agent Configurations

To use agent configurations, you must be running an Oracle Cloud Infrastructure instance with the supported operating system (see Agent Management on page 2621). Agent configurations give you a central experience to easily configure what custom logs you want to ingest across your fleet of hosts. A configuration allows you to select:

- Which hosts you want to collect logs from.
- Exactly which logs you want to ingest from those hosts.
- A log group/log destination.

Configurations are managed through the Console and Logging API. In addition, since you can choose to create an agent configuration later after creating a custom log, you can use the Agent Configurations page to set up the agent configuration and point it to your custom log.

The Agent Configurations page is organized in terms of the following:

- Name
- Config OCID
To create a new agent configuration

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Agent Configurations. The Agent Configurations page is displayed.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. Click Create Agent Config. The Agent Configurations panel is displayed.
4. In Name and compartment, enter a Configuration Name in the corresponding field, and select a Compartment you have permissions to work in. Avoid entering confidential information.
5. In Choose Host Groups, select a Group Type from the list, whether Dynamic Group or User Group. Click Add Host Group to add more groups.
6. In Configure Log Inputs, select an Input Type form the list, whether Windows Event Log or Log Directory.
   - For Windows Event Log, enter an Input Name and select an Event Channels option from the list.
   - For Log Directory, enter an Input Name and a Path in the corresponding fields.
7. In Select log destination, the User Group or Dynamic Group in the configuration that you select in Compartment needs to have permission to work in the compartment. Select the Log Group, and the Log Name from the corresponding drop-down lists. The Log Name can only point to a custom log and the custom log must exist in the chosen log group for the configuration to work.
8. Optionally, after clicking Show Additional Options, specify any preferred tag settings.
9. Click Create. The agent configuration is created and appears in the Agent Configurations page.

To view an agent configuration

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Agent Configurations. The Agent Configurations page is displayed.
2. Under List Scope, Compartment, choose a compartment you have permission to work in.
3. Click the linked agent configuration name under Name in the table. The agent configuration detail page is displayed. This page displays the following on the Log Information tab:
   - OCID
   - Compartment
   - Created date and time in UTC format
   - Status (Creating, Active, Updating, Inactive, Deleting, Deleted)
   - The Tags tab shows associated tags for this log.
   - Under Log Details the following is displayed: the compartment, the linked log group and log name.

In the Configuration resource, the Host Group and Log Input configuration settings are listed in corresponding tables. Under Host Group you can view the Group Type, Group Name, and the OCID. Click the linked Group Type (whether a User Group or Dynamic Group), which opens the IAM Groups or Dynamic Groups section of the Console, respectively. See Managing Groups on page 2419 and About Dynamic Groups on page 2422 for more information.

Under Log Input you can view the Input Type, Input Name, File Paths, Parser, and Parser Parameters (if applicable for the chosen parser).

In the Explore Log resource, log data is displayed in a similar manner as the Log Data on the Search page. You can apply some simple filters, such as sorting by newest or oldest from the Sort field, or filtering by time from the corresponding Filter by Time field.

Clicking Explore with Log Search allows you to view this log on the Search page directly. After clicking this link, the Search page opens with the Select Logs to Search field populated with the log in the filter settings. At this point, you can perform more analysis and investigation related to this log directly on the Search page. For more information, see Searching Logs on page 2634.

To edit an agent configuration
Logging

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Agent Configurations**. The **Agent Configurations** page is displayed.

2. Under **List Scope, Compartment**, choose a compartment you have permission to work in.

3. Click the linked agent configuration name under **Name** in the table. The agent configuration detail page is displayed.

4. Click **Edit**. The **Agent Configurations** panel is displayed.

   From the main **Agent Configurations** page, for the agent configuration you want to edit, you can also click the the Actions icon (three dots), and then click **Edit** to access the **Agent Configurations** panel.

5. Make your changes and click **Update**.

**To enable or disable an existing agent configuration**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Agent Configurations**. The **Agent Configurations** page is displayed.

2. Under **List Scope, Compartment**, choose a compartment you have permission to work in.

3. Click the linked agent configuration name under **Name** in the table. The agent configuration detail page is displayed.

4. Click **Disable/Enable**. A confirmation dialog is displayed regarding the disabling or enabling of the agent configuration.

5. Confirm by clicking **Disable/Enable**. The agent configuration detail page changes its status and displays **Inactive** (for a disabled configuration), or **Active** (for an enabled configuration) in the status field, both on the agent configuration detail page and the **Agent Configurations** page.

   From the main **Agent Configurations** page, for the agent configuration you want to disable/enable, you can also click the the Actions icon (three dots), and then click **Disable/Enable**.

**To delete an agent configuration**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Agent Configurations**. The **Agent Configurations** page is displayed.

2. Under **List Scope, Compartment**, choose a compartment you have permission to work in.

3. Click the linked agent configuration name under **Name** in the table. The agent configuration detail page is displayed.

4. Click **Delete**. A confirmation dialog is displayed regarding the delete operation.

5. Confirm by clicking **Delete**. The agent configuration is removed from the **Agent Configurations** page.

   From the main **Agent Configurations** page, for the agent configuration you want to delete, you can also click the the Actions icon (three dots), and then click **Delete**.

**To move an agent configuration to a different compartment**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Agent Configurations**. The **Agent Configurations** page is displayed.

2. Under **List Scope, Compartment**, choose a compartment you have permission to work in.

3. Click the linked agent configuration name under **Name** in the table. The agent configuration detail page is displayed.

4. Click **Move Resource**. The **Move Resource to a Different Compartment** dialog is displayed.

5. Choose the new compartment and then click **Move Resource**.

   From the main **Agent Configurations** page, for the agent configuration you want to move to a new compartment, you can also click the the Actions icon (three dots), and then click **Move Resource**.

**Selecting Target Hosts with Dynamic Groups**

To set up a configuration for multiple hosts, you can use the **Dynamic Group** feature from IAM. The overall process first involves creating a compartment, then placing all the instances in the compartment you want to collect logs from. Next, you can create the Dynamic Group. The Dynamic Group policy statement would then point to the compartment that contains the instances. Lastly, create a log group, custom log, and its associated agent configuration.
Logging

Set the following policy statement:

```
allow dynamic-group <dynamic_group_name> to use log-content in tenancy
```

This policy statement allows the agent configuration to push logs to the Logging service backend, which you can later see in the Logging Service's Search page.

In the Dynamic Groups configuration, set up your Dynamic Group to have a rule that includes all the agents that you want to use to send logs to the Logging service. For example, in a Rule inside the Dynamic Group it can state:

```
ANY {instance.id = 'ocid1.instance.<region>.<location>.<unique_ID>',
     instance.compartment.id = 'ocid1.compartment.<region>..<unique_ID>'}
```

If you remove `instance.id = 'ocid1.instance.<region>.<location>.<unique_ID>'` and just have:

```
ANY {instance.compartment.id = 'ocid1.compartment.<region>..<unique_ID>'}
```

this means use all the instances under this compartment to send logs. For more information on Dynamic Groups, see About Dynamic Groups on page 2422.

Next, create the log group (see To create a log group on page 2583). After the log group is created, you can then create the custom log and the agent configuration (see Creating Custom Logs on page 2619 for steps to create the custom log and agent configuration). During the agent configuration, you can use the Dynamic Group you created earlier and select it in the Choose Host Groups section of the Agent Configurations panel. This links the log configuration with the instance you want to send logs to. Once the agent configuration is active, the logs you see are sent by the instance, inside the Dynamic Group you earlier set up. You can later click Explore with Log Search in the agent configuration to view the logs through the Search page (see Searching Logs on page 2634).

Log Inputs and Parsers

Agent configurations allow you to easily select which types of logs you want to ingest, and how to parse them. The following are the supported log inputs in agent configurations:

- Windows Event Logs
- Log Directory (Tail)

For Log Directory inputs, you can specify parsers to structure your logs. The following are the list of supported parsers:

- None
- Auditd (https://github.com/linux-audit/audit-documentation/wiki)
- JSON (https://docs.fluentd.org/parser/json)
- CSV (https://docs.fluentd.org/parser/csv)
- TSV (https://docs.fluentd.org/parser/tsv)
- Syslog (https://docs.fluentd.org/parser/syslog)
- Apache2 (https://docs.fluentd.org/parser/apache2)
- Apache_Error (https://docs.fluentd.org/parser/apache_error)
- Msgpack (https://docs.fluentd.org/parser/msgpack)
- Regexp (https://docs.fluentd.org/parser/regexp)
- Multiline (https://docs.fluentd.org/parser/multiline)

Log Destination

You can choose the exact log group and log object where you want your log events to be indexed. All incoming log events from your hosts are ingested and indexed in your selected log object. After they are ingested, you can view and search your log events on the Search page (see Searching Logs on page 2634). All existing Oracle Cloud Infrastructure Identity and Access Management policies in both the log group and compartment apply both during ingestion and search. So, only authorized users can view and ingest logs in your tenancy.
Logging

Viewing Custom Logs in a Compute Instance

The Logs resource on a Compute Instance page allows you to view logging details for the instance in the selected compartment. Logging Search APIs are called and any available logs are pulled for the instance. Instances can have a customer application running on them (for example, a gaming server), and they can configure logs from the gaming server to be collected by the Unified Monitoring Agent, and then be pushed into the Logging service and be indexed there. Logs are pulled and displayed on the Logs resource. As such, when a customer views their Compute instance, they can see that their application is pushing logs to the Logging service. Logs, however, cannot be enabled or created from this interface.

Under Explore Logs, you can sort log entries (Newest, the default or Oldest), or filter by time (the default Past 5 minutes, Past 15 minutes, Past hour, Past 24 hours, Today, Custom). Otherwise the functionality is the same as when you are viewing logs under Log Data in the central logging Search page (see Using the Console on page 2635).

Click Explore with Log Search to open the central logging Search page, where you can add or remove filters and so on. The Search page loads with instanceid of the instance already set as a filter under Filters.

Click Create Custom Log to open the central Logs page, where you can create custom logs for the instance. Custom logs are sent from Oracle Cloud Infrastructure Compute VM instances.

For the Logs resource to be available on such an instance, the following is required:

- The Custom Logs Monitoring plugin must be enabled, and all plugins must be running. For more information, see Managing Plugins with Oracle Cloud Agent on page 740.
- The instance must have one of the supported operating systems:
  - Oracle Linux 7, Oracle Linux 8
  - CentOS 7, CentOS 8

If the operating system is not supported, then this Logs resource is not displayed. If the operating system is supported by the Oracle Cloud Agent and is not enabled, a warning is displayed that you must enable the agent to create logs.

Agent Troubleshooting

The following topics describe troubleshooting tips related to the Unified Monitoring Agent, for both Linux and Windows.

Hardware Requirements

Depending on your logging requirements and configuration (number of logs, type of buffering, and so on), the hardware requirements and performance of the Unified Monitoring Agent can vary widely. When no operational pressure is present (less than 1,000 log events per minute), the agent should not consume more than 200 MB of RAM, and 20% of a CPU core. The Unified Monitoring Agent service hard-coded limits are 5 GB RAM, and 40% of a core. 1 GB of RAM is also recommended.

Enabling Monitoring

Monitoring can aid with troubleshooting. See Enabling Monitoring for Compute Instances on page 783 for more information on how you can enable monitoring (metrics and logging) in your Oracle Cloud Infrastructure Compute instances.

Linux

systemd Units

The Unified Monitoring Agent is based on systemd units, and is composed of the following components:

1. unified-monitoring-agent.service: The main Unified Monitoring Agent service.
2. unified-monitoring-agent_config_downloader.service: The configuration automatic updater service.
3. **unified-monitoring-agent_config_downloader.timer**: The timer unit, which triggers the automatic downloader service on specified, randomized, intervals.

4. **unified-monitoring-agent_restarter.path**: The path unit, which triggers the reload of the configuration by the Unified Monitoring Agent, if a change is detected (because of a new configuration being downloaded by the automatic updater service).

**Note:**
Remember that most of the `systemctl` or `journalctl` commands must be run with super user privileges (either as `root`, or through `sudo`).

To verify the correct operation of these systemd units, you can use the `systemctl` command like the following:

```bash
systemctl status <unit_name>
```

Where `<unit_name>` must be replaced with one of the following values:

1. **unified-monitoring-agent.service**
2. **unified-monitoring-agent_config_downloader.service**
3. **unified-monitoring-agent_config_downloader.timer**
4. **unified-monitoring-agent_restarter.path**

Typically these `systemctl` commands show output similar to the following:

```bash
systemctl status unified-monitoring-agent.service
# unified-monitoring-agent.service - unified-monitoring-agent: Fluentd based data collector for Oracle Cloud Infrastructure
    Loaded: loaded (/usr/lib/systemd/system/unified-monitoring-agent.service; enabled; vendor preset: disabled)
    Active: active (running) since Tue 2020-09-29 13:54:03 UTC; 1min 37s ago
      Docs: https://docs.cloud.oracle.com/
      Process: 2337 ExecReload=/bin/kill -USR2 ${MAINPID} (code=exited, status=0/SUCCESS)
      Main PID: 2327 (fluentd)
      Memory: 66.3M (limit: 5.0G)
      CGroup: /system.slice/unified-monitoring-agent.service
```

```bash
systemctl status unified-monitoring-agent_config_downloader.timer
# unified-monitoring-agent_config_downloader.timer - Run unified-monitoring-agent configuration automatic updater.
```

```bash
systemctl status unified-monitoring-agent_config_downloader.service
# unified-monitoring-agent_config_downloader.service - unified-monitoring-agent_config_downloader.service
    Loaded: loaded (/usr/lib/systemd/system/unified-monitoring-agent_config_downloader.service; enabled; vendor preset: disabled)
    Active: inactive (dead) since Tue 2020-09-29 13:54:38 UTC; 1min 30s ago
      Main PID: 2333 (code=exited, status=0/SUCCESS)
```
Logging

The most important parts of the systemctl command output are the Loaded and Active fields. The Loaded field has the value loaded for all system units. The Active field has the following values:

- active (running) for the unified-monitoring-agent.service unit.
- active (waiting) or active (running) for the unified-monitoring-agent_restarter.path and the unified-monitoring-agent_config_downloader.timer units.
- active (running) or inactive (dead) for the unified-monitoring-agent_config_downloader.service unit. For the latter value, the field Main PID includes the value code=exited, status=0/SUCCESS).

Processes

Another way to further verify the correct operation of the Unified Monitoring Agent, is to check the system’s running processes. When operating correctly, the Unified Monitoring Agent runs two processes: one supervisor process, and one worker process. You can verify their existence by running the following command in a terminal (sample output included):

```
ps aux | grep unified-monitoring-agen[t]
```

As shown in the preceding sample, there are two processes running, with the same arguments, except for the extra –under-supervisor added to the second one. This denotes the worker process, thus making the process without this parameter the supervisor.

Logs

**Note:**

Remember that most of the systemctl or journalctl commands must be run with super user privileges (either as root, or through sudo).

The Unified Monitoring Agent logs are available at /var/log/unified-monitoring-agent/unified-monitoring-agent.log. This file includes logs from the Unified Monitoring Agent itself.

Besides the agent’s logs, which do not contain system-related events (for example, service start, service stop, and so on), you can also view the logs from journald, systemd's system logging service. To view the system logs specific to a unit, you can use the journalctl command like the following:

```
journalctl -u <unit_name>
```

Where <unit_name> must be replaced with one of the following values:
1. `unified-monitoring-agent.service`
2. `unified-monitoring-agent_config_downloader.service`
3. `unified-monitoring-agent_config_downloader.timer`
4. `unified-monitoring-agent_restarter.path`

When querying `journald` logs through `journalctl`, you can also define specific time ranges:

```
journalctl --since "2020-12-30 00:00:01" --until "2020-12-31 23:59:59"
```

The date format used is `YYYY-MM-DD HH:MM:SS`.

You can also tail the journal logs, by adding the `-f` parameter:

```
journalctl -f
```

**Troubleshooting Scenarios**

**Problem:** The Unified Monitoring Agent is not installed.

**Solution:** For newly created instances, it can take up to 25 minutes for the automatic installation of the agent. If it is not installed after this time period, check the following:

1. The network connectivity of the instance.
2. Whether monitoring is enabled in the Console.

You can also check the log file `/var/log/oracle-cloud-agent/plugins/unifiedmonitoring/unifiedmonitoring.log` for information regarding the installation of the Unified Monitoring Agent by the Oracle Cloud Agent.

**Problem:** The Unified Monitoring Agent is not running. Its status is not loaded/active, nor are both supervisor and worker processes running.

**Solution:** Restart the Unified Monitoring Agent and check the logs for any problems:

```
systemctl restart unified-monitoring-agent
```

**Problem:** Configuration is not automatically downloaded.

**Solution:** Ensure you have followed the steps in Installing the Agent on page 2621 and Verify Agent Installation on page 2623. Consult the journal of the automatic configuration updater service by running:

```
journalctl -u unified-monitoring-agent_config_downloader.service
```

**Problem:** Configuration is not automatically reloaded.

**Solution:** Ensure you have followed the steps in Installing the Agent on page 2621 and Verify Agent Installation on page 2623. Consult the journal of all the units:

1. The timer unit must have run at least one time.
2. The automatic configuration download service must have run after the relevant time unit has triggered it. You can verify from its logs that the configuration has been downloaded and extracted to the Unified Monitoring Agent's configuration directory. You can also verify this by listing the files in that directory:

   ```
   ls -lhatR /etc/unified-monitoring-agent
   ```

3. Verify that the path unit is active by checking its status:

   ```
   systemctl status unified-monitoring-agent_restarter.path
   ```

4. Verify that a reload signal has been received by the Unified Monitoring Agent, by inspecting its journal:

   ```
   journalctl -u unified-monitoring-agent_config_downloader.service "Reloading unified-monitoring-agent" appears in the output of this command.
   ```

**Problem:** You are testing your parsing pattern and need to force the agent to download the configuration right away.
**Solution**: Run the following command:

```
systemctl restart unified-monitoring-agent_config_downloader
```

**Note:**
Automatic update of the configuration on the agent side can take up to 30 minutes.

**Data Collection**

If you want to open a ticket so an engineer can help you with your problem regarding the Unified Monitoring Agent, include the output of the following commands. Super user privileges might be required for some of them.

```
yum info unified-monitoring-agent
rpm -ql unified-monitoring-agent | xargs sha512sum
systemctl status --full unified-monitoring-agent.service
systemctl status --full unified-monitoring-agent_config_downloader.service
systemctl status --full unified-monitoring-agent_config_downloader.timer
systemctl status --full unified-monitoring-agent_restarter.path
journalctl -a --no-pager -u unified-monitoring-agent.service
journalctl -a --no-pager -u unified-monitoring-agent_config_downloader.service
journalctl -a --no-pager -u unified-monitoring-agent_config_downloader.timer
journalctl -a --no-pager -u unified-monitoring-agent_restarter.path
```

Also include an archive of the files under `/var/log/unified-monitoring-agent/` and `/var/log/oracle-cloud-agent/`. You can create a gzipped tar archive of these directories with the command:

```
tar cvzf agent_logs_${(date +%s)}.tar.gz /var/log/unified-monitoring-agent/ /var/log/oracle-cloud-agent/
```

If the Unified Monitoring Agent is running but has erratic behavior, you can also include backtrace and memory profile information, by running the following command and including the files `/tmp/sigdump-<integer>.log` in your report (where `<integer>` is an integer with 1–6 digits, even though in rare cases it might have more than that).

```
ps aux | grep unified-monitoring-agent[t] | grep ruby | awk '{print $2}' | xargs kill -SIGCONT
```

What this command does is to find the Unified Monitoring Agent process PIDs, and send them the SIGCONT signal, which causes a dump to be generated in `/tmp/sigdump-<integer>.log`.

**Uninstall and Reinstall**

You can remove the Unified Monitoring Agent, without removing the agent's configuration, by running the following command:

```
yum -y remove unified-monitoring-agent
```

The agent's configuration remains under the `/etc/unified-monitoring-agent/` directory. If you do not want to keep the configuration for a future (re)installation of the Unified Monitoring Agent package, you need to remove it manually:

```
# use the following command to print the contents of the agent's configuration directory
find /etc/unified-monitoring-agent/
# use the following command to remove the directory and all of its contents
# (this step cannot be undone)
```
The agent is automatically reinstalled by the Oracle Cloud Agent, at most 25 minutes. You need to have monitoring enabled for your instance in the Console for this to occur. See Managing Plugins with Oracle Cloud Agent on page 740 for more information.

**Windows**

**Unified Monitoring Agent Troubleshooting Steps**

**Check the service status:**

1. The agent runs as part of a Windows service, to see its status, open the start menu and type Services.msc and open it. Go to the service Oracle Cloud Unified Monitoring Service to see the status.
2. Right-click the service and select Properties for more information. Start/stop/restart are available here.
3. From the Start menu type cmd, right-click on Command Prompt and select Run as Administrator. Run the following commands:
   - To view Unified Monitoring Agent service status:
     ```bash
     sc query unified-monitoring-agent
     ```
   - Restart the Unified Monitoring Agent service:
     ```bash
     sc stop unified-monitoring-agent
     sc start unified-monitoring-agent
     ```

   **Note:**
   The preceding commands do not work in PowerShell, so you must instead use the Windows Command Prompt.

**Find Windows Service errors:**

1. From the Start menu, type Event Viewer and select it.
2. Open Windows Logs, then System. Every time a service starts or stops, fails to do either, or crashes suddenly, it is recorded here.

   **Note:**
   On most Windows machines, there is a cap on how many events can be in the event viewer. As a result, if an event happened a long time ago, the logs might not be available.

**Fluentd logs:**

1. Open explorer.exe (file icon on the task bar)
2. Go to C:\oracle_unified_agent.
3. If there is only one file, it means that there isn’t a valid configuration file on the machine.
4. If there are two files, then there is a supervisor log that will have all the setup/start-up logs, and a worker log with all the parsing/output logs. unified-monitoring-agent.conf is the name of the configuration file if it has been downloaded properly.
5. Run Fluentd manually. Try the preceding steps to identify the issue, but if needed, you can debug an issue by manually running Fluentd.

   **Note:**
   Running Fluentd manually runs it in the Windows service, which stops the service from running as normally, which is different behavior than on Linux.
6. Use the following command to run Fluentd manually. This can be run in PowerShell or Command Prompt, but it needs to be run as Administrator:

```
C:\oracle_unified_agent\unified-monitoring-agent\embedded\bin\fluentd -c C:\oracle_unified_agent\unified-monitoring-agent.conf -vv
```

**Automatic Configuration Updater Troubleshooting Steps**

1. Verify Task Scheduler is running as expected.
2. From the Start menu, and type Task Scheduler.
3. Go to Task Scheduler (Local), then Task Scheduler Library. Find the task named UnifiedAgentConfigUpdater.
4. Verify the Last Run Time. If it was at an invalid date, or it says not run, then the Next Run time will be when it should run for the first time. For debugging, select the task and select Run if you need it to run immediately.
5. Last Run Result specifies the outcome of downloading the configuration from the control plane. If there is an error result, you need to run it manually to determine what happened. Task Scheduler does not keep output logs.
6. Run the configuration updater manually.

**Note:** Run the updater in PowerShell as an Administrator for the best experience.

```
C:\oracle_unified_agent\unified-monitoring-agent\embedded\bin\ruby.exe C:\oracle_unified_agent\unified-monitoring-agent\embedded\lib\ruby\gems\2.6.0\gems\fluent-public-config-updater-0.0.1\lib\fluent_config_updater.rb -c C:\oracle_unified_agent -b 10
```

**Oracle Cloud Agent Troubleshooting Steps**

Check the Oracle Cloud Agent logs. For Windows Server 2012r2 or 2016, the log file locations are:

- C:\Users\OCA\AppData\Local\Local\OracleCloudAgent\agent.log
- C:\Users\OCAUM\AppData\Local\OracleCloudAgent\plugins\unifiedmonitoring \unifiedmonitoring.log (runtime logs)
- C:\Users\OCAUM\AppData\Local\OracleCloudAgent\plugins\unifiedmonitoring \unifiedmonitoring_msi.log (install logs)
- C:\oracle_unified_agent\unified-monitoring-agent-0.log (agent worker log, which might not exist depending on state)
- C:\oracle_unified_agent\unified-monitoring-agent-supervisor-0.log (agent supervisor log, which might not exist depending on state)

Windows Server 2019 log file locations:

- C:\Windows\ServiceProfiles\OCA\AppData\Local\OracleCloudAgent\agent.log
- C:\Windows\ServiceProfiles\OCAUM\AppData\Local\OracleCloudAgent\plugins \unifiedmonitoring\unifiedmonitoring.log (runtime logs)
- C:\Windows\ServiceProfiles\OCAUM\AppData\Local\OracleCloudAgent\plugins \unifiedmonitoring\unifiedmonitoring_msi.log (install logs)
- C:\oracle_unified_agent\unified-monitoring-agent-0.log (agent worker log, which might not exist depending on state)
- C:\oracle_unified_agent\unified-monitoring-agent-supervisor-0.log (agent supervisor log, which may not exist depending on state)

**Intermittent Failed MSI Install**

An intermittent failed MSI install can occur for one of two reasons:
1. An MSI installation was interrupted (system reboot, process stop, and so on), and on the second run, the msiexec.exe process is still holding a file handle to a folder that it created.
2. During an upgrade where the MSI fails to get access to the main agent folder, because Ruby.exe doesn’t end like it should (a Fluentd issue). This causes the MSI to fail and to clean up the system, removing much of the agent (not the position or buffer files though).

In both instances, a second install or letting Oracle Cloud Agent run through the install a second time resolves this issue. If it still is stuck in this state do the following:

1. Stop all msiexec and ruby processes in Task Manager, Details.
2. Rename C:\oracle_unified_agent to C:\oracle_unified_agent_old.
3. Install the agent again, or wait for Oracle Cloud Agent to install it.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operation to ingest custom logs directly:

- **PutLogs**

The following is a sample log entry payload that can be used with PutLogs:

```json
{
   "specversion": "1.0",
   "logEntryBatches": [
      {
         "entries": [
            {
               "data": "Random test",
               "id": "sha123",
               "time": "2020-11-25T21:10:29.600Z"
            }
         ],
         "source": "hostname",
         "type": "sampleType",
         "subject": "/var/application.log",
         "defaultlogentrytime": "2020-11-25T21:10:29.600Z"
      }
   ]
}
```

**Searching Logs**

This topic describes how to search your logs using the **Search** page.

**Overview of Log Search**

Logging provides a powerful tool to search indexed logs. Use the Console to perform any of the following tasks:

- Search logs, whether in a basic user interface mode, or by typing custom queries in an advanced mode.
- Filter on values in logs, whether by log fields, text search, or time intervals, all in terms of chosen compartments or log groups.
- Visualize log data in a bar chart view, along with accompanying tabular data.
- Explore each log line in more detail. View the raw JSON payload, and view before/after information.
- Export search results to a JSON file.

Logs are indexed by default, which allows them to be searched using the Console.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

Administrators: For specific examples of policy, see Required Permissions for Searching Logs on page 2635.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to know more about writing policies for Logging, see Details for Logging on page 2294.

Required Permissions for Searching Logs

To search indexed logs, a user must have the read permission on the log content and read access to the log group.

allow group GroupA to read log-groups in tenancy
allow group GroupA to read log-content in tenancy

To search indexed logs, you must have access to the log group that contains the indexed logs. For more information, see Required Permissions for Working with Logs and Log Groups on page 2577.

To view and search Audit Logs on page 2617, you must also have the corresponding Audit-related permissions. See Details for the Audit Service on page 2177 for more information. For example:

- search "compartment" requires AUDIT_EVENT_READ, and if there are any log objects, it would also require LOG_CONTENT_READ
- search "compartment/_Audit" requires just AUDITEVENT_READ.
- search "compartmentOcid/logGroupNameOrOcid/logNameOrOcid" requires LOG_CONTENT_READ only.
- search "compartmentOcid1/_Audit" "compartmentOcid2/logGroupNameOrOcid/logNameOrOcid" requires LOG_CONTENT_READ on compartmentOcid2 and AUDIT_EVENT_READ on compartmentOcid1.

Using the Console

You can perform log searches by using either the Basic mode filter controls in the interface, or the Advanced mode custom query language interface. See Basic Search Queries on page 2635 and Advanced Search Queries on page 2636 for more information.

Basic Search Queries

To search and filter logs:

1. Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Search.
2. In Select Logs to Search, the root compartment is already selected by default for filtering. Click this field to open the Select Logs to Search panel, where you can filter by compartments you have permission to work in, in addition to filtering by Log Groups and Logs. You can filter by multiple compartments and log groups. For any filters you create in this panel that you want to remove, click the filter X icon in the Select Logs to Search field.
3. In Filter By Field or Text Search, you can start typing to automatically display filter settings, along with operators. For example, entering d displays filters starting with that letter. Use the up or down
Logging

arrow keys to select from the list, or continue typing to enter what you want to filter on. For example, `data.compartmentName='<tenancy_name>'`.

4. In Logs, select one or more logs.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To limit the logs available to choose from, select one or more log groups from Log Groups.</td>
</tr>
</tbody>
</table>

5. Click Continue to apply the filter. The log data in the Explore and Visualize tab is reloaded according to the new filter settings.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Since the Search page automatically refreshes after applying filters and selecting logs, you do not need to click the Click Enter to search button as you select different filters. You will, however, need to click Click Enter to search again after some time has passed and new logs have appeared. When performing Advanced Mode queries however, you do need to always click this button to submit a query.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter settings are maintained when switching to Advanced Mode.</td>
</tr>
</tbody>
</table>

To remove a filter(s) from the Search page, under Filters, click the X icon next to the filter.

To search with Quick Start Queries

You can quickly search according to several predetermined queries. From Quick Start Queries, select a query from the list. The Search page displays the results for the chosen query.

To limit results to a specific time range

In Filter By Time, select a time range from the list, or select Custom to specify a date range in the calendar Start Date and End Date. You can also specify a time value in the box next to the calendar. Use an end time to refine the time window.

Didn't get the result you expected?

Try specifying a time range:

- Under Filter By Time, select a predetermined time range or specify a custom date range. Use an end time to refine the time window, then click Click Enter to search.

Advanced Search Queries

When performing a search on the Logging Search page, you can click Show Advanced Mode to enter your own custom log search queries. In addition, Advanced Mode searching provides more comprehensive search options that are not available in Basic Mode.

Be default, the following is displayed in the Query field after clicking Show Advanced Mode:

```
search "ocid1.tenancy.oc1..<unique_id>" | sort by datetime desc
```

For example, you can modify this default search by entering:

```
search "ocid1.tenancy.oc1..<unique_id>" | sort by datetime desc | summarize count() as cnt by rounddown(datetime, '15m') as interval
```

This returns `{"interval": 1600364700000,"cnt": 31}` and `{"interval": 1600365600000,"cnt": 220}` under Log Data in the Explore tab.

When entering search queries, auto-complete hints are providing as you type (which you can select from a pop-up menu as you type), and syntax validation is performed in real time in the background as you type a query.
When you switch from **Advanced Mode** to **Basic Mode**, the query is lost and is not available in **Basic Mode**. A warning is displayed for this scenario to confirm your preference.

The **Advanced Mode** search uses a specific syntax, using the Logging query language, which is described in **Logging Query Language Specification** on page 2639.

**To search with Quick Start Queries**

You can quickly search according to several predetermined queries. From **Quick Start Queries**, select a query from the list. The **Search** page displays the results for the chosen query.

**Saved Searches**

You can save the search parameters that you use for any searches performed in both **Basic Mode** and **Advanced Mode**.

To save a search:

1. Open the navigation menu. Under **Solutions and Platform**, go to **Logging**, and then click **Saved Searches**.
2. Under **List Scope, Compartment**, choose a compartment you have permission to work in. The **Saved Searches** page is displayed.
3. You can start the save operation using one of these two methods:
   - From the **Saved Searches** page, click **New Search**, which opens the Logging **Search** page, where you can begin a search.
   - From the **Search** page directly, whether in **Basic Mode** and **Advanced Mode**.
4. Click **Save Search**. The **New Saved Search** panel is displayed.
5. In **Search Name**, enter a name to associate with your saved search. Avoid entering confidential information.
6. In **Compartment**, select a compartment you have permissions to work in.
7. In **Description**, enter a description for the saved search.
8. Click **Save Search** to save your search.

   **Note:**
   
   The **Search Query** field cannot be edited and is view-only. It only displays the contents of your search parameters.

The search is saved and a message appears with the linked name of your saved search. Clicking the linked saved search name opens the details page for the saved search, where you can view more information about it. This page displays the following on the **Saved Search Information** tab:

- OCID
- Region
- Compartment
- Description
- **Created** date and time in UTC format.
- **Last Modified** date and time in UTC format.
- **Search Query** view-only description of the search parameters in the saved search.
- The **Tags** tab shows associated tags for this log.
- Under **Latest Results**, log data is displayed under **Saved Search Data**, in a similar manner as the **Log Data** on the **Search** page. You can apply some simple filters, such as sorting by newest or oldest from the **Sort** field, or filtering by time from the corresponding **Filter by Time** field.

11. **Click Explore with Log Search**, which allows you to view this saved search on the **Search** page directly. After clicking this link, the **Search** page opens with the saved search loaded, whether it is a basic or advanced mode.
search. At this point, you can perform more analysis and investigation related to this search directly on the **Search** page. For more information, see **Searching Logs** on page 2634.

While on the **Search** page, you can also switch between any of the saved searches by selecting them from the **Saved Searches** list.

### Note:

When editing a saved search from the **Saved Searches** page, you can only change the **Search Name**, **Compartment**, and **Description** fields in the **Edit Saved Search** panel. If you need to change the search parameters, create a new saved search.

---

**Viewing and Working with Search Results**

After you get an initial set of results, you can view more details, whether in terms of the log fields, JSON, or before and after states, and visually as a chart. On the **Explore** tab under **Log Data**, a **Number of Log Events Per Minute** bar graph displays the number of log events, according to your filter settings.

### Note:

You will need to click **Click Enter to search** after time has passed, to see the latest logs.

### Note:

For any actions taken on the **Explore** and **Visualize** tabs, you can define how often to refresh the data on the **Search** page, by selecting a value from the **Autorefresh Interval** list (choose from **OFF**, **5 Minutes**, or **15 Minutes**). The default is **OFF**.

---

**To examine a single log entry**

- In the **Explore** tab under **Log Data**, click the down arrow (▼) to expand the log entry in **JSON** view.

  The **JSON** view is displayed. In JSON view you can view the log data fields and values, collapse and expand nodes, or click the copy icon to copy the log entry to the clipboard.

**To switch between JSON and Before & After view**

- In the **Explore** tab under **Log Data**, click the down arrow (▼) to expand the log entry and click **JSON**.

  The JSON view is displayed. Click the **Before & After** tab to switch to its view.

**To examine Before & After view**

- In the **Explore** tab under **Log Data**, click the down arrow (▼) to expand the log entry and click **Before & After**.

  The **Before & After** view is displayed. In contrast to the entry labeled as **Current**, this view displays the exact preceding and successive logging lines in the log object.

**Right-click to view more log options**
In the **Explore** tab, each entry has three interactive header columns, which correspond to: the log timestamp, the plugin where the log occurred, and the log message.

Right-click one of the log entry columns to open a context-sensitive menu for that entry and the column header. These options are available whether the log entry is collapsed or expanded. The following right-click options are available:

- **Copy value**

**Note:**
This is the only option available for the third column’s right-click menu.

- **Filter matching**
- **Filter not matching**
- **Remove from summary view**

**To export log data**

At the top-left portion of **Log Data**, click **Export Log Data (JSON)**. This feature allows you to export the log data to a JSON file that you can save to your system.

**To visualize log data as a chart**

You can view log data graphically as a chart, along with accompanying tabular data.

Select from the following chart settings:

- **Visualization Type**: Select Bar. The Bar charts are organized in terms of time (UTC) on the X-axis, with time on the Y-axis. You can hover the mouse over bars when stacked bars appear, which displays the number of log records in a tool tip.
- **Interval**: Select from 1 minute (the default), 5 minutes, 15 minutes, 30 minutes, or 1 hour.
- **Group By**: Select a logging field to group the results by.

For any chart type being viewed, you can click to expand the `<number of> records found` list below the chart, which lists the total record sum, and the number of records at each time interval.

**Using the Command Line Interface (CLI)**

For more information on installing the CLI, see Quickstart on page 4195, and logging-search for command documentation.

**Submit a query to search logs**

Open a command prompt and run:

```
oci logging-search search-logs --search-query, --time-end, --time-start
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operation to search logs:

- **SearchLogs**

Use the following for saved searches:

- **LogSavedSearch**

**Logging Query Language Specification**

This topic describes the query syntax components that can be used with Advanced Search Queries on page 2636 and Saved Searches on page 2637.
Query Components

The logging query language processing is based on a data flow model. Each query can reference one or more logs, and produces a table dataset as a result. The query language provides several operators for searching, filtering, and aggregating structured and unstructured logs.

A logging query includes the following components:

- Log streams
- Fields
- Data types
- Stream expressions
- Pipe expressions
- Operators

Log Streams

To begin your search, you must first define the set of logs you want to search. You can choose to search specific log objects, log groups, or compartments. You can mix and match as many logs as you need. The search scope is defined using the following pattern:

```
search <log_stream> (,? <log_stream>)*
```

The query language fetches log entries from the scope you provide, and constructs a log stream that you can filter, aggregate, and visualize.

Log stream:

```
<log_stream> := "<compartment_ocid> ( /<log_group_ocid> ( /<log_object_ocid> )? )?"
```

Examples:

- `search "compartmentOcid/logGroupNameOrOcid/logNameOrOcid"`
- `search "compartmentOcid/logGroupNameOrOcid"
- `search "compartmentOcid"
- `search "compartmentOcid/logGroupNameOrOcid/logNameOrOcid", "compartmentOcid_2/logGroupNameOrOcid_2", "compartmentOcid_3"

Fields

All fields in log streams are case-sensitive. Although actual logs have indexed fields in lower case only, you can also create new fields in the query with mixed case:

```
search "." | select event as EventName
```

Fields are in JSON notation, therefore, special characters must be in quotes.

```
Fields: <field_name> := <identifier> (DOT <identifier>)*
```

For Identifier:

```
<identifier> := a-zA-Z_[a-zA-Z_0-9]* | ("" ("" | "") | "")
```
Logging

Examples:
- type
- data.message
- data.request.URL
- "type"
- "data"."message"
- "data.message" (not the same as "data"."message")
- data."$event"
- data."first name"
- data."an example of escaped ("\") double quotes"

Data Types

The following key data types are supported by the query language. These are (long and double) 8 bytes.
For details about the representation of the values of the corresponding types, see Literals on page 2647.

- Strings
- Numbers (integer, float-point)
- Arrays
- Booleans
- Timestamps
- Intervals

Stream Expressions

All expressions which produce a stream are stream expressions. Stream expressions can be formed using the following operators:

- Tabular operators
- Aggregate operators

Pipe Expressions

A pipe (|) applies an operator on the left side to a stream expression on the right side. The pipe expression is a stream expression.

The operator on the right side of a pipe must consume only one stream (for example, aggregate operations, filters).

The left side becomes the "current stream" for the right side expression, making all fields in the current stream available according to short names. For example:

```
search "application"
  | where level = 'ERROR'

>>
  {"timestamp": "2019-01-03T00:04:01", "level":"ERROR", "host":"host1", "message":"download failed...", "impact":2}
  {"timestamp": "2019-01-03T00:06:39", "level":"ERROR", "host":"host2", "message":"reached 90% file size limit...", "impact":4}
  {"timestamp": "2019-01-03T00:06:59", "level":"ERROR", "host":"host2", "message":"reached 95% file size limit...", "impact":5}
```

Operators

The following are supported when performing advanced queries:

- Tabular operators
Logging

- Scalar operators
- Aggregate operators

Tabular Operators

A tabular operator creates or modifies a log stream by filtering out or changing log entries. Also refer to BNF syntax notation. The following are tabular operators:

- **search**
- **where**
- **top**
- **sort**
- **dedup**
- **select**
- **extend**

**search**

Constructs a log stream from actual log objects. Also see Log Streams on page 2640 for details.

```
search "compartmentOCID/loggroup1/logname1" "compartmentOCID/loggroup2/logname2" "compartmentOCID/loggroup3/logname3"
```

**where**

Filters the current log stream using a Boolean expression.

```
search "application" | where level = 'ERROR'
```

where is optional:

```
search "application"  
  | where level = 'ERROR'
```

Some example comparisons with numbers and Boolean field comparisons are the following:

```
| data.statusCode = 200

| data.isPar
```

You can perform a full text search by specifying a filter on the entire content of the log. A search on logContent returns any log line where a value matches your string. This functionality supports wildcards. For example:

```
search "application"  
  | where logContent = 'ERROR' -- returns log lines with a value matching "ERROR"
```

```
search "application"  
  | where logContent = '*ERROR*' -- returns log lines with a value containing "ERROR"
```
**top**

Fetches only a specified number of rows from the current log stream, sorted based on some expression.

\[
\text{<top>} := \text{top } [0-9]+ \text{ by } \text{<expr>}
\]

Examples:

- `top 3 by datetime`
- `top 3 by *`
- `top 3 by (a + b)`

A number of rows must be a constant positive integer, and a sorting expression must be provided.

```
search "application" | top 3 by impact
```

```
>>
[{"timestamp": "2019-01-03T00:06:59", "level": "ERROR", "host": "host2", "message": "reached 95% file size limit...", "impact": 5},
{"timestamp": "2019-01-03T00:06:39", "level": "ERROR", "host": "host2", "message": "reached 90% file size limit...", "impact": 4},
{"timestamp": "2019-01-03T00:04:01", "level": "ERROR", "host": "host1", "message": "download failed...", "impact": 2}]
```

**sort**

Sorts the current log stream by the specified columns, in either ascending (default) or descending order. The operator uses the "DESC" and "ASC" keywords to specify the type of the order. The default sort order is asc.

\[
\text{<sort>} := \text{sort by } \text{<sort_expr>} (, \text{<sort_expr>})*
\]

\[
\text{<sort_expr>} := \text{<expr> (asc | desc) ?}
\]

Example:

```
search "application" | sort by impact desc
```

```
>>
[{"timestamp": "2019-01-03T00:06:59", "level": "ERROR", "host": "host2", "message": "reached 95% file size limit...", "impact": 5},
{"timestamp": "2019-01-03T00:06:39", "level": "ERROR", "host": "host2", "message": "reached 90% file size limit...", "impact": 4},
{"timestamp": "2019-01-03T00:04:01", "level": "ERROR", "host": "host1", "message": "download failed...", "impact": 2},
{"timestamp": "2019-01-03T00:05:33", "level": "WARNING", "host": "host2", "message": "reached 70% file size limit...", "impact": 1},
{"timestamp": "2019-01-03T00:04:05", "level": "INFO", "host": "host1", "message": "host list updated..."},
{"timestamp": "2019-01-03T00:06:59", "level": "INFO", "host": "host2", "message": "fs clean up started..."}
```

More than one column can be used to specify the order:

```
search "application" | sort by host, impact desc
```

```
>>
[{"timestamp": "2019-01-03T00:06:59", "level": "ERROR", "host": "host2", "message": "reached 95% file size limit...", "impact": 5},
{"timestamp": "2019-01-03T00:06:39", "level": "ERROR", "host": "host2", "message": "reached 90% file size limit...", "impact": 4},
{"timestamp": "2019-01-03T00:05:33", "level": "WARNING", "host": "host2", "message": "reached 70% file size limit...", "impact": 1}]
```
Logging

{"timestamp": "2019-01-03T00:06:59", "level":"INFO", "host":" host2",
"message":"fs clean up started..."}
{"timestamp": "2019-01-03T00:04:01", "level":"ERROR", "host":"host1",
"message":"download failed...", "impact":2}
{"timestamp": "2019-01-03T00:04:05", "level":"INFO", "host":" host1",
"message":"host list updated..."}
dedup
Processes the current log stream by filtering out all duplicates by specified columns. If more than one column is
specified, all columns have to be delimited by commas.
<dedup> := dedup <expr> (, <expr>)
Examples:
search "application"
| dedup host
>>
{"timestamp": "2019-01-03T00:04:01", "level":"ERROR", "host":"host1",
"message":"download failed...", "impact":2}
{"timestamp": "2019-01-03T00:05:33", "level":"WARNING", "host":"host2",
"message":"reached 70% file size limit... ", "impact":1}
search "application"
| dedup host, impact
{"timestamp": "2019-01-03T00:04:01", "level":"ERROR", "host":"host1",
"message":"download failed...", "impact":2}
{"timestamp": "2019-01-03T00:05:33", "level":"WARNING", "host":"host2",
"message":"reached 70% file size limit... ", "impact":1}
{"timestamp": "2019-01-03T00:06:39", "level":"ERROR", "host":"host2",
"message":"reached 90% file size limit... ", "impact":4}
{"timestamp": "2019-01-03T00:06:59", "level":"ERROR", "host":"host2",
"message":"reached 95% file size limit... ", "impact":5}
select
Applies a series of named scalar expressions to the current log stream. See summarize for an aggregation version of
select.
<select> := select <select_expr> (, <select_expr>)*
<select_expr> := ( * | <expr> (as <identifier>)? )
Example:
search "application"
| select level, host, impact+10 as impact, timestamp
>>
{"level":"ERROR", "host":"host1", "impact": 12, "timestamp":
"2019-01-03T00:04:01"}
{"level":"INFO", "host":" host1", "timestamp": "2019-01-03T00:04:05"}
{"level":"WARNING", "host":"host2", "impact": 11, "timestamp":
"2019-01-03T00:05:33"}
{"level":"ERROR", "host":"host2", "impact": 14, "timestamp":
"2019-01-03T00:06:39"}
{"level":"ERROR", "host":"host2", "impact": 15, "timestamp":
"2019-01-03T00:06:59"}
{"level":"INFO", "host":" host2", "timestamp": "2019-01-03T00:06:59"}
extend

Oracle Cloud Infrastructure User Guide

2644


Logging

Extends the current log stream with a computed column.

\[ \text{<extend>} \ := \ \text{extend} \ \text{<expr>} \ \text{as} \ \text{<identifier>})? \]

Example:

```
search "application"
    | extend concat(host, 'us.oracle.com') as fqn

{"timestamp": "2019-01-03T00:04:01", "level":"ERROR", "host":"host1",
  "message":"download failed...", "impact":2, "fqn": "host1.us.oracle.com"
{"timestamp": "2019-01-03T00:04:05", "level":"INFO", "host": "host1",
  "message":"host list updated...", "fqn": "host1.us.oracle.com"}
{"timestamp": "2019-01-03T00:05:33", "level":"WARNING", "host": "host2",
  "message":"reached 70% file size limit...", "impact":1, "fqn":
  "host2.us.oracle.com"}
{"timestamp": "2019-01-03T00:06:39", "level":"ERROR", "host": "host2",
  "message":"reached 90% file size limit...", "impact":4, "fqn":
  "host2.us.oracle.com"}
{"timestamp": "2019-01-03T00:06:59", "level":"ERROR", "host": "host2",
  "message":"reached 95% file size limit...", "impact":5, "fqn":
  "host2.us.oracle.com"}
{"timestamp": "2019-01-03T00:06:59", "level":"INFO", "host": "host2",
  "message":"fs clean up started...", "fqn": "host2.us.oracle.com"}
```

Scalar Operators

Scalar operators are applicable to individual values.

Arithmetic operations are the following:

- +
- -
- *
- /

Boolean operators are the following:

- and
- or

Unary operator:

- \(- (<\text{expr}>))\)

Comparison operators are the following (numeric expressions only):

- \(<\text{expr}> < <\text{expr}>\)
- \(<\text{expr}> > <\text{expr}>\)
- \(<\text{expr}> <= <\text{expr}>\)
- \(<\text{expr}> >= <\text{expr}>\)
- \(<\text{expr}> = <\text{expr}>\)
- \(<\text{expr}> != <\text{expr}>\)

String comparison:

- \(<\text{expr}> = <\text{expr}>\)

Functions:

- \(\text{not} \ (<\text{expr}>))\)
• `contains_ci/contains_cs (<expr>, <expr>, (true | false))`

  The last parameter is case-sensitive.

• `rounddown (<expr>, '[0-9]+(d | h | m | s)')`

  The last parameter is the time interval in days, hours, minutes, or seconds.

• `concat (<axpr>, <expr>)`

• `upper (<expr>)`

• `lower (<expr>)`

• `substr (<expr>, [0-9]+, ([0-9]+)?)`

  The second argument is the start index, while the third argument is optional, namely, how many characters to take.

• `isnull (<expr>)`

• `isnotnull (<expr>)`

### Aggregate Operators

#### count

Calculates a number of rows in the current log stream:

```
search "application"
  | count
>>
{"count": 6}
```

#### summarize

Groups the current log stream by the specified columns and time interval, and aggregates using named expressions. If grouping columns are not specified, `summarize` aggregates over the whole stream.

```
search "application"
  | summarize count(impact) as impact by level interval 1m
>>
{"timestamp": "2019-01-03T00:04:00", "level":"ERROR", "impact": 2}
{"timestamp": "2019-01-03T00:04:00", "level":"INFO", "impact": 0}
{"timestamp": "2019-01-03T00:05:00", "level":"WARNING", "impact":1}
{"timestamp": "2019-01-03T00:06:00", "level":"ERROR", "impact":5}
{"timestamp": "2019-01-03T00:06:00", "level":"INFO", "impact": 0}
```

**interval** is optional:

```
search "application"
  | summarize max(impact)
>>
{"impact": 5}
```

### Special Columns

#### logContent

`logContent` is a special column which represents the text of the whole original message. For example:

```
search "application"
  | where logContent = '*ERROR*' -- returns log lines with a value containing "ERROR"
```
**Comments**
Both single line and multi-line comments are supported, for example:

```plaintext
search "application"
  | count -- this is a single line comment

/** this is a
  multi-line
  comment */
```

**Identifiers**
Identifiers are the names of all available entities in the query. An identifier can reference a field in the current log stream, or a parameter defined in the beginning of the query. Identifiers have the following format:

```
name: \$?[a-zA-Z_]\[a-zA-Z_0-9]*
```

For example: `level`, `app_severity`, `$level`.

The quoted form allows special symbols in the names (except double quotes):

```
name: "\^[^"]*"
```

For example: "opc-request-id", "-level".

All parameter references start with a dollar sign ($), for example: `$level`.

**Literals**

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>'hello', 'world!'</td>
</tr>
<tr>
<td>wildcard pattern</td>
<td>&quot;acc-*&quot;</td>
</tr>
<tr>
<td>integer</td>
<td>-1, 0, +200</td>
</tr>
<tr>
<td>float</td>
<td>1.2, 0.0001, 1.2e10</td>
</tr>
<tr>
<td>array</td>
<td>[1,2,3,4], []</td>
</tr>
<tr>
<td>interval</td>
<td>3h, 2m</td>
</tr>
<tr>
<td>nullable</td>
<td>null</td>
</tr>
</tbody>
</table>

**Functions**
Scalar functions are the following:

- `isnull(expr1)`
- `concat(expr1, ...)`

Aggregate functions are the following:

- `sum(expr1)`
- `min(expr1)`
- `max(expr1)`
- `count()`: Counts a number of rows.
- `count(expr)`: Counts a number of non-null expr values.
System parameters

All parameters with the prefix "query." are reserved. The following parameters are supported:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>query.from</td>
<td>String with date time in ISO 8601 format.</td>
<td>'2007-04-05T14:30'</td>
<td>Specifies starting time of the query window.</td>
</tr>
<tr>
<td>query.to</td>
<td>String with date time in ISO 8601.</td>
<td>'2007-04-05T14:30+05:00'</td>
<td>Specifies end time of the query window.</td>
</tr>
</tbody>
</table>
Chapter 24

Marketplace

This chapter explains how to work with listings in the Oracle Cloud Infrastructure Marketplace.

Overview of Marketplace

Oracle Cloud Infrastructure Marketplace is an online store that offers solutions specifically for customers of Oracle Cloud Infrastructure. In the Oracle Cloud Infrastructure Marketplace catalog, you can find listings for two types of solutions from Oracle and trusted partners: images and stacks. These listing types include different categories of applications. Also, some listings are free and others require payment.

Images are templates of virtual hard drives that determine the operating system and software to run on an instance. You can deploy image listings on an Oracle Cloud Infrastructure Compute instance. Marketplace also offers stack listings. Stacks represent definitions of groups of Oracle Cloud Infrastructure resources that you can act on as a group. Each stack has a configuration consisting of one or more declarative configuration files. With an image or a stack, you have a customized, more streamlined way of getting started with a publisher's software.

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

While the resources created from Marketplace images and stacks have an OCID to identify them, the listings themselves have a listing ID and a package version ID for every package version in the listing. Listing IDs are numeric values. Package version IDs are string values. These identifiers are unique to Marketplace and unrelated to OCIDs.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create
new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For the actual policy statements required to perform tasks related to Marketplace, see the topic specific to the task.

**Working with Listings**

This topic describes how to work with listings in the Oracle Cloud Infrastructure Marketplace catalog. You can do the following:

- Search for listings to find what you want to deploy
- Filter listings to refine application results
- View a listing to learn about the product that it offers
- Launch an instance from an image listing
- Launch stack resources from a stack listing
- Download Terraform configuration files from stack listings to update deployed applications

By default, Marketplace displays all listings in its catalog. However, an individual's ability to see or launch particular listings varies by tenancy, according to what permissions the individual has, and the pricing model for the listing.

Listings are either image listings or stack listings. Image listings have a **Launch Instance** button. Stack listings have a **Launch Stack** button.

For information about pricing and how it affects whether you can see a listing, see Pricing for Listings on page 2653.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For administrators, the policies you need to create to provide users with access to Marketplace depend on whether the tenancy is in a commercial region, the United Kingdom Government Cloud region, or the United States Government Cloud realm.

**Note:**

In commercial regions and the United Kingdom Government Cloud region, administrators do not need to write policies to grant users the ability to list or read listings. In these regions, you can see individual listings and lists of listings by default. Furthermore, to reduce the scope of access to a particular compartment, specify the specific compartment instead of the tenancy in the policy statement.

**For a Tenancy in a Commercial Region or the United Kingdom Government Cloud**

- The following policy gives the specified example group, MarketplaceUsers, the ability to list accepted terms of use agreements. However, it does not include the ability to accept a terms of use agreement. The terms of use agreement for a given listing must be viewed and accepted prior to launch. For a policy that includes the ability
to use listings, see the policy statements later in this section that grant access to the type of listing you want to launch, whether an image listing or a stack listing.

- The following policy gives the specified example group, MarketplaceUsers, the ability to not only list and read, but also use Marketplace listings. It does not include the ability to create instances using images from listings. (For that, see the next set of policy statements.)

- The policies described in Policies for Managing Resources Used with Resource Manager on page 2476 grant access to stacks and jobs in the tenancy. Use the appropriate policy statements to give a group the ability to list, read, and use Marketplace stack listings. (Users do not need permission to run destroy jobs to launch a stack from a Marketplace listing, but they do need permissions to run plan jobs and apply jobs.)

If you need to write more restrictive policies, see the policy references on which these policies were based, Details for the Core Services on page 2181 and Details for Resource Manager on page 2336, as needed.

**For a Tenancy in the US Government Cloud Realm**

- The following policy gives the specified example group, MarketplaceUsers, the ability to view all listings in the specified example compartment:

- The following policy gives the specified example group, MarketplaceUsers, the ability to work with all listings in the specified example compartment in any way possible. The statements include the ability to accept terms of use agreements, view listings, and create images and stacks from listings:
Marketplace

Allow group MarketplaceUsers to manage virtual-network-family in compartment ABC
Allow group MarketplaceUsers to manage orm-stack in compartment ABC
Allow group MarketplaceUsers to manage orm-job in compartment ABC

• The following policy gives the specified example group, MarketplaceUsers, the ability to work with specific listings in the specified example compartment in any way possible. The statements include the ability to list and subscribe to images and the ability to create images and stacks from listings:

Allow group MarketplaceUsers to manage app-catalog-listings in compartment ABC
Allow group MarketplaceUsers to use marketplace-listings in compartment ABC where any {listing.id='123456', listing.id='987654'}
Allow group MarketplaceUsers to manage instance-family in compartment ABC
Allow group MarketplaceUsers to use volume-family in compartment ABC
Allow group MarketplaceUsers to manage virtual-network-family in compartment ABC
Allow group MarketplaceUsers to manage orm-stack in compartment ABC
Allow group MarketplaceUsers to manage orm-job in compartment ABC

• The following policy gives the specified example group, AgreementAcceptors, the ability to accept the terms of use agreement for any listing in the specified example compartment. The statements make it possible for anyone with the appropriate permissions to launch an image or stack from a listing without having the permission to accept the terms of use agreement themselves:

Allow group AgreementAcceptors to read marketplace-listings in compartment ABC
Allow group AgreementAcceptors to manage app-catalog-listings in compartment ABC

If you need to write more restrictive policies, see the policy reference on which policies for tenancies in the US Government Cloud realm were based, Details for the Marketplace Service on page 2319.

Pricing for Listings

Marketplace listings belong to one of several pricing models available to and set by the publisher when the publisher creates the listing. Pricing models include:

• **Free**: usage incurs no charge
• **BYOL**: usage relies on software licenses that you already own
• **Paid**: usage incurs charges based on hourly rates, either according to OCPU hours consumed or according to the number of instances (irrespective of OCPU hours consumed by each)

The listing price does not include any additional fees that you might incur for the use of infrastructure resources.

For a cloud account to access paid listings, it must have a United States mailing address and the form of payment provided when the account was created must support payment in United States dollars. United States-based customers can deploy most paid listings in any commercial region data center, but some paid listings can only be deployed in United States commercial regions. These listings have a region restriction label that marks them as **US-only**.

Customers in US Government Cloud realms can see all paid listings from Oracle and third-party publishers. Users in United Kingdom government tenancies do not have access to any paid listings.

Using the Console

To find a listing

1. Open the navigation menu. Under the **Solutions and Platform** group, go to **Marketplace**.
2. Under **Scope**, in the **Compartment** list, click the name of the compartment where you want to look for listings.
3. Click the **Search for listings by entering a name, ID, category, or publisher name** text box.
4. Provide a search string, and then press ENTER. (If you provide a listing ID, it must contain the full, exact listing ID to match. Marketplace supports partial matching for other listing search types.)
Marketplace displays all current listings that contain the search string in either the name, listing ID, application category, or publisher name. To refine the results, you can filter them.

To filter listings

1. Open the navigation menu. Under the Solutions and Platform group, go to Marketplace.
2. Under Scope, in the Compartment list, click the name of the compartment where you want to look for listings.
3. Under Filters, do one or more of the following:
   - To display listings of a certain deployment type, click Type, and then click either Image or Stack.
   - To display listings from a specific publisher, click Publisher, and then click a publisher name.
   - To display listings from a particular product category, click Category, and then click a category name.
   - To display listings according to price, click Price, and then click a pricing model.

You can combine multiple filters to further narrow down listings. You can also clear filters to expand the list of listings that you see.

To view a listing's details

1. Open the navigation menu. Under the Solutions and Platform group, go to Marketplace.
2. Under Scope, in the Compartment list, click the name of the compartment where you want to view a listing.
3. Click the listing that you're interested in.
4. Marketplace displays the listing overview by default. To view other details, do the following:
   - To view information about the publisher, click Provider.
   - To view other listings from the same publisher, click More Apps.
   - To view instructions for using the instance that you create from the listing, click Usage Information.

To launch an instance based on an image

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you create an instance, several other resources are involved (for example, an image, a cloud network, or a subnet). Those other resources can be in the same compartment with the instance or in other compartments. You must have the required level of access to each of the compartments involved in order to launch the instance. This is also true when you attach a volume to an instance; they don't have to be in the same compartment, but if they’re not, you need the required level of access to each of the compartments.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under the Solutions and Platform group, go to Marketplace.
2. Under Scope, in the Compartment list, click the name of the compartment where you want to find the listing to launch.
3. Click the listing that you're interested in.
4. Review the Usage Instructions tab to ensure you understand what you will need to deploy and to access the instance after you launch it. Both Linux and Windows instances require a cloud network to launch the instance into. For more information, see Networking Overview on page 2748. Depending on the type of instance, to access it, you might need an SSH key pair or a security list that enables Remote Desktop Protocol. For more information, see Managing Key Pairs on Linux Instances on page 693 and Creating a Windows Instance on page 702.
5. Under Version, click the package version of the image that you want to install. By default, the menu displays the latest version.
6. Under Compartment, click the name of the compartment where you want to launch the instance. (If you don't have permissions to launch the instance in the selected compartment, it will be launched in the root compartment instead.)
7. Select the check box to accept the terms of use, and then click Launch Instance.
8. To finish launching the instance, follow the instructions in Creating an Instance.

The information you need to connect to an instance after you create it might be in the Usage Information or the Related Documents sections of the listing.
To launch a stack

Tip:

When you create a stack, potentially many other resources are involved (for example, an instance, a cloud network, or a subnet), aside from the stacks and jobs resources. You must have the required access to all involved resources to create a stack. Those other resources can be in the same compartment with the instance or in other compartments. You must have the required level of access to each of the compartments involved in order to launch the instance. This is also true when you attach a volume to an instance; they don't have to be in the same compartment, but if they're not, you need the required level of access to each of the compartments.

1. Open the navigation menu. Under the Solutions and Platform group, go to Marketplace.

2. Under Scope, in the Compartment list, click the name of the compartment where you want to find the listing to launch.

3. Click the listing that you're interested in.

4. Click the listing that you're interested in.

5. Review the Usage Instructions tab and ensure you understand what you will need to deploy and to access the instance after the stack finishes deployment.

6. Under Version, click the package version of the stack that you want to install. By default, the menu displays the latest version.

7. Under Compartment, click the name of the compartment where you want to launch the instance. (If you don't have permissions to launch the instance in the selected compartment, it will be launched in the root compartment instead.)

8. Select the check box to accept the terms of use, and then click Launch Stack.

9. On the Stack Information page, configure the following:

   • Name. Optionally, provide a name by which you can refer to the stack after it's deployed. Avoid entering confidential information.

   • Description. Optionally, provide a description of the stack. For example, you can specify the name of the application that will run on the instance after the stack is deployed.

   • Create in Compartment. This is the compartment where the stack will be created in the tenancy. (Stacks are attached to a specific region. However, where necessary, the resources on a given stack can be deployed across multiple regions.)

   • Tags. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

   When you are ready, click Next.

10. On the Configure Variables page, verify that the values for variables extracted from the Terraform configuration file are as you want them. Some variables might be required, but don't have a default value and must be configured before you can proceed. These vary from listing to listing, but often include the following: availability domain and compartment. Optionally, you can change default values, such as any display names automatically given to resources, to help differentiate them. For some stacks, you can customize additional variables by selecting the Additional Customization or WLS Instance Advanced Configuration check box. The variables in these sections otherwise use default values. When you are ready, click Next.

11. On the Review page, confirm that variables have been configured properly. (Marketplace does not display variables that have default values or variables that you didn't change.) Then, click Create.

Resource Manager runs the plan job and the apply job to create stack resources accordingly. The information you need to connect to the instance created as part of the stack can appear in the Application Information tab or in the Usage Information or Related Documents sections of the listing.

To download a Terraform configuration file

1. Open the navigation menu. Under the Solutions and Platform group, go to Marketplace.
2. Click the listing that you're interested in.
3. Under **Version**, click the package version of the stack that you want. By default, the menu displays the latest version.
4. Under **Compartment**, click the name of any compartment. (You must select a compartment in order to accept the terms of use in the next step.)
5. Select the check box to accept the terms of use, and then click **Download**.
6. Follow the prompts to save the configuration file locally.

For information about how to use the file to edit a stack or create a stack, see Managing Stacks and Jobs on page 3557.

### Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

#### To filter listings

Open a command prompt and run `oci marketplace listing list` to view listings that meet specified filter criteria:

```
oci marketplace listing list --package-type <package_type> --publisher-id <unique_publisher_ID> --category <product_category> --pricing <pricing_model>
```

For example, the following command lists only image listings:

```
oci marketplace listing list --package-type image
```

The following command lists only listings from the specified publisher:

```
oci marketplace listing list --publisher-id 29367738
```

The following command lists only listings from the specified product category:

```
oci marketplace listing list --category "database management"
```

The following command lists only listings that have the specified pricing model:

```
oci marketplace listing list --pricing byol
```

#### To view a listing's details

Open a command prompt and run `oci marketplace listing get` to view detailed information about a listing:

```
oci marketplace listing get --listing-id <listing_ID>
```

For example:

```
oci marketplace listing get --listing-id 29367738
```

#### To launch an instance

Open a command prompt and run `oci compute instance launch` to launch an instance:

```
oci compute instance launch --availability-domain <availability_domain> --compartment-id <compartment_OCID> --shape <instance_shape> --subnet-id <subnet_OCID> --image-id <image_OCID>
```
For example:

```
oci compute instance launch --availability-domain Uocm:PHX-AD-1 --compartment-id ocid1.compartment.oc1..example1example25qr1po4agcmothkbqgmuz2zzum45ibplooqtawbk3zz --shape VM.Standard1.2 --subnet-id ocid1.subnet.oc1.phx.exampleahetdvobxd5cvbgfcmjw2ddryahoqrp4ot2fauxvbdeteirpa2gpt2a --image-id ocid1.image.oc1.phx.exampleae44ah3b5xyet6t1vli23cvbtetyugfckfwgg6fywrk3fauuxscyq
```

**Using the API**

For information about using the API and signing requests, see REST APIs and Security Credentials. For information about SDKs, see Software Development Kits and Command Line Interface.

Use the following operations to work with listings:

- GetListing
- GetPackage
- ListCategories
- ListListings
- ListPackages
- ListPublishers

**Publishing Listings**

Applications listed in Oracle Cloud Infrastructure Marketplace are provided by publishers. Publishers belong to the Oracle PartnerNetwork. Oracle reviews and approves the applications submitted by publishers. If you would like to become a publisher, see How do I become a marketplace publisher? in the Oracle Cloud Marketplace Partner Portal documentation.

**Viewing Accepted Terms of Use Agreements**

Before you can launch an image or a stack from a Marketplace listing, you must first read and accept all software terms of use agreements associated with the package version that you choose. This topic describes how to see what terms of use agreements you have accepted through Oracle Cloud Infrastructure Marketplace. Your organization might need or want to review the specific terms of use associated with a particular package version after you deploy one or more Marketplace listings.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For administrators, the following policies provide access to Marketplace.

- The following policy gives the specified group the ability to list accepted terms of use agreements. The terms of use agreement for a given listing must be viewed and accepted prior to launch. The policy does not include the ability to list, read, or use listings themselves. For that, see the policy statements that grant access to the type of listing you want to launch, whether an image listing or a stack listing.

```
Allow group <IAM_group_name> to inspect compartments in tenancy
```

- The following policy gives the specified group the ability to list, read, and use Marketplace image listings. It does not include the ability to create instances using images from listings. (For that, see the next policy.) Furthermore,
to reduce the scope of access to just creating subscriptions in a particular compartment, specify that compartment instead of the tenancy.

Allow group <IAM_group_name> to manage app-catalog-listing in tenancy

- The following policy gives the specified group general access to managing instances and images, along with the required level of access to attach existing block volumes to the instances. Use this policy in conjunction with the preceding policy for users who need to launch instances from image listings. For users who need to launch stacks from stack listings, use this policy in conjunction with the next set of policies.

Allow group <IAM_group_name> to manage instance-family in compartment ABC
Allow group <IAM_group_name> to read app-catalog-listing in tenancy
Allow group <IAM_group_name> to use volume-family in compartment ABC
Allow group <IAM_group_name> to use virtual-network-family in compartment XYZ

- The policies described in Policies for Managing Resources Used with Resource Manager on page 2476 grant access to stacks and jobs in the tenancy. Use the appropriate policy statements to give a group the ability to list, read, and use Marketplace stack listings. (Users do not need permission to run destroy jobs to launch a stack from a Marketplace listing, but they do need permissions to run plan jobs and apply jobs.)

If you need to write more restrictive policies, see the policy references on which these policies were based, Details for the Core Services on page 2181 and Details for Resource Manager on page 2336, as needed.

Using the Console
To view the accepted terms of use agreements for a given compartment

1. Open the navigation menu. Under the Solutions and Platform group, go to Marketplace.
2. Click Accepted Agreements.
3. Under Scope, click Compartment, and then click the name of the compartment where you accepted a terms of use agreement that you now want to view.
4. In the list, next to the listing that you're interested in, click the Actions menu ( ). (Marketplace independently lists package versions with their distinct terms of use agreements. Also, Marketplace tracks what agreements you accept regardless of whether you actually complete the software deployment. Therefore, the list might show the names of listings that you didn't actually finish deploying in your tenancy.)
5. To review any of the terms of use agreements you accepted for the specified listing and package version, click its name.

Using the Command Line Interface (CLI)
For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

To view the accepted terms of use agreements for a given compartment

Open a command prompt and run oci marketplace accepted-agreement list to view a list of terms of use agreements that you previously accepted:

oci marketplace accepted-agreement list --compartment-id <compartment_id>

For example:
Using the API

For information about using the API and signing requests, see REST APIs and Security Credentials. For information about SDKs, see Software Development Kits and Command Line Interface.

Use the following operations to work with a listing's terms of use agreements:

- CreateAcceptedAgreement
- DeleteAcceptedAgreement
- GetAcceptedAgreement
- GetAgreement
- ListAcceptedAgreements
- ListAgreements
- UpdateAcceptedAgreement
Chapter 25

Monitoring

This chapter explains how to actively and passively monitor performance and usage metrics for your resources.

Monitoring Overview

The Oracle Cloud Infrastructure Monitoring service enables you to actively and passively monitor your cloud resources using the Metrics and Alarms features.

How Monitoring Works

The Monitoring service uses metrics to monitor resources and alarms to notify you when these metrics meet alarm-specified triggers.

Metrics are emitted to the Monitoring service as raw data points, or timestamp-value pairs, along with dimensions and metadata. Metrics come from a variety of sources:

- Resource metrics automatically posted by Oracle Cloud Infrastructure resources. For example, the Compute service posts metrics for monitoring-enabled Compute instances through the oci_computeagent namespace. One such metric is CpuUtilization. See Supported Services on page 2669 and Viewing Default Metric Charts on page 2671.
- Custom metrics published using the Monitoring API.
- Data sent to new or existing metrics using Service Connector Hub.

Metric data posted to the Monitoring service is only presented to you or consumed by the Oracle Cloud Infrastructure features that you enable to use metric data.
When you query a metric, the Monitoring service returns aggregated data according to the specified parameters. You can specify a range (such as the last 24 hours), statistic, and interval. The Console displays one monitoring chart per metric for selected resources. The aggregated data in each chart reflects your selected statistic and interval. API requests can optionally filter by dimension and specify a resolution. API responses include the metric name along with its source compartment and metric namespace. You can feed the aggregated data into a visualization or graphing library.

Metric and alarm data is accessible via the Console, CLI, and API. For retention periods, see Storage Limits on page 2671.

The Alarms feature of the Monitoring service publishes alarm messages to configured destinations managed by the Notifications service. Each destination is a topic with a set of subscribers. For more information about the Notifications service, see Notifications Overview on page 3350.

## Message types

The message type indicates the reason that the message was sent.

- **OK_TO_FIRING**: The alarm changed from OK status to FIRING status.
- **FIRING_TO_OK**: The alarm changed from FIRING status to OK status.
- **REPEAT**: The alarm is maintaining a FIRING status and repeat notifications are configured.
- **RESET**: The alarm is not detecting the metric firing; the metric is no longer being emitted. The resource that was emitting the metric might have been moved or terminated.

### Important:
When a RESET status change occurs, determine the health of the resource.

## Message format and examples

Alarm message format:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dedupekey</td>
<td>string</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>Unique identifier for all the alarm messages of the alarm. Use for de-duplication.</td>
</tr>
<tr>
<td>title</td>
<td>string</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>The alarm's configured display name.</td>
</tr>
<tr>
<td>body</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>The alarm's configured message body.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>The reason for sending the notification message. Valid values: See Message types on page 2661.</td>
</tr>
<tr>
<td>severity</td>
<td>string</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>The highest severity level of the listed alarms. Valid values: CRITICAL, ERROR, WARNING, and INFO</td>
</tr>
<tr>
<td>timestampEpochMillis</td>
<td>long</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td>The time when the alarm was triggered, in milliseconds since epoch time.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>timestamp</td>
<td>string</td>
</tr>
<tr>
<td>Required</td>
<td>The time when the alarm was triggered, in ISO-8601 format. Same information as in timestampEpochMillis.</td>
</tr>
<tr>
<td>alarmMetadata</td>
<td>array of objects</td>
</tr>
<tr>
<td>Required</td>
<td>List of alarms related to this notification message.</td>
</tr>
<tr>
<td>version</td>
<td>int</td>
</tr>
<tr>
<td>Required</td>
<td>The version of the alarm message format.</td>
</tr>
</tbody>
</table>

**alarmMetadata format:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>string</td>
</tr>
<tr>
<td>Required</td>
<td>The alarm OCID.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
</tr>
<tr>
<td>Required</td>
<td>The alarm state. Valid values: OK, FIRING</td>
</tr>
<tr>
<td>severity</td>
<td>string</td>
</tr>
<tr>
<td>Required</td>
<td>The alarm severity level. Valid values: CRITICAL, ERROR, WARNING, INFO</td>
</tr>
<tr>
<td>query</td>
<td>string</td>
</tr>
<tr>
<td>Required</td>
<td>The alarm's configured query.</td>
</tr>
<tr>
<td>totalMetricsFiring</td>
<td>int</td>
</tr>
<tr>
<td>Required</td>
<td>The number of metric streams represented in this notification message.</td>
</tr>
<tr>
<td>dimensions</td>
<td>array of objects</td>
</tr>
<tr>
<td></td>
<td>List of dimension key-value pairs that identify each metric stream. The list is limited to a hundred entries. Empty for an alarm with a status of OK.</td>
</tr>
</tbody>
</table>

Example messages, by subscription protocol, for an alarm titled "High CPU Utilization" that is continuing to be in the FIRING state. In this example, the message includes two metric streams: one for "myinstance1" and another for "myinstance2."

**Email and Slack**

```json
{"dedupeKey":"exampleuniqueID","title":"High CPU Utilization","body":"Follow runbook at http://example.com/runbooks","type":"REPEAT","severity":"CRITICAL","timestampEpochMillis":1542406320000,"alarmMetaData":[]}
```
SMS

119L3T: [CRITICAL] "High CPU Utilization" has transitioned to OK_TO_FIRING at 2021-02-10T05:52:00Z

https://cloud.oracle.com/monitoring/alarms/status

Metrics Feature Overview

The Metrics feature relays metric data about the health, capacity, and performance of your cloud resources. A metric is a measurement related to health, capacity, or performance of a given resource. Resources, services, and applications emit metrics to the Monitoring service. Common metrics reflect data related to:

- Availability and latency
- Application uptime and downtime
- Completed transactions
- Failed and successful operations
- Key performance indicators (KPIs), such as sales and engagement quantifiers

By querying Monitoring for this data, you can understand how well the systems and processes are working to achieve the service levels you commit to your customers. For example, you can monitor the CPU utilization and disk reads of your Compute instances. You can then use this data to determine when to launch more instances to handle increased load, troubleshoot issues with your instance, or better understand system behavior.

Example Metric: Failure Rate

For application health, one of the common KPIs is failure rate, for which a common definition is the number of failed transactions divided by total transactions. This KPI is usually delivered through application monitoring and management software.

As a developer, you can capture this KPI from your applications using custom metrics. Simply record observations every time an application transaction takes place and then post that data to the Monitoring service. In this case, set up metrics to capture failed transactions, successful transactions, and transaction latency (time spent per completed transaction).
The Alarms feature of the Monitoring service works with the Notifications service to notify you when metrics meet alarm-specified triggers. The previous illustration depicts the flow, starting with resources emitting metric data points to Monitoring. When triggered, an alarm sends an alarm message to the configured topic (in Notifications), which then sends the message on to all of the topic's subscriptions. (This illustration does not cover raw and aggregated metric data. For these details, see the "Monitoring Overview" illustration.)

When configured, repeat notifications remind you of a continued firing state at the configured repeat interval. You are also notified when an alarm transitions back to the OK state, or when an alarm is reset.

You can search for alarms using Search-supported attributes. For more information about Search, see Overview of Search on page 3626.

**Search-Supported Attributes for Alarms**

For attribute descriptions, see Alarm Reference.

- id
- displayName
- compartmentId
- metricCompartmentId
- namespace
- query
- severity
- destinations
- suppression
- isEnabled
- lifecycleState
- timeCreated
Monitoring Concepts

The following concepts are essential to working with Monitoring.

aggregated data

The result of applying a statistic and interval to a selection of raw data points for a given metric. For example, you can apply the statistic max and interval 1h (one hour) to the last 24 hours of raw data points for the metric CpuUtilization. Aggregated data is displayed in default metric charts in the Console. You can also build metric queries for specific sets of aggregated data. For instructions, see Viewing Default Metric Charts on page 2671 and Building Metric Queries on page 2700.

alarm

The alarm query to evaluate and the notification destination to use when the alarm is in the firing state, along with other alarm properties. For instructions on managing alarms, see Managing Alarms on page 2719.

alarm query

The Monitoring Query Language (MQL) expression to evaluate for the alarm. An alarm query must specify a metric, statistic, interval, and a trigger rule (threshold or absence). The Alarms feature of the Monitoring service interprets results for each returned time series as a Boolean value, where zero represents false and a non-zero value represents true. A true value means that the trigger rule condition has been met. For more information, see Building Metric Queries on page 2700 and the query attribute description in the Alarm API reference.

data point

A timestamp-value pair for the specified metric. Example: 2018-05-10T22:19:00Z, 10.4

A data point is either raw or aggregated. Raw data points are posted by the metric namespace to the Monitoring service using the PostMetricData operation. The frequency of the data points posted varies by metric namespace. For example, your custom namespace might send data points for a given metric at a 20-second frequency.

Aggregated data points are the result of applying a statistic and interval to raw data points. The interval of the aggregated data points is determined by the SummarizeMetricsData request. For example, a request specifying the statistic sum and interval 1h (one hour) returns a sum value for each hour of available raw data points for the given metric.

dimension

A qualifier provided in a metric definition. Example: Resource identifier (resourceId), provided in the definitions of oci_computeagent metrics. Use dimensions to filter or group metric data. Example dimension name-value pair for filtering by availability domain: availabilityDomain = "VeBZ:PHX-AD-1"

frequency

The time period between each posted raw data point for a given metric. (Raw data points are posted by the metric namespace to the Monitoring service.) While frequency varies by metric, default service metrics typically have a frequency of 60 seconds (that is, one data point posted per minute). See also resolution.

interval

The time window used to convert the given set of raw data points.

The timestamp of the aggregated data point corresponds to the end of the time window during which raw data points are assessed. For example, for a five-minute interval, the timestamp "2:05" corresponds to the five-minute time window from 2:00 to 2:05:00.
The following example query specifies a 5-minute interval. \texttt{CpuUtilization[5m].max()} For supported values, see Monitoring Query Language (MQL) Reference on page 2741.

\begin{itemize}
  \item \textbf{Note:}
  \begin{itemize}
    \item Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the \texttt{1h} or \texttt{1d} interval values are supported.
  \end{itemize}
\end{itemize}

To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

See also \textit{resolution}.

\textbf{message}

The content that the Alarms feature of the Monitoring service publishes to topics in the \textit{alarm}'s configured notification destinations. A message is sent when the \textit{alarm} transitions to another state, such as from "OK" to "FIRING." For more information about messages, see How Monitoring Works on page 2660.

\textbf{metadata}

A reference provided in a \textit{metric definition}. Example: unit (bytes), provided in the definition of the \texttt{oci_computeagent metricDiskBytesRead}. Use metadata to determine additional information about a given metric. For metric definitions, see \textit{Supported Services} on page 2669.

\textbf{metric}

A measurement related to health, capacity, or performance of a given resource. Example: The \texttt{oci_computeagent metricCpuUtilization}, which measures usage of a Compute instance. For metric definitions, see \textit{Supported Services} on page 2669.

\begin{itemize}
  \item \textbf{Note:}
  \begin{itemize}
    \item Metric resources do not have \textit{OCIDs}.
  \end{itemize}
\end{itemize}

\textbf{metric definition}

A set of references, qualifiers, and other information provided by a \textit{metric namespace} for a given \textit{metric}. For example, the \texttt{oci_computeagent metricDiskBytesRead} is defined by \textit{dimensions} (such as resource identifier) and \textit{metadata} (specifying bytes for unit) as well as identification of its \textit{metric namespace} (\texttt{oci_computeagent}). Each posted set of \textit{data points} carries this information. Use the \texttt{ListMetricData} API operation to get metric definitions. For metric definitions, see \textit{Supported Services} on page 2669.

\textbf{metric namespace}

Indicator of the \textit{resource}, service, or application that emits the \textit{metric}. Provided in the \textit{metric definition}. For example, the \texttt{CpuUtilization metric definition} emitted by the Oracle Cloud Agent software on Compute \textit{instances} lists the \textit{metric namespace} \texttt{oci_computeagent} as the source of the \texttt{CpuUtilization metric}. For metric definitions, see \textit{Supported Services} on page 2669.
**Monitoring**

**metric stream**
An individual set of *aggregated data for a metric*. A stream can be either specific to a single *resource* or aggregated across all resources in the compartment. Within a *metric chart* in the Console, each metric stream is represented as a line. By default, metric streams are resource-specific, so the chart displays a line for each resource. If you choose to *aggregate all metric streams*, then the chart displays one line for all resources.

**notification destination**
Protocol and other details for sending *messages* when the *alarm* transitions to another state, such as from "OK" to "FIRING." The details and setup may vary by destination service. For the Notifications service, each destination includes a topic and subscription protocol (such as PagerDuty). For more information about messages, topics, and subscriptions, see *Notifications Overview* on page 3350.

**Oracle Cloud Agent software**
Software that allows a Compute instance to post raw *data points* to the Monitoring service. Automatically installed with the latest versions of supported images. See *Enabling Monitoring for Compute Instances* on page 783.

**query**
The Monitoring Query Language (MQL) expression to evaluate for returning *aggregated data*. The query must specify a *metric*, *statistic*, and *interval*. For more information, see *Building Metric Queries* on page 2700.

**resolution**
The period between time windows, or the regularity at which time windows shift. For example, use a resolution of *1m* to retrieve aggregations every minute.
To specify a non-default resolution that differs from the interval, use the *SummarizeMetricsData* operation.

**Note:**
For metric queries, the *interval* you select drives the default *resolution* of the request, which determines the maximum time range of data returned.
For more information about the resolution parameter as used in metric queries, see *SummarizeMetricsData*.

**Maximum time range returned for a query**
The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.

The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>
To specify a non-default resolution that differs from the interval, use the `SummarizeMetricsData` operation.

**See examples of returned data**

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of 1m, and the end time defaults to the current time (2019-01-08T10:00:00.789Z). This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z).

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th (2019-01-06T10:00:00.789Z), the earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z). Therefore, only 5 days of metric data points can be returned in this example.

For alarm queries, the specified `interval` has no effect on the `resolution` of the request. The only valid value of the resolution for an alarm query request is 1m. For more information about the `resolution` parameter as used in alarm queries, see `Alarm`.

As shown in the following illustration, `resolution` controls the start time of each aggregation window relative to the previous window while `interval` controls the length of the windows. Both requests apply the statistic max to the data within each five-minute window (from the interval), resulting in a single aggregated `data point` representing the highest `CPUUtilization` counter for that window. Only the resolution value differs. This resolution changes the regularity at which the aggregation windows shift, or the start times of successive aggregation windows. Request A does not specify a resolution and thus uses the default value equal to the `interval` (5 minutes). This request's five-minute aggregation windows are thus taken from the sets of data points emitted from 0:n to 5:00, 5:n to 10:00, and so forth. Request B specifies a 1-minute resolution, so its five-minute aggregation windows are taken from the set of data points emitted every minute from 0:n to 5:00, 1:n to 6:00, and so forth.

A custom string provided with a custom metric that can be used as a filter or to aggregate results. The `resource group` must exist in the definition of the posted metric. Only one `resource group` can be applied per metric.
**statistic**

The aggregation function applied to the given set of raw data points. For supported statistics, see Monitoring Query Language (MQL) Reference on page 2741.

**suppression**

A configuration to avoid publishing messages during the specified time range. Useful for suspending alarm notifications during system maintenance. Each suppression applies to a single alarm. In the Console, you can apply one definition of a suppression to multiple alarms. The result is an individual suppression for each alarm. For instructions on suppressing alarms, see To suppress alarms on page 2738.

**trigger rule**

The condition that must be met for the alarm to be in the firing state. A trigger rule can be based on a threshold or absence of a metric.

**Availability**

The Monitoring service is available in all Oracle Cloud Infrastructure commercial regions. See About Regions and Availability Domains on page 180 for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

**Supported Services**

The following services have resources or components that can emit metrics to Monitoring:

- API Gateway - see API Gateway Metrics on page 478
- Big Data - see View Cluster Metrics
- Block Storage - see Block Volume Metrics on page 585
- Blockchain Platform - see Blockchain Platform Metrics
- Compute - see these topics:
  - Compute Instance Metrics on page 788
  - Instance Pool Metrics on page 793
  - Infrastructure Health Metrics on page 795
  - Compute Management Metrics on page 798
- Container Engine for Kubernetes - see Container Engine for Kubernetes Metrics on page 963
- Data Catalog - see Data Catalog Metrics
- Data Integration - see Data Integration Metrics
- Database - see Database Metrics on page 1578
- Digital Assistant - see Digital Assistant Metrics
- DNS - see DNS Metrics on page 1704
- Events - see Events Metrics on page 1917
- Email Delivery - see Email Delivery Metrics on page 1756
- File Storage - see File System Metrics on page 1997
- Functions - see Function Metrics on page 2107
- Health Checks - see Health Checks Metrics on page 2121
- Integration - see Viewing Message Metrics
- Load Balancing - see Load Balancing Metrics on page 2567
- Management Agent - see Management Agent Metrics
- MySQL Database - see MySQL Database Metrics
• Networking - see these topics:
  • VNIC Metrics on page 3321
  • FastConnect Metrics on page 3236
  • VPN Connect Metrics on page 3164
  • Service Gateway Metrics on page 3325
• NoSQL Database Cloud - see Service Metrics
• Notifications - see Notifications Metrics on page 3389
• Object Storage - see Object Storage Metrics on page 3499
• OS Management - see OS Management Metrics
• Streaming - see Streaming Metrics on page 3896
• Vault - see Vault Metrics on page 4020
• WAF - see WAF Metrics on page 4170

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

Note:
Metric resources do not have OCIDs.

Ways to Access Monitoring

You can access the Monitoring service using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

Console: To access Monitoring using the Console, you must use a supported browser. Oracle Cloud Infrastructure supports the following browsers and versions:
• Google Chrome 69 or later
• Safari 12.1 or later
• Firefox 62 or later

Open the navigation menu. Under Solutions and Platform, go to Monitoring.

API: To access Monitoring through APIs, use Monitoring API for metrics and alarms and Notifications API for notifications (used with alarms).

Moving Alarms to a Different Compartment

You can move alarms from one compartment to another. When you move an alarm to a new compartment, its associated metrics remain where they are. After you move the alarm to the new compartment, inherent policies apply immediately and affect access to the alarm through the Console. For more information on moving resources to other compartments, see To move a resource to a different compartment on page 2444.

Important:
To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Monitoring resources, see Details for Monitoring on page 2320.
Monitoring

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Administrators: For common policies that give groups access to metrics, see Let users view metric definitions in a compartment on page 2155 and Restrict user access to a specific metric namespace on page 2156. For a common alarms policy, see Let users view alarms on page 2156. To authorize resources, such as instances, to make API calls, add the resources to a dynamic group. Use the dynamic group's matching rules to add the resources, and then create a policy that allows that dynamic group access to metrics. See Let instances make API calls to access monitoring metrics in the tenancy on page 2156.

Limits on Monitoring

See Monitoring Limits on page 227 for a list of applicable limits and instructions for requesting a limit increase.

Other limits include the following.

Storage Limits

<table>
<thead>
<tr>
<th>Item</th>
<th>Time range stored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric definitions</td>
<td>14 days</td>
</tr>
<tr>
<td>Alarm history entries</td>
<td>90 days</td>
</tr>
</tbody>
</table>

Returned Data Limits (Metrics)

When you query metrics and view metric charts, the returned data is subject to certain limits. Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

Troubleshooting Limits

If you see an error that the query has exceeded the maximum number of metric streams, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

Viewing Default Metric Charts

This topic describes how to view metric charts for selected resources or a single resource and create alarms based on queries used for charts. Charts are available using the Console.

Prerequisites

- IAM policies: Viewing metric charts is part of monitoring. To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized,
confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications. For common policies that give groups access to metrics, see Let users view metric definitions in a compartment on page 2155 and Restrict user access to a specific metric namespace on page 2156.

- **Metrics exist in Monitoring:** The resources that you want to monitor must emit metrics to the Monitoring service.
- **Compute instances:** To emit metrics, the Compute Instance Monitoring plugin must be enabled on the instance, and plugins must be running. The instance must also have either a service gateway or a public IP address to send metrics to the Monitoring service. For more information, see Enabling Monitoring for Compute Instances on page 783.

### Working with Default Metric Charts

For background information on metrics in Oracle Cloud Infrastructure, see Metrics Feature Overview on page 2663. For default metrics by service, see Supported Services on page 2669.

Default metric charts use predefined service *queries*. You can select *resources* of interest and update the *interval*, *statistic*, and time range.

**Note:**
Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power). Units correspond to the selected metric and do not change by statistic.

**Using the Console**

**To view default metric charts for all resources**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Choose the Metric Namespace for the resource types of interest in the selected compartment.
   
   For example, choose `oci_lbaas` to see metrics for load balancers.

Default charts are displayed for all resources in the selected **Metric Namespace** and **Compartment**. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).

**Don't see all expected resources or metrics?**

- Try a different time range.
- Make sure the correct **Compartment** is selected.

Metric namespaces are shown only when associated resources exist in the selected compartment. For example, the `oci_autonomous_database` namespace is shown only when Autonomous Databases exist in the selected compartment.

- Confirm that the missing resources are emitting metrics. See Enabling Monitoring for Compute Instances on page 783.
- Review limits information. Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

**To investigate missing resources or metrics**

- Try a different time range.
- Make sure the correct **Compartment** is selected.

Metric namespaces are shown only when associated resources exist in the selected compartment. For example, the `oci_autonomous_database` namespace is shown only when Autonomous Databases exist in the selected compartment.

- Confirm that the missing resources are emitting metrics. See Enabling Monitoring for Compute Instances on page 783.
• Review limits information. Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

To filter results

Filter results to limit the data plotted on the metric chart. For example, filter results to a resource or region of interest.

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. Choose a Compartment and Metric Namespace to view the default charts for the resources of interest.
3. To the right of Dimensions, click Add.
4. In the Edit dimensions dialog box, select a Dimension Name and Dimension Value.

   Dimension fields

   • Dimension Name: A qualifier specified in the metric definition. For example, the dimension resourceId is specified in the metric definition for CpuUtilization.

   Note:

   Long lists of dimensions are trimmed.
   • To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
   • To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

   • Dimension Value: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
   • + Additional dimension: Adds another name-value pair for a dimension.

5. Click Done.

The default charts show the filtered results of your query.

To select different resources

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. Choose a Compartment and Metric Namespace to view the default charts for the resources of interest.
3. To select resources on a different compartment, select the Compartment.

   The default charts update to show results for the selected compartment.

4. To select a specific resource within the selected compartment, filter results by a resource-specific dimension, such as resourceDisplayName:
   a. To the right of Dimensions, click Add.
   b. For Dimension Name, select resourceDisplayName or other resource-specific dimension.

   Note:

   Long lists of dimensions are trimmed.
   • To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
   • To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

   c. For Dimension Value, select the value corresponding to the resource you want.
   d. Click Done.

   The default charts update to show filtered results.

To aggregate data from all metric streams

Aggregate all metric streams to view the average. For example, aggregate all metric streams for CPU Utilization to view the average data across all resources. By default, a chart represents each metric stream with a line, which results
Monitoring in multiple lines per chart. When you aggregate metric streams, a chart represents all metric streams with a single line, which results in just one line per chart.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Choose a **Compartment** and **Metric Namespace** to view the default charts for the resources of interest.
3. Select **Aggregate Metric Streams**.

**To change the time range**

Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the **1h** or **1d** interval values are supported.

For metric queries, the *interval* you select drives the default *resolution* of the request, which determines the maximum time range of data returned.

For more information about the resolution parameter as used in metric queries, see [SummarizeMetricsData](#).

**Maximum time range returned for a query**

The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.

The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>

To specify a non-default resolution that differs from the interval, use the [SummarizeMetricsData](#) operation.

**See examples of returned data**

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of **1m**, and the end time defaults to the current time (**2019-01-08T10:00:00.789Z**). This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st (**2019-01-01T10:00:00.789Z**).

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th (**2019-01-06T10:00:00.789Z**), the earliest data point possible within this seven-day period would be 10:00 on January 1st (**2019-01-01T10:00:00.789Z**). Therefore, only 5 days of metric data points can be returned in this example.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Choose a **Compartment** and **Metric Namespace** to view the default charts for the resources of interest.
3. To select a period of time, such as **Last hour**, click **Start Time** or **End Time**.
4. To enter a time value, click in **Start Time** or **End Time** and then type a value.

**To change a chart interval or statistic**

Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range,
then all interval values are supported. If you select 90 days for the time range, then only the \textbf{1h} or \textbf{1d} interval values are supported.

For metric queries, the \textit{interval} you select drives the default \textit{resolution} of the request, which determines the maximum time range of data returned.

For more information about the resolution parameter as used in metric queries, see \texttt{SummarizeMetricsData}.

\textbf{Maximum time range returned for a query}

The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.

The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>

To specify a non-default resolution that differs from the interval, use the \texttt{SummarizeMetricsData} operation.

\textbf{See examples of returned data}

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of \texttt{1m}, and the end time defaults to the current time \texttt{(2019-01-08T10:00:00.789Z)}. This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st \texttt{(2019-01-01T10:00:00.789Z)}.

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th \texttt{(2019-01-06T10:00:00.789Z)}, the earliest data point possible within this seven-day period would be 10:00 on January 1st \texttt{(2019-01-01T10:00:00.789Z)}. Therefore, only 5 days of metric data points can be returned in this example.

1. Open the navigation menu. Under \texttt{Solutions and Platform}, go to \texttt{Monitoring} and click \texttt{Service Metrics}.
2. Choose a \texttt{Compartment} and \texttt{Metric Namespace} to view the default charts for the resources of interest.
3. At the top of the chart you want, select an \texttt{Interval} or \texttt{Statistic}.

For supported values, see \texttt{Monitoring Query Language (MQL) Reference} on page 2741.

\textbf{To go back to the default charts}

On the upper right of the \texttt{Service Metrics} page, click \texttt{Reset charts}.

\textbf{To view chart details}

Chart details include the \texttt{query} as a Monitoring Query Language (MQL) expression and the names and OCIDs of represented \texttt{resources}.

1. Open the navigation menu. Under \texttt{Solutions and Platform}, go to \texttt{Monitoring} and click \texttt{Service Metrics}.
2. Choose a \texttt{Compartment} and \texttt{Metric Namespace} to view the default charts for the resources of interest.
3. Click the chart you want.
4. To view a list of resources represented in the chart, click the arrow to the left of the query displayed under the chart.

You can copy the OCID for a resource by clicking **Copy** to the right of the resource OCID.

**To share a chart**

**Note:**

The person you share the chart with must have the required IAM policies for access to metrics.

On the **Service Metrics** page, on the upper right of the chart you want, go to **Options**, and then click **Copy Chart URL**.

**To view a query in Metrics Explorer**

On the **Service Metrics** page, on the upper right of the chart you want, go to **Options**, and then click **View Query in Metrics Explorer**.

**To copy a query (MQL expression)**

On the **Service Metrics** page, on the upper right of the chart you want, go to **Options**, and then click **Copy Query (MQL)**.

**To view default metric charts for a single resource**

On the page for the resource of interest, under **Resources**, click **Metrics**.

For example, to view metric data for a Compute instance:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance you're interested in.
3. On the instance details page, under **Resources**, click **Metrics**.

   A chart is shown for each metric. For a list of metrics related to Compute instances, see **Compute Instance Metrics** on page 788.

The Console displays the last hour of metric data for the selected resource. A chart is shown for each metric emitted by the selected resource.

For a list of metrics emitted by your resource, see **Supported Services** on page 2669.

**To create an alarm from a chart query**

Follow the instructions for the page on which the query appears: Service Metrics or Metrics Explorer.

**Service Metrics page**

To create an alarm from a chart query (Service Metrics)

1. View the **Service Metrics** page: Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. Choose a **Compartment** and **Metric Namespace** to view the default charts for the resources of interest.
3. At the top of the chart you're interested in, go to Options, and then select **Create an Alarm on this Query**.
4. On the Create Alarm page, under Define alarm, add the trigger, and fill in or update other alarm settings as needed:

**Alarm settings**

**Basic Mode (default)**

By default, this page uses Basic Mode, which separates the metric from its dimensions and its trigger rule.

- **Alarm Name:**
  User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

- **Alarm Severity:** The perceived type of response required when the alarm is in the firing state.

- **Alarm Body:** The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."

- **Tags (optional):** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description:** The metric to evaluate for the alarm condition.
  - **Compartment:** The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace:** The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group (optional):** The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Metric Name:** The name of the metric. Only one metric can be specified. Example: CpuUtilization
  - **Interval:** The aggregation window, or the frequency at which data points are aggregated.

**Interval values**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Note:**
  Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To
determine valid alarm intervals for a given metric, check the relevant service's metric reference.

- **1m** - 1 minute
- **5m** - 5 minutes
- **1h** - 1 hour
- **1d** - 1 day

**Note:**

For alarm queries, the specified *interval* has no effect on the *resolution* of the request. The only valid value of the resolution for an alarm query request is **1m**. For more information about the resolution parameter as used in alarm queries, see *Alarm*.

**Statistic:** The aggregation function.

Statistic values:

- **COUNT** - The number of observations received in the specified time period.
- **MAX** - The highest value observed during the specified time period.
- **MEAN** - The value of Sum divided by Count during the specified time period.
- **MIN** - The lowest value observed during the specified time period.
- **P50** - The value of the 50th percentile.
- **P90** - The value of the 90th percentile.
- **P95** - The value of the 95th percentile.
- **P99** - The value of the 99th percentile.
- **P99.5** - The value of the 99.5th percentile.
- **RATE** - The per-interval average rate of change.
- **SUM** - All values added together.

**Metric dimensions:** Optional filters to narrow the metric data evaluated.

**Dimension fields**

- **Dimension Name:** A qualifier specified in the metric definition. For example, the dimension resourceId is specified in the metric definition for CpuUtilization.

**Note:**

Long lists of dimensions are trimmed.

- To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
• To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

• **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.

• **Additional dimension**: Adds another name-value pair for a dimension.

• **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.

• **Operator**: The operator used in the condition threshold.

  **Operator values**
  • greater than
  • greater than or equal to
  • equal to
  • less than
  • less than or equal to
  • **between** (inclusive of specified values)
  • **outside** (inclusive of specified values)
  • **absent**

• **Value**: The value to use for the condition threshold.

• **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click **Advanced Mode** or **Switch to Advanced Mode** to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See **Monitoring Query Language (MQL) Reference** on page 2741.

• **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

  **Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

• **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.

• **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."

• **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.
  
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  
  - **Query Code Editor box**: The alarm query as a Monitoring Query Language (MQL) expression.


```
Note:

Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.
```

Example alarm query:

```
CpuUtilization[1m]
{availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
```

For query syntax and examples, see Working with Metric Queries on page 2700.

- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).
5. Under **Notifications**, select or create at least one notification destination:

Notifications settings

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    
    Available options:
    
    - **Notifications Service**.
    
    - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
    
    - **Topic**: The *topic* to use for notifications. Each topic supports a *subscription* protocol, such as PagerDuty.
    
    - **Create a topic**: Sets up a *topic* and *subscription* protocol in the selected compartment, using the specified destination service.

      - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team" for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
      
      - **Topic Description**: Description of the new topic.
      
      - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:

        **Email subscription**

        Sends an email message when you publish a *message* to the subscription's parent *topic*.

        Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

        Some message types allow friendly formatting.

        - **Subscription Protocol**: Select Email.
        
        - **Subscription Email**: Type an email address.

        **HTTPS (Custom URL) subscription**

        Sends specified information when you publish a *message* to the subscription's parent *topic*.

        Endpoint format (URL using HTTPS protocol):

        ```
        https://<anyvalidURL>
        ```

        Basic access authentication is supported, allowing you to specify a username and password in the URL, as in `https://user:password@domain.com` or `https://user@domain.com`. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Subscription Protocol**: Select **HTTPS (Custom URL)**.
- **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a message to the subscription's parent topic.

Endpoint format (URL):

```plaintext
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the [PagerDuty documentation](https://developer.pagerduty.com/docs/).

- **Subscription Protocol**: Select **PagerDuty**.
- **Subscription URL**: Type (or copy and paste) the integration key portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a message to the subscription's parent topic.


Sends a message to the specified Slack channel by default when you publish a message to the subscription's parent topic.

Endpoint format (URL):

```plaintext
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the [Slack documentation](https://developer.slack.com/docs).

- **Subscription Protocol**: Select **Slack**.
- **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a message to the subscription's parent topic. Supported endpoint formats: **E.164 format**.

**Note:**

SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service...
Connector Hub. SMS messages sent by unsupported services are dropped. Troubleshoot dropped messages.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

**Available Countries and Regions**

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
</tbody>
</table>
### Metrics Explorer page

To create an alarm from a chart query (Metrics Explorer)

1. View the Metrics Explorer page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. If necessary, open the query for editing: Click the Edit query icon.
3. Click Create Alarm.
4. On the Create Alarm page, under Define alarm, add the trigger, and fill in or update other alarm settings as needed:

   **Alarm settings**

   **Basic Mode (default)**

   By default, this page uses Basic Mode, which separates the metric from its dimensions and its trigger rule.

   **Alarm Name:**

   User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

   **Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
</tbody>
</table>
### Monitoring

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.

- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."

- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description**: The metric to evaluate for the alarm condition.
  
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  
  - **Metric Name**: The name of the metric. Only one metric can be specified. Example: `CpuUtilization`
  
- **Interval**: The aggregation window, or the frequency at which data points are aggregated.

  **Interval values**

  - **1m** - 1 minute
  - **5m** - 5 minutes
  - **1h** - 1 hour
  - **1d** - 1 day

  **Note:**

  Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

  - **1m** - 1 minute
  - **5m** - 5 minutes
  - **1h** - 1 hour
  - **1d** - 1 day

  **Note:**

  For alarm queries, the specified interval has no effect on the resolution of the request. The only valid value of the resolution for an alarm
Monitoring query request is 1m. For more information about the resolution parameter as used in alarm queries, see Alarm.

- **Statistic**: The aggregation function.
  
  Statistic values
  
  - **COUNT**: The number of observations received in the specified time period.
  - **MAX**: The highest value observed during the specified time period.
  - **MEAN**: The value of Sum divided by Count during the specified time period.
  - **MIN**: The lowest value observed during the specified time period.
  - **P50**: The value of the 50th percentile.
  - **P90**: The value of the 90th percentile.
  - **P95**: The value of the 95th percentile.
  - **P99**: The value of the 99th percentile.
  - **P99.5**: The value of the 99.5th percentile.
  - **RATE**: The per-interval average rate of change.
  - **SUM**: All values added together.

- **Metric dimensions**: Optional filters to narrow the metric data evaluated.

  **Dimension fields**

  - **Dimension Name**: A qualifier specified in the metric definition. For example, the dimension `resourceId` is specified in the metric definition for `CpuUtilization`.

  **Note:**

  Long lists of dimensions are trimmed.
  
  - To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **Additional dimension**: Adds another name-value pair for a dimension.
- **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.
  - **Operator**: The operator used in the condition threshold.
    - **Operator values**
      - greater than
      - greater than or equal to
      - equal to
      - less than
      - less than or equal to
      - between (inclusive of specified values)
      - outside (inclusive of specified values)
      - absent
    - **Value**: The value to use for the condition threshold.
    - **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click Advanced Mode or Switch to Advanced Mode to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See Monitoring Query Language (MQL) Reference on page 2741.

- **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

**Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."
- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Query Code Editor** box: The alarm query as a Monitoring Query Language (MQL) expression.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.</td>
</tr>
</tbody>
</table>

Example alarm query:

```
CpuUtilization[1m]{availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
```

For query syntax and examples, see Working with Metric Queries on page 2700.

- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).
5. Under **Notifications**, select or create at least one notification destination:

Notifications settings

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    
    Available options:
    
    - **Notifications Service**.
    
    - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
    
    - **Topic**: The *topic* to use for notifications. Each topic supports a *subscription* protocol, such as PagerDuty.
    
    - **Create a topic**: Sets up a *topic* and *subscription* protocol in the selected compartment, using the specified destination service.
      
      - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team " for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
      
      - **Topic Description**: Description of the new topic.
      
      - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:
        
        **Email subscription**
        
        Sends an email message when you publish a *message* to the subscription's parent *topic*.
        
        Message contents and appearance vary by message type. See *alarm messages*, *event messages*, and *service connector messages*.
        
        Some message types allow friendly formatting.
        
        - **Subscription Protocol**: Select Email.
        
        - **Subscription Email**: Type an email address.
        
        **HTTPS (Custom URL) subscription**
        
        Sends specified information when you publish a *message* to the subscription's parent *topic*.
        
        Endpoint format (URL using HTTPS protocol):
        
        ```
        https://<anyvalidURL>
        ```
        
        Basic access authentication is supported, allowing you to specify a username and password in the URL, as in https://user:password@domain.com or https://user@domain.com. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Subscription Protocol**: Select HTTPS (Custom URL).
- **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the PagerDuty documentation.

- **Subscription Protocol**: Select PagerDuty.
- **Subscription URL**: Type (or copy and paste) the *integration key* portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the Slack documentation.

- **Subscription Protocol**: Select Slack.
- **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: E.164 format.

**Note:**

SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service...
Monitoring Connector Hub. SMS messages sent by unsupported services are dropped. Troubleshoot dropped messages.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

**Available Countries and Regions**

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Country or region</td>
<td>ISO code</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
</tbody>
</table>

- **Additional destination service**: Adds another destination service and topic to use for notifications.

  **Note:**
  
  Each alarm is limited to one destination per supported destination service.

- **Repeat Notification?**: While the alarm is in the firing state, resends notifications at the specified interval.
- **Notification Interval**: The period of time to wait before resending the notification.
- **Suppress Notifications**: Sets up a suppression time window during which to suspend evaluations and notifications. Useful for avoiding alarm notifications during system maintenance periods.
  
  - **Suppression Description**
  - **Start Time**
  - **End Time**

6. If you want to disable the new alarm, clear **Enable This Alarm?**.
7. Click **Save alarm**.

   The new alarm is listed on the **Alarm Definitions** page.

   For more information about alarms, see **Alarms Feature Overview** on page 2664.

**resource page**

Examples of resource pages are Compute instance detail pages and Block Volume volume detail pages. Alarms are available from these pages for resources that emit metrics.

To create an alarm from a chart query (resource page)

1. To view charts: On the resource page, under **Resources**, click **Metrics**.
2. At the top of the chart you're interested in, go to **Options**, and then select **Create an Alarm on this Query**.
3. On the **Create Alarm** page, under **Define alarm**, add the trigger, and fill in or update other alarm settings as needed:

   **Alarm settings**
   
   **Basic Mode (default)**
   
   By default, this page uses **Basic Mode**, which separates the metric from its dimensions and its trigger rule.
   
   - **Alarm Name**:
     
     User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

   **Rendering of the title by protocol**
   
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Rendering of the title</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: “High CPU usage alert. Follow runbook instructions for resolution.”
- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
- **Metric description**: The metric to evaluate for the alarm condition.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Metric Name**: The name of the metric. Only one metric can be specified. Example: **CpuUtilization**
  - **Interval**: The aggregation window, or the frequency at which data points are aggregated.

**Interval values**

**Note:**

Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

- **1m** - 1 minute
- **5m** - 5 minutes
- **1h** - 1 hour
- **1d** - 1 day

**Note:**

For alarm queries, the specified interval has no effect on the resolution of the request. The only valid value of the resolution for an alarm
monitoring query request is 1m. For more information about the resolution parameter as used in alarm queries, see Alarm.

- **Statistic**: The aggregation function.
  - **COUNT**: The number of observations received in the specified time period.
  - **MAX**: The highest value observed during the specified time period.
  - **MEAN**: The value of Sum divided by Count during the specified time period.
  - **MIN**: The lowest value observed during the specified time period.
  - **P50**: The value of the 50th percentile.
  - **P90**: The value of the 90th percentile.
  - **P95**: The value of the 95th percentile.
  - **P99**: The value of the 99th percentile.
  - **P99.5**: The value of the 99.5th percentile.
  - **RATE**: The per-interval average rate of change.
  - **SUM**: All values added together.

- **Metric dimensions**: Optional filters to narrow the metric data evaluated.

**Dimension fields**

- **Dimension Name**: A qualifier specified in the metric definition. For example, the dimension resourceId is specified in the metric definition for CpuUtilization.

**Note:**

Long lists of dimensions are trimmed.

- To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
• To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **+ Additional dimension**: Adds another name-value pair for a dimension.
- **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.

- **Operator**: The operator used in the condition threshold.
  
  **Operator values**
  
  - greater than
  - greater than or equal to
  - equal to
  - less than
  - less than or equal to
  - between (inclusive of specified values)
  - outside (inclusive of specified values)
  - absent

- **Value**: The value to use for the condition threshold.
- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click **Advanced Mode** or **Switch to Advanced Mode** to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See **Monitoring Query Language (MQL) Reference** on page 2741.

- **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

  **Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."
- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Query Code Editor** box: The alarm query as a Monitoring Query Language (MQL) expression.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.</td>
</tr>
</tbody>
</table>

Example alarm query:

```
CpuUtilization[1m]
{availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
```

For query syntax and examples, see Working with Metric Queries on page 2700.

- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).
4. Under **Notifications**, select or create at least one notification destination:

Notifications settings

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    
    Available options:
    
    - **Notifications Service**.
    
    - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
    
    - **Topic**: The *topic* to use for notifications. Each topic supports a *subscription* protocol, such as PagerDuty.
    
    - **Create a topic**: Sets up a *topic* and *subscription* protocol in the selected compartment, using the specified destination service.
      
      - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team " for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
      
      - **Topic Description**: Description of the new topic.
      
      - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:

        **Email subscription**
        
        Sends an email message when you publish a *message* to the subscription's parent *topic*.
        
        Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.
        
        Some message types allow friendly formatting.
        
        - **Subscription Protocol**: Select Email.
        
        - **Subscription Email**: Type an email address.

        **HTTPS (Custom URL) subscription**
        
        Sends specified information when you publish a *message* to the subscription's parent *topic*.
        
        Endpoint format (URL using HTTPS protocol):
        
        ```
        https://<anyvalidURL>
        ```
        
        Basic access authentication is supported, allowing you to specify a username and password in the URL, as in https://user:password@domain.com or https://user@domain.com. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Subscription Protocol**: Select HTTPS (Custom URL).
- **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the PagerDuty documentation.

- **Subscription Protocol**: Select PagerDuty.
- **Subscription URL**: Type (or copy and paste) the *integration key* portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the Slack documentation.

- **Subscription Protocol**: Select Slack.
- **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: E.164 format.

**Note:**

SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service...
Connector Hub. SMS messages sent by unsupported services are dropped. **Troubleshoot dropped messages.**

Message contents and appearance vary by message type. See [alarm messages](#), [event messages](#), and [service connector messages](#).

### Available Countries and Regions

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
</tbody>
</table>
### Building Metric Queries

This topic describes how to query metrics for resources of interest, create alarms from a given query, and share Console charts.

#### Prerequisites

- **IAM policies**: Querying metrics is part of monitoring. To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications. For common policies that give groups access to metrics, see Let users view metric definitions in a compartment on page 2155 and Restrict user access to a specific metric namespace on page 2156.

- **Metrics exist in Monitoring**: The resources that you want to monitor must emit metrics to the Monitoring service.

- **Compute instances**: To emit metrics, the Compute Instance Monitoring plugin must be enabled on the instance, and plugins must be running. The instance must also have either a service gateway or a public IP address to send metrics to the Monitoring service. For more information, see Enabling Monitoring for Compute Instances on page 783.

#### Working with Metric Queries

This section shows MQL syntax of metric and alarm queries.
Use metric **queries** to actively and passively monitor your cloud resources. Actively monitor with metric queries that you generate spontaneously, on demand. In the Console, update a chart to show data from multiple queries. Store queries you want to reuse. Passively monitor with alarms that add a condition, or trigger rule, to a metric query.

Metric query syntax (boldface elements are required):

```
metric[interval]{dimensionname=dimensionvalue}.groupingfunction.statistic
```

Threshold Alarm query syntax (boldface elements are required):

```
metric[interval]{dimensionname=dimensionvalue}.groupingfunction.statistic
alarmoperator alarmvalue
```

For supported parameter values, see Monitoring Query Language (MQL) Reference on page 2741.

For background information on metrics in Oracle Cloud Infrastructure, see Metrics Feature Overview on page 2663.

**Example queries**

**Simple metric query**

 Maximum CPU Utilization at a one-minute interval.

 Number of lines displayed in the metric chart (Console): 1 per resource.

```
CpuUtilization[1m].max()
```

**Filtered metric query**

 Maximum CPU Utilization at a one-minute interval, filtered to a single resource.

 Number of lines displayed in the metric chart (Console): 1.

```
CpuUtilization[1m]{resourceId="ocid1.instance.oc1.phx.exampleuniqueID"}.max()
```

**Aggregated metric query**

 All IopsRead at a one-minute interval, filtered to a compartment, aggregated for the maximum.

 Number of lines displayed in the metric chart (Console): 1.

```
IopsRead[1m]
{compartmentId="ocid1.compartment.oc1.phx..exampleuniqueID"}.grouping().max()
```

**Group-aggregated metric query**

 Aggregated average of CPU Utilization by availability domain and pool ID, filtered to Compute instances that use the specified shape.

 Number of lines displayed in the metric chart (Console): 1 per pool and 1 per availability domain.

```
CPUUtilization[1m]
{shape="VM.Standard2.8"}.groupBy(availabilityDomain,poolId).mean()
```

**Alarm query (threshold)**

 Triggered when the 90th percentile of CPU Utilization, aggregated by pool ID, and filtered to the specified availability domain, exceeds 85.

 Number of lines displayed in the metric chart (Console): 1 per pool.

```
CpuUtilization[1m]{availabilityDomain="VeBZ:PHX-AD-1"}.groupBy(poolId).percentile(0.9) > 85
```
**Monitoring**

**Grouped count of resources (alarm query or metric query)**

**Note:**

Nested alarm queries are not currently supported in the Console. Use the API to create alarms with nested queries.

An example of a nested query is a grouped count of hosts with up time greater than zero, where the alarm query to identify these hosts is defined within parentheses:

```
(metric[1h].groupBy(host).min() > 0).grouping().count()
```

You can use such a query to either define an alarm or query a metric.

**Using the Console**

**To create a query**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Metrics Explorer**.

   The **Metrics Explorer** page displays an empty chart with fields to build a query.

2. Fill in the fields for a new query.

   - **Compartment**: The compartment containing the resources that you want to monitor. By default, the first accessible compartment is selected.
   - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
   - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
   - **Metric Name**: The name of the metric. Only one metric can be specified. Metric selections depend on the selected compartment and metric namespace. Example: **CpuUtilization**
   - **Interval**: The aggregation window.

   **Interval values**

   Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the **1h** or **1d** interval values are supported.

   - **1m** - 1 minute
   - **5m** - 5 minutes
   - **1h** - 1 hour
   - **1d** - 1 day

   **Note:**

   For metric queries, the *interval* you select drives the default *resolution* of the request, which determines the maximum time range of data returned.

   For more information about the resolution parameter as used in metric queries, see **SummarizeMetricsData**.

   **Maximum time range returned for a query**

   The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.

   The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.
<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>

To specify a non-default resolution that differs from the interval, use the `SummarizeMetricsData` operation.

**See examples of returned data**

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of 1m, and the end time defaults to the current time (2019-01-08T10:00:00.789Z). This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z).

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th (2019-01-06T10:00:00.789Z), the earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z). Therefore, only 5 days of metric data points can be returned in this example.

- **Statistic**: The aggregation function.

  **Statistic values**
  - **COUNT**: The number of observations received in the specified time period.
  - **MAX**: The highest value observed during the specified time period.
  - **MEAN**: The value of Sum divided by Count during the specified time period.
  - **MIN**: The lowest value observed during the specified time period.
  - **P50**: The value of the 50th percentile.
  - **P90**: The value of the 90th percentile.
  - **P95**: The value of the 95th percentile.
  - **P99**: The value of the 99th percentile.
  - **P99.5**: The value of the 99.5th percentile.
  - **RATE**: The per-interval average rate of change.
  - **SUM**: All values added together.

- **Metric dimensions**: Optional filters to narrow the metric data evaluated.

  **Dimension fields**
  - **Dimension Name**: A qualifier specified in the metric definition. For example, the dimension `resourceId` is specified in the metric definition for `CpuUtilization`.

**Note:**

Long lists of dimensions are trimmed.

- To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **+ Additional dimension**: Adds another name-value pair for a dimension.
- **Aggregate Metric Streams**: Aggregates all results to plot a single aggregated average for all metric streams. This average is plotted as a single line on the metric chart. This operation is helpful when you want to plot a metric as one line for all resources.

3. Click **Update Chart**.

The chart shows the results of your new query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power). Units correspond to the selected metric and do not change by statistic.

**Troubleshooting Errors and Query Limits**

If you see an error that the query has exceeded the maximum number of *metric streams*, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

4. To customize the y-axis label or range, type the label you want into **Y-Axis Label** or type the minimum and maximum values you want into **Y-Axis Min Value** and **Y-Axis Max Value**.

Only numeric characters are allowed for custom ranges. Custom labels and ranges are not persisted in shared queries (MQL).

5. To view the query as a Monitoring Query Language (MQL) expression, click **Advanced Mode**.

**Advanced Mode** is located on the right, under the chart.

Use Advanced Mode to edit your query using MQL syntax to aggregate results by group. The MQL syntax also supports additional parameter values. For more information about query parameters in Basic Mode and Advanced Mode, see Monitoring Query Language (MQL) Reference on page 2741.

6. To create another query, click **Add Query** below the chart.

**To change the time range**

Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the **1h** or **1d** interval values are supported.

For metric queries, the *interval* you select drives the default *resolution* of the request, which determines the maximum time range of data returned.

For more information about the resolution parameter as used in metric queries, see SummarizeMetricsData.

**Maximum time range returned for a query**

The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.

The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
</tbody>
</table>
Monitoring

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>

To specify a non-default resolution that differs from the interval, use the SummarizeMetricsData operation.

See examples of returned data

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of 1m, and the end time defaults to the current time (2019-01-08T10:00:00.789Z). This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z).

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th (2019-01-06T10:00:00.789Z), the earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z). Therefore, only 5 days of metric data points can be returned in this example.

1. View the Metrics Explorer page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. To select a period of time, such as Last hour, click Start Time or End Time.
3. To enter a time value, click in Start Time or End Time and then type a value.

To filter results

Filter results to limit the data plotted on the metric chart. For example, filter results to a resource or pool of interest. Filtering is done through selected dimensions; available dimensions vary by metric.

You can also match resource groups provided with the metric. Blank (null) for resource group returns metric data that does not have a resource group.

To filter by dimensions

1. View the Metrics Explorer page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. If necessary, open the query for editing: Click the Edit query icon.
3. Under Metric dimensions, select a Dimension Name and Dimension Value.

Dimension fields

- Dimension Name: A qualifier specified in the metric definition. For example, the dimension resourceId is specified in the metric definition for CpuUtilization.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long lists of dimensions are trimmed.</td>
</tr>
<tr>
<td>• To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.</td>
</tr>
<tr>
<td>• To retrieve all dimensions for a given metric, use the following API operation: ListMetrics</td>
</tr>
</tbody>
</table>

- Dimension Value: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- + Additional dimension: Adds another name-value pair for a dimension.
4. To add a dimension name-value pair, click + Additional dimension.
5. Click **Update Chart**.
   The chart shows the filtered results of your query.

   **Troubleshooting Errors and Query Limits**

   If you see an error that the query has exceeded the maximum number of *metric streams*, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

   Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

6. To view the query as a Monitoring Query Language (MQL) expression, click **Advanced Mode**.

   The dimension name-value fragment appears after the metric-interval fragment.

   In the following example query, the dimension name-value fragment is `{resourceId="ocid1.instance.oc1.phx.exampleuniqueID"}`, which filters results by the specified resource identifier.

   ```
   CpuUtilization[1m]
   {resourceId="ocid1.instance.oc1.phx.exampleuniqueID"}.max()
   ```

   The **MQL** syntax supports more parameter values. See Monitoring Query Language (MQL) Reference on page 2741.

   **To match resource group**

   You can match *resource groups* provided with the metric.

   ```
   Note:
   Blank (null) for resource group returns metric data that does not have a resource group.
   ```

   1. View the **Metrics Explorer** page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click **Metrics Explorer**.
   2. If necessary, open the query for editing: Click the **Edit query** icon.
   3. Select the **Resource Group** you want to use as a filter.
   4. Click **Update Chart**.

      The chart shows query results that match the resource group.

   **Troubleshooting Errors and Query Limits**

   If you see an error that the query has exceeded the maximum number of *metric streams*, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

   Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

   **To aggregate all results**

   Aggregate all results to plot a single aggregated average for all *metric streams*. This average is plotted as a single line on the metric chart. This operation is helpful when you want to plot a metric as one line for all resources.

   1. View the **Metrics Explorer** page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click **Metrics Explorer**.
   2. If necessary, open the query for editing: Click the **Edit query** icon.
   3. Click **Aggregate Metric Streams**.
4. Click **Update Chart**.

The chart shows the results of your query.

**Troubleshooting Errors and Query Limits**

If you see an error that the query has exceeded the maximum number of *metric streams*, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See **MetricData Reference**.

5. To view the query as a Monitoring Query Language (MQL) expression, click **Advanced Mode**.

The *grouping()* function appears before the statistic. For example, the following query returns the maximum (\(\text{max}()\)) IopsRead metric data at a one-minute interval, filtered to a compartment, with all results aggregated.

\[ \text{IopsRead}[1m](\text{compartmentID} = "<\text{compartment\_OCID}>\}).\text{grouping()}.\text{max}() \]

Edit your query in **MQL** to **aggregate results by group**. The MQL syntax also supports more parameter values. See **Monitoring Query Language (MQL) Reference** on page 2741.

To aggregate results by group

<table>
<thead>
<tr>
<th><strong>Note:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregating query results by group requires the <em>groupBy()</em> function, which is available in <strong>Advanced Mode</strong> only.</td>
</tr>
</tbody>
</table>

Aggregate query results by group to plot group-specific aggregated averages. Each group's average is plotted as a single line on the metric chart. This operation is helpful when you want to identify trends by group rather than individual resource.

For example, the following query returns the average (\(\text{mean}()\)) CPU Utilization metric data at a one-minute interval. Results are filtered to the specified *shape* and grouped by *availability domain*. If you have Compute instances of this shape sending metrics across three availability domains, then three lines are plotted on the metric chart.

\[ \text{CPUUtilization}[1m]\{\text{shape}="\text{VM.Standard1.1}"\}.\text{groupBy}(\text{availabilityDomain}).\text{mean}() \]

You can also aggregate by resource groups when provided with the metric (*groupBy*(resourceGroup)).

1. View the **Metrics Explorer** page: Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Metrics Explorer**.
2. If necessary, open the query for editing: Click the **Edit query** icon.
3. Select **Advanced Mode** below the chart on the right.
4. In the **Query Code Editor** box, insert the *groupBy*({dimension}) function between the metric-interval fragment and the statistic, where {dimension} is the name of a dimension provided in the definition of the indicated metric.

For example, insert the following fragment to group by availability domain, assuming that the dimension is available for the selected metric.

\[ \text{groupBy}(\text{availabilityDomain}) \]

The **MQL** syntax supports more parameter values. See **Monitoring Query Language (MQL) Reference** on page 2741.

5. Click **Update Chart**.

The chart is updated to show a single line for each grouped result.

**Troubleshooting Errors and Query Limits**

If you see an error that the query has exceeded the maximum number of *metric streams*, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams
by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

To edit a query using MQL syntax

Edit your query using MQL syntax to aggregate results by group or for more parameter values. See Monitoring Query Language (MQL) Reference on page 2741.

1. View the Metrics Explorer page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. If necessary, open the query for editing: Click the Edit Query icon.
3. Click Advanced Mode.

   The query is displayed as a Monitoring Query Language (MQL) expression.
4. In the Query Code Editor box, edit the query as needed.
5. Click Update Chart.

   The chart is updated.

Troubleshooting Errors and Query Limits

If you see an error that the query has exceeded the maximum number of metric streams, then update the query to evaluate a number of metric streams that is within the limit. For example, you can reduce the metric streams by specifying dimensions. You can continue to evaluate all metric streams that were in the original query by spreading the metric streams across multiple queries (or alarms).

Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.

To create an alarm from a query

Create an alarm to passively monitor for a condition in results from metric queries. Creating an alarm from a query involves adding a trigger rule to the query and setting up notifications.

1. View the Metrics Explorer page: Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. If necessary, open the query for editing: Click the Edit Query icon.
3. Click Create Alarm.
4. On the Create Alarm page, under Define alarm, add the trigger, and fill in or update other alarm settings as needed:

   Alarm settings
   
   Basic Mode (default)
   
   By default, this page uses Basic Mode, which separates the metric from its dimensions and its trigger rule.

   • Alarm Name:
     
     User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

   Rendering of the title by protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>
• **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.

• **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."

• **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

• **Metric description**: The metric to evaluate for the alarm condition.
  
  • **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  
  • **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  
  • **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  
  • **Metric Name** (optional): The name of the metric. Only one metric can be specified. Example: `CpuUtilization`
  
  • **Interval**: The aggregation window, or the frequency at which data points are aggregated.

**Interval values**

<table>
<thead>
<tr>
<th>Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1m</td>
<td>1 minute</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
</tr>
<tr>
<td>1d</td>
<td>1 day</td>
</tr>
</tbody>
</table>

**Note:**

Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

For alarm queries, the specified interval has no effect on the resolution of the request. The only valid value of the resolution for an alarm
query request is 1m. For more information about the resolution parameter as used in alarm queries, see Alarm.

- **Statistic**: The aggregation function.

  Statistic values
  - **COUNT**: The number of observations received in the specified time period.
  - **MAX**: The highest value observed during the specified time period.
  - **MEAN**: The value of Sum divided by Count during the specified time period.
  - **MIN**: The lowest value observed during the specified time period.
  - **P50**: The value of the 50th percentile.
  - **P90**: The value of the 90th percentile.
  - **P95**: The value of the 95th percentile.
  - **P99**: The value of the 99th percentile.
  - **P99.5**: The value of the 99.5th percentile.
  - **RATE**: The per-interval average rate of change.
  - **SUM**: All values added together.

- **Metric dimensions**: Optional filters to narrow the metric data evaluated.

  **Dimension fields**
  - **Dimension Name**: A qualifier specified in the metric definition. For example, the dimension resourceId is specified in the metric definition for CpuUtilization.

  **Note:**

  Long lists of dimensions are trimmed.
  - To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
• To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **Additional dimension**: Adds another name-value pair for a dimension.
- **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.
  - **Operator**: The operator used in the condition threshold.
    - **Operator values**
      - greater than
      - greater than or equal to
      - equal to
      - less than
      - less than or equal to
      - between (inclusive of specified values)
      - outside (inclusive of specified values)
      - absent
    - **Value**: The value to use for the condition threshold.
  - **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click **Advanced Mode** or **Switch to Advanced Mode** to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See [Monitoring Query Language (MQL) Reference](#) on page 2741.

- **Alarm Name**
  - User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.
  - **Rendering of the title by protocol**
    - **Protocol** | **Rendering of the title**
      - Email | Subject line of the email message.
      - HTTPS (Custom URL) | Not rendered.
      - PagerDuty | Title field of the published message.
      - Slack | Not rendered.
      - SMS | Not rendered.

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."
- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Query Code Editor** box: The alarm query as a Monitoring Query Language (MQL) expression.

  **Note:**

  Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

Example alarm query:

```
CpuUtilization[1m] {availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
```

For query syntax and examples, see Working with Metric Queries on page 2700.

- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).
5. Under **Notifications**, select or create at least one notification destination:

**Notifications settings**

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    
    Available options:
    
    - **Notifications Service**.
    
    - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
    
    - **Topic**: The *topic* to use for notifications. Each topic supports a subscription protocol, such as PagerDuty.
    
    - **Create a topic**: Sets up a *topic* and subscription protocol in the selected compartment, using the specified destination service.
      
      - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team " for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
      
      - **Topic Description**: Description of the new topic.
      
      - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:
        
        **Email subscription**
        
        Sends an email message when you publish a *message* to the subscription's parent *topic*.
        
        Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.
        
        Some message types allow friendly formatting.
        
        - **Subscription Protocol**: Select Email.
        
        - **Subscription Email**: Type an email address.
        
        **HTTPS (Custom URL) subscription**
        
        Sends specified information when you publish a *message* to the subscription's parent *topic*.
        
        Endpoint format (URL using HTTPS protocol):
        
        ```
        https://<anyvalidURL>
        ```
        
        Basic access authentication is supported, allowing you to specify a username and password in the URL, as in `https://user:password@domain.com` or `https://user@domain.com`. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

• **Subscription Protocol**: Select HTTPS (Custom URL).
• **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the PagerDuty documentation.

• **Subscription Protocol**: Select PagerDuty.
• **Subscription URL**: Type (or copy and paste) the integration key portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/). Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the Slack documentation.

• **Subscription Protocol**: Select Slack.
• **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: E.164 format.

**Note:**

SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service...
Connector Hub. SMS messages sent by unsupported services are dropped. **Troubleshoot dropped messages.**

Message contents and appearance vary by message type. See [alarm messages](#), [event messages](#), and [service connector messages](#).

### Available Countries and Regions

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Country or region</td>
<td>ISO code</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
</tbody>
</table>

• **Additional destination service**: Adds another destination service and topic to use for notifications.

**Note:**
Each alarm is limited to one destination per supported destination service.

• **Repeat Notification?**: While the alarm is in the firing state, resends notifications at the specified interval.
• **Notification Interval**: The period of time to wait before resending the notification.
• **Suppress Notifications**: Sets up a suppression time window during which to suspend evaluations and notifications. Useful for avoiding alarm notifications during system maintenance periods.
  • **Suppression Description**
  • **Start Time**
  • **End Time**

6. If you want to disable the new alarm, clear **Enable This Alarm?**.
7. Click **Save alarm**.

The new alarm is listed on the **Alarm Definitions** page.

For more information about alarms, see **Alarms Feature Overview** on page 2664.

**To hide a query from the chart**

1. View the **Metrics Explorer** page: Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Metrics Explorer**.
2. Click the **Toggle query on chart** icon for the query that you want to hide.

**To share a query**

1. View the **Metrics Explorer** page: Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Metrics Explorer**.
2. If necessary, open the query for editing: Click the **Edit query** icon.
3. Click **Advanced Mode**.
4. In the **Query Code Editor** box, copy the query.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use this API operation to find metric names and dimensions (view **metric definitions**):

`ListMetrics`

Use this API operation to query metrics by name (and optionally filter by **dimension**):

`SummarizeMetricsData`
Publishing Custom Metrics

This topic describes how to publish your own custom metrics to the Monitoring service.

You can publish your own metrics to Monitoring using the API. You can view charts of your published metrics using the Console, query metrics using the API, and set up alarms using the Console or API.

Prerequisites

IAM policies: To publish custom metrics, you must be given the required type of access in a policy written by an administrator. This requirement applies whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, check with your administrator. You may not have the required type of access in the current compartment. Administrators: For a related common policy, see Let users publish custom metrics on page 2156.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Note:

When defining your custom metrics, note the following:

- Ensure that your custom metrics do not exceed limits. For example, note the valid range of dimensions and maximum number of streams for custom metrics. See PostMetricData.
- Define your metrics with aggregation in mind. While custom metrics can be posted as frequently as every second (minimum frequency of one second), the minimum aggregation interval is one minute.
- Define your metrics with return limits in mind. Limits information for returned data includes the 100,000 data point maximum and time range maximums (determined by resolution, which relates to interval). See MetricData Reference.
- When retrieving custom metrics, you can match to a resource group. Blank (null) for resource group returns metric data that does not have a resource group.

Use this API operation to publish custom metrics:

PostMetricData

Note:

Oracle recommends the following:

- Send batched requests to maximize metric streams per request. A batched request contains multiple metrics or metric namespaces. Note limits. See PostMetricData.
- Publish metrics only when relevant contexts require monitoring; that is, when data points need to be collected. If you want to publish metrics during inactive periods when no observations exist, then you can manually create "0" values for publishing.

You can access your published custom metrics the same way you access any other metrics stored by the Monitoring service. View charts from queries using the Console, query metrics using the CLI or API, and set up alarms using the Console, CLI, or API.
Example of a batched request

This example shows a single request containing data points for metrics across two metric namespaces.

```json
[
  {
    "namespace":"myFirstNamespace",
    "compartmentId":"ocid1.compartment.oc1..exampleuniqueID",
    "resourceGroup":"myFirstResourceGroup",
    "name":"successRate",
    "dimensions":{
      "resourceId":"ocid1.exampleresource.region1.phx.exampleuniqueID",
      "appName":"myAppA"
    },
    "metadata":{
      "unit":"percent",
      "displayName":"MyAppA Success Rate"
    },
    "datapoints":[
      {
        "timestamp":"2019-03-10T22:19:20Z",
        "value":83.0
      },
      {
        "timestamp":"2019-03-10T22:19:40Z",
        "value":90.1
      }
    ]
  },
  {
    "namespace":"myFirstNamespace",
    "compartmentId":"ocid1.compartment.oc1..exampleuniqueID",
    "resourceGroup":"mySecondResourceGroup",
    "name":"successRate",
    "dimensions":{
      "resourceId":"ocid1.exampleresource.region1.phx.differentuniqId",
      "appName":"myAppA"
    },
    "metadata":{
      "unit":"percent",
      "displayName":"MyAppA Success Rate"
    },
    "datapoints":[
      {
        "timestamp":"2019-03-10T22:19:10Z",
        "value":100.0
      },
      {
        "timestamp":"2019-03-10T22:19:30Z",
        "value":100.0
      }
    ]
  },
  {
    "namespace":"mySecondNamespace",
    "compartmentId":"ocid1.compartment.oc1..exampleuniqueID",
    "name":"deliveryRate",
    "dimensions":{
      "resourceId":"ocid1.exampleresource.region1.phx.exampleuniqueID",
      "appName":"myAppB"
    },
    "metadata":{
      "unit":"bytes",
      "displayName":"MyAppB Delivery Rate"
    }
  }
]
```
Managing Alarms

This topic describes how to create, update, suppress, and delete alarms, as well as how to retrieve alarm history. See also Best Practices for Your Alarms on page 2739.

Prerequisites

- IAM policies: Managing alarms is part of monitoring. To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications. For a common alarms policy, see Let users view alarms on page 2156.
- Metrics exist in Monitoring: The resources that you want to monitor must emit metrics to the Monitoring service.
- Compute instances: To emit metrics, the Compute Instance Monitoring plugin must be enabled on the instance, and plugins must be running. The instance must also have either a service gateway or a public IP address to send metrics to the Monitoring service. For more information, see Enabling Monitoring for Compute Instances on page 783.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Using the Console

To see all firing alarms

Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Status. You can suppress alarms during a given time range. You can also disable and delete alarms.

To create an alarm

This section includes steps to create example alarms as well as any kind of alarm.

To create an example threshold alarm

This procedure walks through creation of an example threshold alarm to detect Compute instances operating at non-optimal thresholds. A threshold alarm is an alarm that checks for metric values outside a given range or value. The procedure uses options as displayed in Basic Mode.

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. Click **Create alarm**.

3. On the **Create Alarm** page, under **Define alarm**, fill in or update the alarm settings:
   - **Alarm Name**: Non-Optimal Alarm
   - **Alarm Severity**: Warning
   - **Alarm Body**: Non-optimal utilization detected. An application or process may be consuming more CPU than usual.
   - **Metric description**:
     - **Compartment**: (select your compartment)
     - **Metric Namespace**: oci_computeagent
     - **Metric Name**: CpuUtilization
     - **Interval**: 1m
   
   **Note:**
   Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.
   - **Statistic**: Count
   - **Trigger rule**:
     - **Operator**: between
     - **Value**: 60
     - **Value**: 80
     - **Trigger Delay Minutes**: 10

4. Set up an email notification under **Notifications, Destinations**:
   - **Destination Service**: Notifications Service
   - **Compartment**: (select your compartment)
   - **Topic**: Click **Create a topic**
     - **Topic Name**: Operations Team
     - **Topic Description**: Resource Monitoring Channel
     - **Subscription Protocol**: Email
     - **Email Addresses**: (type an email address for the operations team here)

5. Repeat notifications every day:
   - **Repeat Notification?**: (select this option)
   - **Notification Interval**: 24 hours

6. Click **Save alarm**.

**To create an example absence alarm**

This procedure walks through creation of an example absence alarm to detect resources that may be down or unreachable. An absence alarm is an alarm that checks for absent metrics (using the absent operator). The procedure uses options as displayed in Basic Mode.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.
2. Click **Create alarm**.
3. On the Create Alarm page, under Define alarm, fill in or update the alarm settings:

- Alarm Name: Up/Down Resource Alarm
- Alarm Severity: Critical
- Alarm Body: Resource may be down. Please investigate. Move workloads to another available resource.
- Metric description:
  - Compartment: (select your compartment)
  - Metric Namespace: oci_computeagent
  - Metric Name: CpuUtilization
  - Interval: 1m

  **Note:**
  Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service’s metric reference.

  - Statistic: Count
  - Trigger rule:
    - Operator: absent
    - Trigger Delay Minutes: 5

4. Set up an email notification under Notifications, Destinations:

- Destination Service: Notifications Service
- Compartment: (select your compartment)
- Topic: Click Create a topic
  - Topic Name: Operations Team
  - Topic Description: Resource Up/Down Channel
  - Subscription Protocol: Email
  - Email Addresses: (type an email address for the operations team here)

  **Note:**
  To add a notification (subscription) for another protocol, such as PagerDuty, create a copy of this alarm and choose the corresponding protocol. For more information about subscription protocols, see To create a subscription on page 3358.

5. Repeat notifications every minute:

- Repeat Notification?: (select this option)
- Notification Interval: 1 minute

6. Click Save alarm.

**To create an alarm (any kind)**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. Click Create alarm.

  **Note:**
  You can also create an alarm from a predefined query on the Service Metrics page. Expand Options and click Create an Alarm on this Query. For more information about service metrics, see Viewing Default Metric Charts on page 2671.
3. On the Create Alarm page, under Define alarm, fill in or update the alarm settings:

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To toggle between Basic Mode and Advanced Mode, click Switch to Advanced Mode or Switch to Basic Mode (to the right of Define Alarm).</td>
</tr>
</tbody>
</table>

**Basic Mode (default)**

By default, this page uses Basic Mode, which separates the metric from its dimensions and its trigger rule.

- **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

  **Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."
- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
- **Metric description**: The metric to evaluate for the alarm condition.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Metric Name**: The name of the metric. Only one metric can be specified. Example: `CpuUtilization`
- **Interval**: The aggregation window, or the frequency at which data points are aggregated.

  **Interval values**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To</td>
</tr>
</tbody>
</table>
determine valid alarm intervals for a given metric, check the relevant service's metric reference.

- **1m** - 1 minute
- **5m** - 5 minutes
- **1h** - 1 hour
- **1d** - 1 day

**Note:**
For alarm queries, the specified *interval* has no effect on the *resolution* of the request. The only valid value of the resolution for an alarm query request is 1m. For more information about the resolution parameter as used in alarm queries, see Alarm.

- **Statistic:** The aggregation function.

  **Statistic values**
  - **COUNT** - The number of observations received in the specified time period.
  - **MAX** - The highest value observed during the specified time period.
  - **MEAN** - The value of Sum divided by Count during the specified time period.
  - **MIN** - The lowest value observed during the specified time period.
  - **P50** - The value of the 50th percentile.
  - **P90** - The value of the 90th percentile.
  - **P95** - The value of the 95th percentile.
  - **P99** - The value of the 99th percentile.
  - **P99.5** - The value of the 99.5th percentile.
  - **RATE** - The per-interval average rate of change.
  - **SUM** - All values added together.

- **Metric dimensions:** Optional filters to narrow the metric data evaluated.

  **Dimension fields**
  - **Dimension Name:** A qualifier specified in the metric definition. For example, the dimension *resourceId* is specified in the metric definition for *CpuUtilization*.

  **Note:**
  Long lists of dimensions are trimmed.
  - To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **+ Additional dimension**: Adds another name-value pair for a dimension.
- **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.
  - **Operator**: The operator used in the condition threshold.
    - **Operator values**
      - greater than
      - greater than or equal to
      - equal to
      - less than
      - less than or equal to
      - between (inclusive of specified values)
      - outside (inclusive of specified values)
      - absent
    - **Value**: The value to use for the condition threshold.
    - **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click Advanced Mode or Switch to Advanced Mode to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See Monitoring Query Language (MQL) Reference on page 2741.

- **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

**Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."
- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.

- **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.

- **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.

- **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.

- **Query Code Editor** box: The alarm query as a Monitoring Query Language (MQL) expression.

  **Note:**

  Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

  Example alarm query:

  ```
  CpuUtilization[1m]
  {availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
  ```

  For query syntax and examples, see Working with Metric Queries on page 2700.

- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    - Available options:
      - **Notifications Service**.
  - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
  - **Topic**: The *topic* to use for notifications. Each topic supports a *subscription* protocol, such as PagerDuty.
  - **Create a topic**: Sets up a *topic* and *subscription* protocol in the selected compartment, using the specified destination service.
    - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team " for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
    - **Topic Description**: Description of the new topic.
    - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:
      - **Email subscription**
        - Sends an email message when you publish a *message* to the subscription’s parent *topic*.
        - Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.
        - Some message types allow friendly formatting.
      - **Subscription Protocol**: Select Email.
      - **Subscription Email**: Type an email address.
    - **HTTPS (Custom URL) subscription**
      - Sends specified information when you publish a *message* to the subscription’s parent *topic*.
      - Endpoint format (URL using HTTPS protocol):
        - `https://<anyvalidURL>`
        - Basic access authentication is supported, allowing you to specify a username and password in the URL, as in `https://user:password@domain.com` or `https://user@domain.com`. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Subscription Protocol**: Select HTTPS (Custom URL).
- **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the [PagerDuty documentation](#).

- **Subscription Protocol**: Select PagerDuty.
- **Subscription URL**: Type (or copy and paste) the *integration key* portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Message contents and appearance vary by message type. See [alarm messages](#), [event messages](#), and [service connector messages](#).

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the [Slack documentation](#).

- **Subscription Protocol**: Select Slack.
- **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: [E.164 format](#).

**Note:**

SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service...
Monitoring

Connector Hub. SMS messages sent by unsupported services are dropped. Troubleshoot dropped messages.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Available Countries and Regions

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
</tbody>
</table>
## Additional destination service

Adds another destination service and topic to use for notifications.

### Note

Each alarm is limited to one destination per supported destination service.

### Repeat Notification?

While the alarm is in the firing state, resends notifications at the specified interval.

### Notification Interval

The period of time to wait before resending the notification.

### Suppress Notifications

Sets up a suppression time window during which to suspend evaluations and notifications. Useful for avoiding alarm notifications during system maintenance periods.

- **Suppression Description**
- **Start Time**
- **End Time**

5. If you want to disable the new alarm, clear **Enable This Alarm?**.
6. Click **Save alarm**.

The new alarm is listed on the **Alarm Definitions** page.

### To disable or enable an alarm

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.
2. Click the alarm that you want to disable or enable.
3. On the alarm detail page, select or clear **Alarm is Enabled**.

### Note

You can also disable and enable alarms when creating or editing an alarm.

### To move an alarm to a different compartment

Associated metrics remain in their current compartments. For more information, see **Moving Alarms to a Different Compartment** on page 2670.

### Note

To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Monitoring resources, see **Details for Monitoring** on page 2320.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.
2. In the **List Scope** section, select a compartment.
3. Click the alarm that you want to move.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To update an alarm
1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. Click the alarm that you want to update.
3. Go to Actions on the right, and then click Edit Alarm.
4. On the Edit Alarm page, under Define alarm, update alarm settings as needed:
   
   **Basic Mode (default)**
   
   By default, this page uses Basic Mode, which separates the metric from its dimensions and its trigger rule.
   
   - **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.
   
   **Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

   - **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
   - **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."
   - **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
   - **Metric description**: The metric to evaluate for the alarm condition.
     
     - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
     
     - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
     
     - **Resource Group (optional)**: The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
     
     - **Metric Name**: The name of the metric. Only one metric can be specified. Example: CpuUtilization
     
     - **Interval**: The aggregation window, or the frequency at which data points are aggregated.

   **Interval values**

   **Note:**

   Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To

Oracle Cloud Infrastructure User Guide
determine valid alarm intervals for a given metric, check the relevant service's metric reference.

- **1m** - 1 minute
- **5m** - 5 minutes
- **1h** - 1 hour
- **1d** - 1 day

**Note:**

For alarm queries, the specified interval has no effect on the resolution of the request. The only valid value of the resolution for an alarm query request is `1m`. For more information about the resolution parameter as used in alarm queries, see Alarm.

- **Statistic:** The aggregation function.

  **Statistic values**
  - **COUNT** - The number of observations received in the specified time period.
  - **MAX** - The highest value observed during the specified time period.
  - **MEAN** - The value of Sum divided by Count during the specified time period.
  - **MIN** - The lowest value observed during the specified time period.
  - **P50** - The value of the 50th percentile.
  - **P90** - The value of the 90th percentile.
  - **P95** - The value of the 95th percentile.
  - **P99** - The value of the 99th percentile.
  - **P99.5** - The value of the 99.5th percentile.
  - **RATE** - The per-interval average rate of change.
  - **SUM** - All values added together.

- **Metric dimensions:** Optional filters to narrow the metric data evaluated.

  **Dimension fields**
  - **Dimension Name:** A qualifier specified in the metric definition. For example, the dimension resourceId is specified in the metric definition for CpuUtilization.

**Note:**

Long lists of dimensions are trimmed.

- To view dimensions by name, type one or more characters in the box. A refreshed (trimmed) list shows matching dimension names.
To retrieve all dimensions for a given metric, use the following API operation: ListMetrics

- **Dimension Value**: The value you want to use for the specified dimension. For example, the resource identifier for your instance of interest.
- **Additional dimension**: Adds another name-value pair for a dimension.
- **Trigger rule**: The condition that must be satisfied for the alarm to be in the firing state. The condition can specify a threshold, such as 90% for CPU Utilization, or an absence.
  - **Operator**: The operator used in the condition threshold.
    - **Operator values**
      - greater than
      - greater than or equal to
      - equal to
      - less than
      - less than or equal to
      - between (inclusive of specified values)
      - outside (inclusive of specified values)
      - absent
    - **Value**: The value to use for the condition threshold.
    - **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

**Advanced Mode**

Click **Advanced Mode** or **Switch to Advanced Mode** to view the alarm query as a Monitoring Query Language (MQL) expression. Edit your query using MQL syntax to aggregate results by group or for additional parameter values. See Monitoring Query Language (MQL) Reference on page 2741.

- **Alarm Name**: User-friendly name for the new alarm. This name is sent as the title for notifications related to this alarm. Avoid entering confidential information.

**Rendering of the title by protocol**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Alarm Severity**: The perceived type of response required when the alarm is in the firing state.
- **Alarm Body**: The human-readable content of the notification delivered. Oracle recommends providing guidance to operators for resolving the alarm condition. Consider adding links to standard runbook practices. Example: "High CPU usage alert. Follow runbook instructions for resolution."

- **Tags (optional)**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For
more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Metric description, dimensions, and trigger rule**: The metric to evaluate for the alarm condition, including dimensions and the trigger rule.
  - **Compartment**: The compartment containing the resources that emit the metrics evaluated by the alarm. The selected compartment is also the storage location of the alarm. By default, the first accessible compartment is selected.
  - **Metric Namespace**: The service or application emitting metrics for the resources that you want to monitor.
  - **Resource Group** (optional): The group that the metric belongs to. A resource group is a custom string provided with a custom metric. Not applicable to service metrics.
  - **Query Code Editor** box: The alarm query as a Monitoring Query Language (MQL) expression.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.</td>
</tr>
</tbody>
</table>

Example alarm query:

```
CpuUtilization[1m]
{availabilityDomain=AD1}.groupBy(poolId).percentile(0.9) > 85
```

For query syntax and examples, see Working with Metric Queries on page 2700.

- **Trigger Delay Minutes**: The number of minutes that the condition must be maintained before the alarm is in firing state.

The chart below the Define alarm section dynamically displays the last six hours of emitted metrics according to currently selected fields for the query. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).
5. Under **Notifications**, update settings as needed:

- **Destinations**
  - **Destination Service**: The provider of the destination to use for notifications.
    
    Available options:
    
    - **Notifications Service**.
  
  - **Compartment**: The *compartment* storing the topic to be used for notifications. Can be a different compartment from the alarm and metric. By default, the first accessible compartment is selected.
  
  - **Topic**: The *topic* to use for notifications. Each topic supports a *subscription* protocol, such as PagerDuty.
  
  - **Create a topic**: Sets up a *topic* and *subscription* protocol in the selected compartment, using the specified destination service.
    
    - **Topic Name**: User-friendly name for the new topic. Example: "Operations Team " for a topic used to notify operations staff of firing alarms. Avoid entering confidential information.
    
    - **Topic Description**: Description of the new topic.
    
    - **Subscription Protocol**: Medium of communication to use for the new topic. Configure your subscription for the protocol you want:
      
      - **Email subscription**
        
        Sends an email message when you publish a *message* to the subscription's parent *topic*.
        
        Message contents and appearance vary by message type. See [alarm messages](#), [event messages](#), and [service connector messages](#).
        
        Some message types allow **friendly formatting**.
        
        - **Subscription Protocol**: Select **Email**.
        
        - **Subscription Email**: Type an email address.
      
      - **HTTPS (Custom URL) subscription**
        
        Sends specified information when you publish a *message* to the subscription's parent *topic*.
        
        Endpoint format (URL using HTTPS protocol):
        
        ```
        https://<anyvalidURL>
        ```
        
        Basic access authentication is supported, allowing you to specify a username and password in the URL, as in `https://user:password@domain.com` or `https://user@domain.com`. The
username and password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Subscription Protocol**: Select HTTPS (Custom URL).
- **Subscription URL**: Type (or copy and paste) the URL you want to use as the endpoint.

### PagerDuty subscription

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the [PagerDuty documentation](https://www.pagerduty.com/docs).

- **Subscription Protocol**: Select PagerDuty.
- **Subscription URL**: Type (or copy and paste) the *integration key* portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

### Slack subscription

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.


Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the [Slack documentation](https://api.slack.com/

- **Subscription Protocol**: Select Slack.
- **Subscription URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

### SMS subscription

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: [E.164 format](https://docs.oracle.com/en/middleware/oci-monitoring/monitoring-docs/monitoring-product-docs/).

**Note:**

SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service...
Connector Hub. SMS messages sent by unsupported services are dropped. **Troubleshoot dropped messages.**

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

**Available Countries and Regions**

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Country or region</td>
<td>ISO code</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
</tbody>
</table>

- **Additional destination service**: Adds another destination service and topic to use for notifications.

**Note:**

Each alarm is limited to one destination per supported destination service.

- **Repeat Notification?**: While the alarm is in the firing state, resends notifications at the specified interval.
- **Notification Interval**: The period of time to wait before resending the notification.
- **Suppress Notifications**: Sets up a suppression time window during which to suspend evaluations and notifications. Useful for avoiding alarm notifications during system maintenance periods.
  - **Suppression Description**
  - **Start Time**
  - **End Time**

6. Select or clear **Enable this alarm?**.
7. Click **Save alarm**.
   
The updated alarm settings are listed on the **Alarm Definitions** page.

### To update an alarm after moving a resource

This section shows how to update the metric compartment of an alarm after you move a resource that is emitting metrics monitored by the alarm. For example, if you move a block volume to another compartment, then the alarm must be updated if you want to continue monitoring metrics from the moved block volume.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.
2. Click the alarm that you want to update.
3. Go to **Actions** on the right, and then click **Edit Alarm**.
4. Update the metric compartment: On the **Edit Alarm** page, under **Metric description** (or **Metric description, dimensions, and trigger rule** for Advanced mode), change the **Compartent** to the compartment where the resource has been moved.

   The chart below the **Define alarm** section dynamically updates according to the selected compartment, displaying the last six hours of emitted metrics. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).

   If the chart is not showing the expected data, then the old compartment might be specified in the query (MQL), as in the following example:

   ```
   IopsRead[1m]
   {compartmentId="ocid1.compartment.oc1.phx..oldcompartmentexampleuniqueID"}.grouping()
   ```
5. If the old compartment is specified in the query, then update the query to reference the new compartment:
   a. Click Advanced Mode or Switch to Advanced Mode to view the alarm query as a Monitoring Query Language (MQL) expression.
   b. In Query Code Editor, update the query to reference the new compartment.

   View example
   Original query:
   ```
   IopsRead[1m]
   {compartmentId="ocid1.compartment.oc1.phx..oldcompartmentexampleuniqueID"}.grouping().max()
   ```
   Updated query:
   ```
   Read[1m]
   {compartmentId="ocid1.compartment.oc1.phx..newcompartmentexampleuniqueID"}.grouping()
   ```

   For more information about query syntax and more examples, see Working with Metric Queries on page 2700.

   The chart below the Define alarm section dynamically updates according to the updated query, displaying the last six hours of emitted metrics. Very small or large values are indicated by International System of Units (SI units), such as M for mega (10 to the sixth power).

   If the chart is not showing the expected data, then confirm that every compartment reference (Compartment, Query Code Editor) points to the new compartment.

6. Click Save alarm.

   The alarm now monitors metrics from the new compartment.

### To suppress alarms

**Important:**

Only one suppression can be configured per alarm. Any existing suppression for the alarm is overwritten when you apply a new suppression.

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. On the Alarm Definitions page, select the check boxes for the alarms you want to suppress.

   **Note:**
   
   You can also suppress alarms from the Alarm Status page or when creating or editing an alarm.

3. Go to Actions and select AddSuppressions.
4. In the Suppress alarms dialog box, select a Start Time and End Time and then optionally fill in a Suppression Description.
5. Click Apply suppressions.

   A suppression is created for each selected alarm. The updated alarm settings are listed on the Alarm Definitions page.

### To delete alarms

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. On the **Alarm Definitions** page, select the check boxes for the alarms you want to delete.

   **Note:**
   
   You can also delete an alarm from its detail page.

3. Go to **Actions** and select **Delete Alarms**.

   The deleted alarms are removed from the compartment and are no longer displayed on the **Alarm definitions** page.

**To view alarm history**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.

2. On the **Alarm Definitions** page, click the alarm that you want to view history for.

   The alarm detail page displays a chart showing data for the indicated time range and a list of timestamped transitions, such as Firing to OK.

   Alarm history is retained for 90 days.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to manage alarms:

- ListAlarms
- GetAlarm
- CreateAlarm
- ChangeAlarmCompartment
- UpdateAlarm
- DeleteAlarm
- ListAlarmsStatus
- RemoveAlarmSuppression
- GetAlarmHistory

**Best Practices for Your Alarms**

This topic describes best practices for working with your **alarms**.

### Create a Set of Alarms for Each Metric

For each metric emitted by your resources, **create alarms** that define the following resource behaviors:

- At risk. The resource is at risk of becoming inoperable, as indicated by metric values.
- Non-optimal. The resource is performing at non-optimal levels, as indicated by metric values.
- Resource is up or down. The resource is either not reachable or not operating.

The following examples use the CpuUtilization metric emitted by the **oci_computeagent metric namespace**. This metric monitors the utilization of the Compute instance and the activity level of any services and applications running on the instance. CpuUtilization is a key performance metric for a cloud service because it indicates CPU usage for the Compute instance and it can be used to investigate performance issues. To learn more about CPU usage, see the following URL: [https://en.wikipedia.org/wiki/CPU_time](https://en.wikipedia.org/wiki/CPU_time).

### At-Risk Example

A typical at-risk threshold for the CpuUtilization metric is any value greater than 80 percent. A Compute instance breaching this threshold is at risk of becoming inoperable. Often the cause of this behavior is one or more applications consuming a high percentage of the CPU.
In this example, you decide to notify the operations team immediately, setting the severity of the alarm as “Critical” because repair is required to bring the instances back to optimal operational levels. You configure alarm notifications to the responsible team by both PagerDuty and email, requesting an investigation and appropriate fixes before the instances go into an inoperable state. You set repeat notifications every minute. When someone responds to the alarm notifications, you temporarily stop notifications using the best practice of suppressing the alarm. Once metrics return to optimal values, you remove the suppression.

Non-Optimal Example
A typical non-optimal threshold for the CpuUtilization metric is from 60 to 80 percent. When the metric values for a Compute instance are within this range, the instance is above the optimal operational range.

In this example, you decide to notify the appropriate individual or team that an application or process is consuming more CPU than usual. You configure a threshold alarm to notify the appropriate contacts, setting the severity of the alarm as “Warning,” as no immediate actions are required to investigate and reduce the CPU. You set notification to email only, directed to the appropriate developer or team, with repeat notifications every 24 hours to reduce email notification noise.

Resource is Up or Down Example
A typical indicator of resource availability is a five-minute absence of the CpuUtilization metric. A Compute instance breaching this threshold is either not reachable or not operating. The resource may have stopped responding, or it might have become unavailable because of connectivity issues.

In this example, you decide to notify the operations team immediately, setting the severity of your absence alarm as “Critical” because repair is required to bring the instances online. You configure alarm notifications to the responsible team by both PagerDuty and email, requesting an investigation and a move of the workloads to another available resource. You set repeat notifications every minute. When someone responds to the alarm notifications, you temporarily stop notifications using the best practice of suppressing the alarm. When the CpuUtilization metric is once again detected from the resource, you remove the suppression.

Select the Correct Alarm Interval for your Metric
Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service's metric reference.

Suppress Alarms During Investigations
Once a team member responds to an alarm, suppress notifications during the effort to investigate or mitigate the issue. Temporarily stopping notifications helps to avoid distractions during the investigation and mitigation. Remove the suppression when the issue has been resolved. For instructions, see To suppress alarms on page 2738.

Routinely Tune Your Alarms
On a regular basis, such as weekly, review your alarms to ensure optimal configuration. Calibrate each alarm's threshold, severity, and notification details, including method, frequency, and targeted audience.
Optimal alarm configuration addresses the following factors:

- Criticality of the resource.
- Appropriate resource behavior. Assess behavior singly and within the context of the service ecosystem. Review metric value fluctuations for a given period of time and then adjust thresholds as needed.
- Acceptable notification noise. Assess the notification method (for example, email or PagerDuty), the appropriate recipients, and the frequency of repeated notifications.

For instructions, see To update an alarm on page 2730.

**Monitoring Query Language (MQL) Reference**

This topic describes the components that appear in *Monitoring Query Language* (MQL) expressions, the order that they appear in, and valid values.

*MQL* syntax governs expressions for querying metrics that are published to the Monitoring service. In the Console, MQL expressions appear in **Advanced Mode**. If you don't need to aggregate results by group or to use other advanced query functionality, then you can create simpler versions of metric queries using **Basic Mode** in the Console.

**Components in an MQL Expression**

An MQL expression includes the following components:

- *metric*
- *interval*
- *dimensions*, as one or more name-value pairs (optional)
- grouping function (optional)
- *statistic*
- comparison operation (optional). Useful for defining alarms.

The query components appear in the following order (boldface components are required):

```
metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic
```

Comparison operation queries used for *alarms* can take the following formats (boldface components are required):

- `metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic (where the statistic is absent())`
- `metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic operator value`
- `metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic operator (value1, value2)`

You can nest alarm queries and metric queries.

**Note:**

Nested alarm queries are not currently supported in the Console. Use the API to create alarms with nested queries.
In a nested query, the alarm portion appears at the beginning (surrounded with parentheses), followed by the grouping function (optional) and the statistic. The following syntax indicates required components using boldface type.

\[(\text{metric}[\text{interval}])\{\text{dimensionname}="\text{dimensionvalue}"\}.\text{groupingfunction}.\text{statistic}\].\text{groupingfunction}.\text{statistic}

Example 1: The number of hosts with CPU utilization greater than 80 percent:

\[(\text{CpuUtilization}[1m].\text{max()} > 80).\text{grouping()}.\text{sum()}\]

Example 2: The number of availability domains with a success rate lower than 0.99:

\[(\text{SuccessRate}[1m].\text{groupBy(availabilityDomain)}.\text{mean()} < 0.99).\text{grouping()}.\text{sum()}\]

### Metric Query Component

The *metric* component of the query appears before the interval.

\[\text{metric}[\text{interval}]{\text{dimensionname}="\text{dimensionvalue}"}.\text{groupingfunction}.\text{statistic}\]

Valid values for *metric* depend on the *resource*. An example of a metric is CpuUtilization, sent by Compute instances. For a list of supported resources with links to their metric references, see [Supported Services](#) on page 2669. You can also use the [ListMetrics](#) operation to find metrics sent by a particular service, such as the Compute service. This operation returns *metric definitions*.

### Interval Query Component

The *interval* component of the query appears between the metric and statistic (before the optional dimension name-value pair and grouping function).

\[\text{metric}[\text{interval}]{\text{dimensionname}="\text{dimensionvalue}"}.\text{groupingfunction}.\text{statistic}\]

Supported values for *interval* depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the *1h* or *1d* interval values are supported.

The Monitoring Query Language (MQL) syntax (**Advanced Mode** in the Console) supports the following range of values for *interval*:

1m-60m, 1h-24h, 1d

The **Interval** option in the Console (**Basic Mode**) supports the following range of values:

- **1m** - 1 minute
- **5m** - 5 minutes
- **1h** - 1 hour
- **1d** - 1 day

### Note:

Valid alarm intervals depend on the frequency at which the metric is emitted. For example, a metric emitted every five minutes requires a 5-minute alarm interval or higher. Most metrics are emitted every minute, which means most metrics support any alarm interval. To determine valid alarm intervals for a given metric, check the relevant service’s metric reference.

For metric queries, the *interval* you select drives the default *resolution* of the request, which determines the maximum time range of data returned.

For more information about the resolution parameter as used in metric queries, see [SummarizeMetricsData](#).

---

**Oracle Cloud Infrastructure User Guide** 2742
Maximum time range returned for a query

The maximum time range returned for a metric query depends on the resolution. By default, for metric queries, the resolution is the same as the query interval.

The maximum time range is calculated using the current time, regardless of any specified end time. Following are the maximum time ranges returned for each interval selection available in the Console (Basic Mode). To specify an interval value that is not available in Basic Mode in the Console, such as 12 hours, switch to Advanced Mode.

<table>
<thead>
<tr>
<th>Interval</th>
<th>Default resolution (metric queries)</th>
<th>Maximum time range returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1 day</td>
<td>90 days</td>
</tr>
<tr>
<td>1h</td>
<td>1 hour</td>
<td>90 days</td>
</tr>
<tr>
<td>5m</td>
<td>5 minutes</td>
<td>30 days</td>
</tr>
<tr>
<td>1m</td>
<td>1 minute</td>
<td>7 days</td>
</tr>
</tbody>
</table>

To specify a non-default resolution that differs from the interval, use the SummarizeMetricsData operation.

See examples of returned data

Example 1: One-minute interval and resolution up to the current time, sent at 10:00 on January 8th. No resolution or end time is specified, so the resolution defaults to the interval value of 1m, and the end time defaults to the current time (2019-01-08T10:00:00.789Z). This request returns a maximum of 7 days of metric data points. The earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z).

Example 2: Five-minute interval with one-minute resolution up to two days ago, sent at 10:00 on January 8th. Because the resolution drives the maximum time range, a maximum of 7 days of metric data points is returned. While the end time specified was 10:00 on January 6th (2019-01-06T10:00:00.789Z), the earliest data point possible within this seven-day period would be 10:00 on January 1st (2019-01-01T10:00:00.789Z). Therefore, only 5 days of metric data points can be returned in this example.

For alarm queries, the specified interval has no effect on the resolution of the request. The only valid value of the resolution for an alarm query request is 1m. For more information about the resolution parameter as used in alarm queries, see Alarm.

Dimension Query Component

The dimensionname="dimensionvalue" component of the query appears between the interval and statistic (before the optional grouping function).

metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic

Surround the dimension value with double quotes. Example dimension name-value pair for filtering by availability domain: availabilityDomain = "VeBZ:PHX-AD-1"

You can specify multiple dimension name-value pairs. Place each pair within the brackets and separate the pairs with commas.
Valid values for `dimensionname` depend on the `metric`. An example of a dimension name is `resourceDisplayName`, included with the `CpuUtilization` metric sent by Compute instances. For a list of supported resources with links to their metric references, including dimensions, see Supported Services on page 2669. You can also use the ListMetrics operation to find metrics (and their dimensions) sent by a particular application or service, such as the Compute service.

### Grouping Function Query Component

The `groupingfunction` component of the query appears between the interval and statistic (after the optional dimension name-value pair).

```
metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic
```

Valid grouping functions are as follows.

<table>
<thead>
<tr>
<th>Grouping function (MQL expression; Advanced Mode in the Console)</th>
<th>Grouping function option (Basic Mode in the Console)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>groupBy()</code></td>
<td>(not available)</td>
<td>Aggregates query results by group (dimension or resource group). For example, <code>groupBy(availabilityDomain)</code> groups results by availability domain so that results from each availability domain are together.</td>
</tr>
<tr>
<td><code>grouping()</code></td>
<td>Aggregate Metric Streams</td>
<td>Aggregates all query results.</td>
</tr>
</tbody>
</table>

### Statistic Query Component

The `statistic` component of the query appears after the interval and optional dimension name-value pair and grouping function.

```
metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic
```

Valid statistics are as follows.

<table>
<thead>
<tr>
<th>Statistic (MQL expression; Advanced Mode in the Console)</th>
<th>Statistic option (Basic Mode in the Console)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>absent()</code></td>
<td>(see absent)</td>
<td>Returns 1 if the metric is not present in the whole interval. Otherwise, returns 0. Useful for defining alarms.</td>
</tr>
<tr>
<td><code>avg()</code></td>
<td>(not available)</td>
<td>Returns the value of Sum divided by Count during the specified time period. Identical to <code>mean()</code>.</td>
</tr>
<tr>
<td><code>count()</code></td>
<td>COUNT</td>
<td>Returns the number of observations received in the specified time period.</td>
</tr>
<tr>
<td><code>increment()</code></td>
<td>(not available)</td>
<td>Returns the per-interval change.</td>
</tr>
<tr>
<td><code>max()</code></td>
<td>MAX</td>
<td>Returns the highest value observed during the specified time period.</td>
</tr>
<tr>
<td><code>mean()</code></td>
<td>MEAN</td>
<td>Returns the value of Sum divided by Count during the specified time period.</td>
</tr>
<tr>
<td>Statistic (MQL expression; Advanced Mode in the Console)</td>
<td>Statistic option (Basic Mode in the Console)</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>min()</td>
<td>MIN</td>
<td>Returns the lowest value observed during the specified time period.</td>
</tr>
<tr>
<td>percentile()</td>
<td>P50 P90 P95 P99 P99.9</td>
<td>Returns the estimated value of the specified percentile. Valid values are greater than 0.0 and less than 1.0. For example, percentile(0.8) returns the value of the 80th percentile.</td>
</tr>
<tr>
<td>rate()</td>
<td>RATE</td>
<td>Returns the per-interval average rate of change. The unit is per-second.</td>
</tr>
<tr>
<td>sum()</td>
<td>SUM</td>
<td>Returns all values added together.</td>
</tr>
</tbody>
</table>

### Operator and Value Query Component

The *operator value* component of the query appears after the statistic in threshold alarm queries. Either one or two values are needed, depending on the operator:

- `metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic operator value`  
- `metric[interval]{dimensionname="dimensionvalue"}.groupingfunction.statistic operator (value1, value2)`

Valid operators are as follows.

<table>
<thead>
<tr>
<th>Operator (MQL expression; Advanced Mode in the Console)</th>
<th>Operator option (Basic Mode in the Console)</th>
<th>Number of values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>greater than</td>
<td>1</td>
</tr>
<tr>
<td>&gt;=</td>
<td>greater than or equal to</td>
<td>1</td>
</tr>
<tr>
<td>==</td>
<td>equal to</td>
<td>1</td>
</tr>
<tr>
<td>!= (not equal to)</td>
<td>(not available)</td>
<td>1</td>
</tr>
<tr>
<td>&lt;</td>
<td>less than</td>
<td>1</td>
</tr>
<tr>
<td>&lt;=</td>
<td>less than or equal to</td>
<td>1</td>
</tr>
<tr>
<td>in (inclusive of specified values)</td>
<td>between (inclusive of specified values)</td>
<td>2</td>
</tr>
<tr>
<td>not in (inclusive of specified values)</td>
<td>outside (inclusive of specified values)</td>
<td>2</td>
</tr>
<tr>
<td>Not applicable. See absent().</td>
<td>absent</td>
<td>0</td>
</tr>
</tbody>
</table>
Chapter 26

Networking

This chapter explains how to set up cloud networks.

Networking Components

Get a high-level overview of the Networking service.

Manage VNICS

Manage Virtual Network Interface Cards (VNICS) in a virtual cloud network.

Set up VPN Connect

Set up a site-to-site virtual private network (VPN).

Troubleshoot Networking

Troubleshoot common issues and error messages.

Features

Virtual Cloud Network (VCN)

A virtual, private network that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use. A VCN resides in a single Oracle Cloud Infrastructure region and covers one or more CIDR blocks of your choice.

See Virtual Cloud Networks for more information.
FastConnect
Oracle Cloud Infrastructure FastConnect provides an easy way to create a dedicated, private connection between your data center and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections.

See FastConnect for more information.

VPN Connect
The VPN connection uses industry-standard IPSec protocols. The Oracle service that provides site-to-site connectivity is named VPN Connect (also referred to as an IPSec VPN).

Other secure VPN solutions include OpenVPN, a Client VPN solution that can be accessed in the Oracle Marketplace. OpenVPN connects individual devices to your VCN, but not whole sites or networks.

See VPN Connect for more information.

DNS
The Domain Name System (DNS) lets computers use hostnames instead of IP addresses to communicate with each other. See DNS in VCNs for more information.

The Oracle Cloud Infrastructure Domain Name System (DNS) service lets you create and manage your DNS zones. You can create zones, add records to zones, and allow Oracle Cloud Infrastructure’s edge network to handle your domain's DNS queries. Also see DNS Service for more information about the DNS service.

Load Balancing
The Oracle Cloud Infrastructure Load Balancing service provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). The service offers a load balancer with your choice of a public or private IP address, and provisioned bandwidth.

A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability. You can configure multiple load balancing policies and application-specific health checks to ensure that the load balancer directs traffic only to healthy instances. The load balancer can reduce your maintenance window by draining traffic from an unhealthy application server before you remove it from service for maintenance.

See Load Balancing for more information.

Traffic Management
The Oracle Cloud Infrastructure Traffic Management Steering Policies service is a critical component of DNS. Traffic Management Steering Policies enable you to configure policies to serve intelligent responses to DNS queries, meaning different answers (endpoints) may be served for the query depending on the logic the customer defines in the policy.

See Traffic Management for more information.

Health Checks
The Oracle Cloud Infrastructure Health Checks service provides users with high frequency external monitoring to determine the availability and performance of any publicly facing service, including hosted websites, API endpoints, or externally facing load balancers. By using Health Checks, users can ensure that they are immediately aware of any availability issue affecting their customers.

See Health Checks for more information.

Service Gateway
Another optional virtual router that you can add to your VCN. It provides a path for private network traffic between your VCN and supported services in the Oracle Services Network (examples: Oracle Cloud Infrastructure Object Storage and Autonomous Database). For example, DB Systems in a private subnet in your VCN can back up data.
Networking Overview

When you work with Oracle Cloud Infrastructure, one of the first steps is to set up a virtual cloud network (VCN) for your cloud resources. This topic gives you an overview of Oracle Cloud Infrastructure Networking components and typical scenarios for using a VCN.

Networking Components

The Networking service uses virtual versions of traditional network components you might already be familiar with:

**VIRTUAL CLOUD NETWORK (VCN)**

A virtual, private network that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use. A VCN resides in a single Oracle Cloud Infrastructure region and covers one or more CIDR blocks of your choice. See Allowed VCN Size and Address Ranges on page 2750. The terms *virtual cloud network, VCN,* and *cloud network* are used interchangeably in this documentation. For more information, see VCNs and Subnets on page 2821.

**SUBNETS**

Subdivisions you define in a VCN (for example, 10.0.0.0/24 and 10.0.1.0/24). Subnets contain virtual network interface cards (VNICs), which attach to instances. Each subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. You can designate a subnet to exist either in a single availability domain or across an entire region (regional subnets are recommended). Subnets act as a unit of configuration within the VCN: All VNICs in a given subnet use the same route table, security lists, and DHCP options (see the definitions that follow). You can designate a subnet as either public or private when you create it. Private means VNICs in the subnet can't have public IP addresses. Public means VNICs in the subnet can have public IP addresses at your discretion. See Access to the Internet on page 2752.

**VNIC**

A virtual network interface card (VNIC), which attaches to an instance and resides in a subnet to enable a connection to the subnet's VCN. The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each instance has a primary VNIC that's created during instance launch and cannot be removed. You can add secondary VNICs to an existing instance (in the same availability domain as the primary VNIC), and remove them as you like. Each secondary VNIC can be in a subnet in the same VCN as the primary VNIC, or in a different subnet that is either in the same VCN or a different one. However, all the VNICs must be in the same availability domain as the instance. For more information, see Virtual Network Interface Cards (VNICs) on page 2855.

**PRIVATE IP**

A private IPv4 address and related information for addressing an instance (for example, a hostname for DNS). Each VNIC has a primary private IP, and you can add and remove secondary private IPs. The primary private IP address on an instance doesn't change during the instance's lifetime and cannot be removed from the instance. For more information, see Private IP Addresses on page 2864.

**PUBLIC IP**

A public IPv4 address and related information. You can optionally assign a public IP to your instances or other resources that have a private IP. Public IPs can be either *ephemeral* or *reserved.* For more information, see Public IP Addresses on page 2875.

**IPV6**

An IPv6 address and related information. IPv6 is currently supported only in the Government Cloud. For more information, see IPv6 Addresses on page 2889.
DYNAMIC ROUTING GATEWAY (DRG)

An optional virtual router that you can add to your VCN. It provides a path for private network traffic between your VCN and on-premises network. You can use it with other Networking components and a router in your on-premises network to establish a connection by way of IPSec VPN or Oracle Cloud Infrastructure FastConnect. It can also provide a path for private network traffic between your VCN and another VCN in a different region. For more information, see Access to Your On-Premises Network on page 2753, Dynamic Routing Gateways (DRGs) on page 2927, and Remote VCN Peering (Across Regions) on page 3280.

INTERNET GATEWAY

Another optional virtual router that you can add to your VCN for direct internet access. For more information, see Access to the Internet on page 2752 and also Scenario A: Public Subnet on page 2756.

NETWORK ADDRESS TRANSLATION (NAT) GATEWAY

Another optional virtual router that you can add to your VCN. It gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections. For more information, see Public vs. Private Subnets on page 2752 and also NAT Gateway on page 3247.

SERVICE GATEWAY

Another optional virtual router that you can add to your VCN. It provides a path for private network traffic between your VCN and supported services in the Oracle Services Network (examples: Oracle Cloud Infrastructure Object Storage and Autonomous Database). For example, DB Systems in a private subnet in your VCN can back up data to Object Storage without needing public IP addresses or access to the internet. For more information, see Access to Oracle Services: Service Gateway on page 3256.

LOCAL PEERING GATEWAY (LPG)

Another optional virtual router that you can add to your VCN. It lets you peer one VCN with another VCN in the same region. Peering means the VCNs communicate using private IP addresses, without the traffic traversing the internet or routing through your on-premises network. A given VCN must have a separate LPG for each peering it establishes. For more information, see Local VCN Peering (Within Region) on page 3267.

REMOTE PEERING CONNECTION (RPC)

A component that you can add to a DRG. It lets you peer one VCN with another VCN in a different region. For more information, see Remote VCN Peering (Across Regions) on page 3280.

ROUTE TABLES

Virtual route tables for your VCN. They have rules to route traffic from subnets to destinations outside the VCN by way of gateways or specially configured instances. Your VCN comes with an empty default route table, and you can add custom route tables of your own. For more information, see Route Tables on page 2921.

SECURITY RULES

Virtual firewall rules for your VCN. They are ingress and egress rules that specify the types of traffic (protocol and port) allowed in and out of the instances. You can choose whether a given rule is stateful or stateless. For example, you can allow incoming SSH traffic from anywhere to a set of instances by setting up a stateful ingress rule with source CIDR 0.0.0.0/0, and destination TCP port 22. To implement security rules, you can use network security groups or security lists. A network security group consists of a set of security rules that apply only to the resources in that group. Contrast this with a security list, where the rules apply to all the resources in any subnet that uses the list. Your VCN comes with a default security list with default security rules. For more information, see Security Rules on page 2833.

DHCP OPTIONS

Configuration information that is automatically provided to the instances when they boot up. For more information, see DHCP Options on page 2917.
Allowed VCN Size and Address Ranges

A VCN covers one or more IPv4 CIDR blocks of your choice. The allowable VCN size range is /16 to /30. Example: 10.0.0.0/16. The Networking service reserves the first two IP addresses and the last one in each subnet's CIDR.

For your VCN, Oracle recommends using the private IP address ranges specified in RFC 1918 (10.0.0.0/16, 172.16/16, and 192.168/16). However, you can use a publicly routable range. Regardless, this documentation uses the term private IP address when referring to IP addresses in your VCN's CIDR. Address ranges that are disallowed are described in IP Addresses Reserved for Use by Oracle on page 2754.

The VCN's CIDR blocks must not overlap with each other, with CIDRs in your on-premises network, or with the CIDRs of another VCN you peer with. The subnets in a given VCN must not overlap with each other. For reference, here's a CIDR calculator.

IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

Availability Domains and Your VCN

Your VCN resides in a single Oracle Cloud Infrastructure region. A region can have multiple availability domains to provide isolation and redundancy. For more information, see Regions and Availability Domains.

Originally subnets were designed to cover only one availability domain (AD) in a region. They were all AD-specific, which means the subnet's resources were required to reside in a particular availability domain. Now subnets can be either AD-specific or regional. You choose the type when you create the subnet. Both types of subnets can co-exist in the same VCN. In the following diagram, subnets 1-3 are AD-specific, and subnet 4 is regional.
Aside from the removal of the AD constraint, regional subnets behave the same as AD-specific subnets. Oracle recommends using regional subnets because they're more flexible. They make it easier to efficiently divide your VCN into subnets while also designing for availability domain failure.

When you create a resource such as a Compute instance, you choose which availability domain the resource will be in. From a virtual networking standpoint, you must also choose which VCN and subnet the instance will be in. You can either choose a regional subnet, or choose an AD-specific subnet that matches the AD you chose for the instance.

**Default Components that Come With Your VCN**

Your VCN automatically comes with these default components:

- Default route table, with no route rules
- Default security list, with default security rules
- Default set of DHCP options, with default values
You can't delete these default components. However, you can change their contents (for example, the rules in the default security list). And you can create your own custom versions of each kind of component in your VCN. There are limits to how many you can create and the maximum number of rules. For more information, see Service Limits on page 215.

Each subnet always has these components associated with it:

- One route table
- One or more security lists (for the maximum number, see Service Limits on page 215)
- One set of DHCP options

During subnet creation, you can choose which route table, security list, and set of DHCP options the subnet uses. If you don't specify a particular component, the subnet automatically uses the VCN's default component. You can change which components the subnet uses at any time.

**Tip:**

Security lists are one way to control traffic in and out of the VCN's resources. You can also use network security groups, which let you apply a set of security rules to a set of resources that all have the same security posture.

**Connectivity Choices**

You can control whether subnets are public or private, and whether instances get public IP addresses. You can set up your VCN to have access to the internet if you like. You can also privately connect your VCN to public Oracle Cloud Infrastructure services such as Object Storage, to your on-premises network, or to another VCN.

**Public vs. Private Subnets**

When you create a subnet, by default it's considered public, which means instances in that subnet are allowed to have public IP addresses. Whoever launches the instance chooses whether it has a public IP address. You can override that behavior when creating the subnet and request that it be private, which means instances launched in the subnet are prohibited from having public IP addresses. Network administrators can therefore ensure that instances in the subnet have no internet access, even if the VCN has a working internet gateway, and security rules and firewall rules allow the traffic.

**How IP Addresses Are Assigned**

Each instance has a primary VNIC that's created during instance launch and cannot be removed. You can add secondary VNICs to an existing instance (in the same availability domain as the primary VNIC) and remove them as you like.

Every VNIC has a private IP address from the associated subnet's CIDR. You can choose the particular IP address (during instance launch or secondary VNIC creation), or Oracle can choose it for you. The private IP address does not change during the lifetime of the instance and cannot be removed. You can also add secondary private IPs to a VNIC.

If the VNIC is in a public subnet, then each private IP on that VNIC can have a public IP assigned to it at your discretion. Oracle chooses the particular IP address. There are two types of public IPs: ephemeral and reserved. An ephemeral public IP exists only for the lifetime of the private IP it's assigned to. In contrast, a reserved public IP exists as long as you want it to. You maintain a pool of reserved public IPs and allocate them to your instances at your discretion. You can move them from resource to resource in a region as you need to.

**Access to the Internet**

There are two optional gateways (virtual routers) that you can add to your VCN depending on the type of internet access you need:

- **Internet gateway:** For resources with public IP addresses that need to be reached from the internet (example: a web server) or need to initiate connections to the internet.
- **NAT gateway:** For resources without public IP addresses that need to initiate connections to the internet (example: for software updates) but need to be protected from inbound connections from the internet.
Networking

Just having an internet gateway alone does not expose the instances in the VCN's subnets directly to the internet. The following requirements must also be met:

- The **internet gateway** must be enabled (by default, the internet gateway is enabled upon creation).
- The subnet must be **public**.
- The subnet must have a **route rule** that directs traffic to the internet gateway.
- The subnet must have **security list rules** that allow the traffic (and each instance's firewall must allow the traffic).
- The instance must have a **public IP address**.

**Tip:**

To access public services such as Object Storage from your VCN without the traffic going over the internet, use a **service gateway**.

Also, notice that traffic through an internet gateway between a VCN and a public IP address that is part of Oracle Cloud Infrastructure (such as Object Storage) is routed without being sent over the internet.

You can also give a subnet **indirect** access to the internet by setting up an internet proxy in your on-premises network and then connecting that network to your VCN by way of a DRG. For more information, see **Access to Your On-Premises Network** on page 2753.

**Access to Public Oracle Cloud Infrastructure Services**

You can use a service gateway with your VCN to enable private access to public Oracle Cloud Infrastructure services such as Object Storage. For example, DB Systems in a private subnet in your VCN can back up data to Object Storage without needing public IP addresses or access to the internet. No internet gateway or NAT is required. For more information, see **Access to Oracle Services: Service Gateway** on page 3256.

**Access to Your On-Premises Network**

There are two ways to connect your on-premises network to Oracle Cloud Infrastructure:

- **VPN Connect**: Offers multiple IPSec tunnels between your existing network's edge and your VCN, by way of a DRG that you create and attach to your VCN.
- **Oracle Cloud Infrastructure FastConnect**: Offers a private connection between your existing network's edge and Oracle Cloud Infrastructure. Traffic does not traverse the internet. Both private peering and public peering are supported. That means your on-premises hosts can access private IPv4 addresses in your VCN as well as regional public IPv4 addresses in Oracle Cloud Infrastructure (for example, Object Storage or public load balancers in your VCN).

You can use one or both types of the preceding connections. If you use both, you can use them simultaneously, or in a redundant configuration. These connections come to your VCN by way of a single DRG that you create and attach to your VCN. Without that DRG attachment and a route rule for the DRG, traffic does not flow between your VCN and on-premises network. At any time, you can detach the DRG from your VCN but maintain all the remaining components that form the rest of the connection. You could then reattach the DRG again, or attach it to another VCN.

**Access to Another VCN**

You can connect your VCN to another VCN over a private connection that doesn't require the traffic to traverse the internet. In general, this type of connection is referred to as **VCN peering**. Each VCN must have specific components to enable peering. The VCNs must also have specific IAM policies, route rules, and security rules that permit the connection to be made and the wanted network traffic to flow over the connection. For more information, see **Access to Other VCNs: Peering** on page 3265.

**Connection to Oracle Cloud Infrastructure Classic**

You can set up a connection between your Oracle Cloud Infrastructure environment and Oracle Cloud Infrastructure Classic environment. This connection can facilitate hybrid deployments between the two environments, or migration from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. For more information, see **Access to Oracle Cloud Infrastructure Classic** on page 3289.
Connection to Microsoft Azure

Oracle and Microsoft have created a cross-cloud connection between Oracle Cloud Infrastructure and Microsoft Azure in certain regions. This connection lets you set up cross-cloud workloads without the traffic between the clouds going over the internet. For more information, see Access to Microsoft Azure on page 3299.

Connection to Other Clouds with Libreswan

You can connect your VCN to another cloud provider by using an IPSec VPN with a Libreswan VM as the customer-premises equipment (CPE). For more information, see Access to Other Clouds with Libreswan on page 3310.

Networking Scenarios

This documentation includes a few basic networking scenarios to help you understand the Networking service and generally how the components work together. See these topics:

- Scenario A: Public Subnet on page 2756
- Scenario B: Private Subnet with a VPN on page 2761
- Scenario C: Public and Private Subnets with a VPN on page 2769

Transit Routing

Scenarios A–C show your on-premises network connected to a VCN by way of FastConnect or VPN Connect, and accessing only the resources in that VCN.

The following advanced routing scenarios give your on-premises network additional access beyond the resources in the connected VCN. Traffic travels from your on-premises network to the VCN, and then transits through the VCN to its destination. See these topics:

- Transit Routing: Access to Multiple VCNs in the Same Region on page 2780: Your on-premises network has access to multiple VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect. The VCNs are in a hub-and-spoke topology, with the on-premises network connected to the VCN that acts as the hub. The spoke VCNs are peered with the hub VCN.
- Transit Routing: Private Access to Oracle Services on page 2803: Your on-premises network has private access to Oracle services in the Oracle Services Network by way of the connected VCN and the VCN's service gateway. The traffic does not go over the internet.

Regions and Availability Domains

Your VCN resides in a single Oracle Cloud Infrastructure region. Each subnet resides in a single availability domain (AD). Availability domains are designed to provide isolation and redundancy in your VCN, as illustrated in Scenario B and C earlier. For example, you could set up your primary set of subnets in a single AD, and then set up a duplicate set of subnets in a secondary AD. The two ADs are isolated from each other in the Oracle data centers, so if one fails, you can easily switch over to the other AD. For more information, see Regions and Availability Domains.

Public IP Address Ranges

For a list of Oracle Cloud Infrastructure public IP ranges, see IP Address Ranges on page 193.

IP Addresses Reserved for Use by Oracle

Certain IP addresses are reserved for Oracle Cloud Infrastructure use and may not be used in your address numbering scheme.

169.254.0.0/16

These addresses are used for iSCSI connections to the boot and block volumes, instance metadata, and other services.
**Class D and Class E**

All addresses from 224.0.0.0 to 239.255.255.255 (Class D) are prohibited for use in a VCN, they are reserved for multicast address assignments in the IP standards. See RFC 3171 for details.

All addresses from 240.0.0.0 to 255.255.255.255 (Class E) are prohibited for use in a VCN, they are reserved for future use in the IP standards. See RFC 1112, Section 4 for details.

**Three IP Addresses in Each Subnet**

These addresses consist of:

- The first IP address in the CIDR (the network address)
- The last IP address in the CIDR (the broadcast address)
- The first host address in the CIDR (the subnet default gateway address)

For example, in a subnet with CIDR 192.168.0.0/24, these addresses are reserved:

- 192.168.0.0 (the network address)
- 192.168.0.255 (the broadcast address)
- 192.168.0.1 (the subnet default gateway address)

The remaining addresses in the CIDR (192.168.0.2 to 192.168.0.254) are available for use.

**Creating Automation with Events**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

**Ways to Access Oracle Cloud Infrastructure**

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.
If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Limits on Your Networking Components**

See [Service Limits](#) on page 215 for a list of applicable limits and instructions for requesting a limit increase.

**Networking Scenarios**

Here are a few basic networking scenarios to help you understand the Networking service and generally how the components work together.

- [Scenario A: Public Subnet](#) on page 2756
- [Scenario B: Private Subnet with a VPN](#) on page 2761
- [Scenario C: Public and Private Subnets with a VPN](#) on page 2769

**Advanced Scenarios with Transit Routing Through a Single VCN**

Scenarios A–C show your on-premises network connected to a VCN by way of [FastConnect](#) or [VPN Connect](#), and accessing only the resources in that VCN.

The following advanced routing scenarios give your on-premises network additional access beyond the resources in the connected VCN. Traffic travels from your on-premises network to the VCN, and then *transits through* the VCN to its destination. See these topics:

- [Transit Routing: Access to Multiple VCNs in the Same Region](#) on page 2780: Your on-premises network has access to *multiple* VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect. The VCNs are in a hub-and-spoke topology, with the on-premises network connected to the VCN that acts as the hub. The spoke VCNs are peered with the hub VCN.
- [Transit Routing: Private Access to Oracle Services](#) on page 2803: Your on-premises network has *private access* to Oracle services in the Oracle Services Network by way of the connected VCN and the VCN's *service gateway*. The traffic does not go over the internet.

**Advanced Scenario with Multiple DRGs and Multiple VCNs**

There's an extra advanced scenario that illustrates the use of multiple VCNs. In this case, each VCN has its own *dynamic routing gateway (DRG)* and its own FastConnect *private virtual circuit*. Contrast this with [Transit Routing: Access to Multiple VCNs in the Same Region](#) on page 2780, in which there's a single DRG with either VPN Connect or a single FastConnect private virtual circuit.

Here are some restrictions for using the scenario that has multiple DRGs:

- The scenario works only with FastConnect through a *third-party provider* or through colocation with Oracle. It is not supported for FastConnect through an Oracle partner.
- The scenario is supported only for VCNs in the same region and same tenancy.

See [FastConnect with Multiple DRGs and VCNs](#) on page 2816.

**Scenario A: Public Subnet**

This topic explains how to set up Scenario A, which consists of a virtual cloud network (VCN) and a regional *public subnet*. There are public servers in separate *availability domains* for redundancy. The VCN is directly connected to the internet by way of an *internet gateway*. The gateway is also used for connectivity to your on-premises network. Any resource in the on-premises network that needs to communicate with resources in the VCN must have a public IP address and access to the internet.

The subnet uses the *default security list*, which has default rules that are designed to make it easy to get started with Oracle Cloud Infrastructure. The rules enable typical required access (for example, inbound SSH connections and any type of outbound connections). Remember that security list rules only *allow* traffic. Any traffic not explicitly covered by a security list rule is implicitly denied.
In this scenario, you add additional rules to the default security list. You could instead create a custom security list for those rules. You would then set up the subnet to use both the default security list and the custom security list.

**Tip:**

Security lists are one way to control traffic in and out of the VCN’s resources. You can also use network security groups, which let you apply a set of security rules to a set of resources that all have the same security posture.

The subnet uses the default route table, which starts out with no rules when the VCN is created. In this scenario, the table has only a single rule for the internet gateway.

See the following figure.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re a member of the Administrators group, you already have the required access to execute Scenario A. Otherwise, you need access to Networking, and you need the ability to launch instances. See IAM Policies for Networking on page 2832.

**Setting Up Scenario A in the Console**

Setup is easy in the Console.

**Task 1: Create the VCN**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.

3. Click Create Virtual Cloud Network.

4. Enter the following:
   - **Name**: A descriptive name for the VCN. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in Compartment**: Leave as is.
   - **CIDR Blocks**: One or more non-overlapping CIDR blocks for the VCN. For example: 172.16.0.0/16. You can add or remove CIDR blocks later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.
   - **Enable IPv6 Address Assignment**: This option is available only if the VCN is in the Government Cloud. For more information, see IPv6 Addresses on page 2889.
   - **Use DNS Hostnames in this VCN**: Required for assignment of DNS hostnames to hosts in the VCN, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the VCN (<VCN_DNS_label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Create Virtual Cloud Network.

The VCN is then created and displayed on the Virtual Cloud Networks page in the compartment you chose.

Task 2: Create the regional public subnet

1. While still viewing the VCN, click Create Subnet.

2. Enter the following:
   - **Name**: A friendly name for the subnet (for example, Regional Public Subnet). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Regional or Availability Domain-Specific**: Select Regional (recommended), which means the subnet spans all availability domains in the region. Later when you launch an instance, you can create it in any availability domain in the region. For more information, see Overview of VCNs and Subnets on page 2822.
   - **CIDR Block**: A single, contiguous CIDR block within the VCN's CIDR block. For example: 172.16.0.0/24. You cannot change this value later. For reference, here's a CIDR calculator.
   - **Enable IPv6 Address Assignment**: This option is available only if the VCN is in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.
   - **Route Table**: Select the default route table.
   - **Private or public subnet**: Select Public Subnet, which means instances in the subnet can optionally have public IP addresses. For more information, see Access to the Internet on page 2752.
   - **Use DNS Hostnames in this Subnet**: This option is available only if you provided a DNS label for the VCN during creation. The option is required for assignment of DNS hostnames to hosts in the subnet, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the subnet, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the subnet (<subnet_DNS_label>.<VCN_DNS_label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - **DHCP Options**: Select the default set of DHCP options.
   - **Security Lists**: Make sure the default security list is selected (the default).
   - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
3. Click Create Subnet.
   The subnet is then created and displayed on the Subnets page.

**Task 3: Create the internet gateway**

1. Under Resources, click Internet Gateways.
2. Click Create Internet Gateway.
3. Enter the following:
   - **Name:** A friendly name for the internet gateway. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in Compartment:** Leave as is.
   - **Tags:** Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
4. Click Create Internet Gateway.

Your internet gateway is created and displayed on the Internet Gateways page. It's already enabled, but you must add a route rule that allows traffic to flow to the gateway.

**Task 4: Update the default route table to use the internet gateway**

The default route table starts out with no rules. Here you add a rule that routes all traffic destined for addresses outside the VCN to the internet gateway. The existence of this rule also enables inbound connections to come from the internet to the subnet, through the internet gateway. You use security list rules to control the types of traffic that are allowed in and out of the instances in the subnet (see the next task).

No route rule is required in order to route traffic within the VCN itself.

1. Under Resources, click Route Tables.
2. Click the default route table to view its details.
3. Click Add Route Rule.
4. Enter the following:
   - **Target Type:** Internet Gateway
   - **Destination CIDR block:** 0.0.0.0/0 (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table goes to the target specified in this rule)
   - **Compartment:** The compartment where the internet gateway is located.
   - **Target:** The internet gateway you created.
   - **Description:** An optional description of the rule.
5. Click Add Route Rule.

The default route table now has a rule for the internet gateway. Because the subnet was set up to use the default route table, the resources in the subnet can now use the internet gateway. The next step is to specify the types of traffic you want to allow in and out of the instances you later create in the subnet.

**Task 5: Update the default security list**

Earlier you set up the subnet to use the VCN's default security list. Now you add security list rules that allow the types of connections that the instances in the VCN will need.

For example: This is a public subnet with an internet gateway, so the instances your launch might need to receive inbound HTTPS connections from the internet (if they're web servers). Here's how to add another rule to the default security list to enable that traffic:

2. Click the default security list to view its details. By default, you land on the Ingress Rules page.
3. Click Add Ingress Rule.
4. To enable inbound connections for HTTPS (TCP port 443), enter the following:
   - Stateless: Unselected (this is a stateful rule)
   - Source Type: CIDR
   - Source CIDR: 0.0.0.0/0
   - IP Protocol: TCP
   - Source Port Range: All
   - Destination Port Range: 443
   - Description: An optional description of the rule.

5. Click Add Ingress Rule.

**Important:**

Security List Rule for Windows Instances

If you're going to launch Windows instances, you need to add a security list rule to enable Remote Desktop Protocol (RDP) access. Specifically, you need a stateful ingress rule for TCP traffic on destination port 3389 from source 0.0.0.0/0 and any source port. For more information, see Security Lists on page 2850.

For a production VCN, you typically set up one or more custom security lists for each subnet. If you like, you can edit the subnet to use different security lists. If you choose not to use the default security list, do so only after carefully assessing which of its default rules you want to duplicate in your custom security list. For example: the default ICMP rules in the default security list are important for receiving connectivity messages.

**Task 6: Create instances in separate availability domains**

Your next step is to create one or more instances in the subnet. The scenario's diagram shows instances in two different availability domains. When you create the instance, you choose the AD, which VCN and subnet to use, and several other characteristics.

Each instance automatically gets a private IP address. When you create an instance in a public subnet, you choose whether the instance gets a public IP address. With this network setup in Scenario A, you must give each instance a public IP address, or else you can't access them through the internet gateway. The default (for a public subnet) is for the instance to get a public IP address.

After creating an instance in this scenario, you can connect to it over the internet with SSH or RDP from your on-premises network or other location on the internet. For more information and instructions, see Launching an Instance.

**Setting Up Scenario A with the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:

1. CreateVcn: Make sure to include a DNS label for the VCN if you want the instances to have hostnames (see DNS in Your Virtual Cloud Network on page 2910).
2. CreateSubnet: Create one regional public subnet. Include a DNS label for the subnet if you want the instances to have hostnames. Use the default route table, default security list, and default set of DHCP options.
3. CreateInternetGateway
4. UpdateRouteTable: To enable communication with the internet gateway, update the default route table to include a route rule with destination = 0.0.0.0/0, and destination target = the internet gateway. This rule routes all traffic destined for addresses outside the VCN to the internet gateway. No route rule is required in order to route traffic within the VCN itself.
5. UpdateSecurityList: To allow specific types of connections to and from the instances in the subnet.

**Important:**

Security List Rule for Windows Instances
If you're going to launch Windows instances, you need to add a security list rule to enable Remote Desktop Protocol (RDP) access. Specifically, you need a stateful ingress rule for TCP traffic on destination port 3389 from source 0.0.0.0/0 and any source port. For more information, see Security Lists on page 2850.

Your next step is to create one or more instances in the subnet. The scenario's diagram shows instances in two different availability domains. When you create the instance, you choose the AD, which VCN and subnet to use, and several other characteristics.

Each instance automatically gets a private IP address. When you create an instance in a public subnet, you choose whether the instance gets a public IP address. With this network setup in Scenario A, you must give each instance a public IP address, or else you can't access them through the internet gateway. The default (for a public subnet) is for the instance to get a public IP address.

After creating an instance in this scenario, you can connect to it over the internet with SSH or RDP from your on-premises network or other location on the internet. For more information and instructions, see Launching an Instance.

Scenario B: Private Subnet with a VPN

This topic explains how to set up Scenario B, which consists of a virtual cloud network (VCN) with a regional private subnet. There are servers in separate availability domains for redundancy. The VCN has a dynamic routing gateway (DRG) and IPSec VPN for connectivity to your on-premises network. The VCN has no direct connection to the internet. Any connection to the internet would need to come indirectly by way of the on-premises network.

The subnet uses the default security list, which has default rules that are designed to make it easy to get started with Oracle Cloud Infrastructure. The rules enable typical required access (for example, inbound SSH connections and any type of outbound connections). Remember that security list rules only allow traffic. Any traffic not explicitly covered by a security list rule is denied.

In this scenario, you add additional rules to the default security list. You could instead create a custom security list for those rules. You would then set up the subnet to use both the default security list and the custom security list.

Tip:

Security lists are one way to control traffic in and out of the VCN's resources. You can also use network security groups, which let you apply a set of security rules to a set of resources that all have the same security posture.

The subnet uses the default route table, which starts out with no rules when the VCN is created. In this scenario, the table has only a single rule for the DRG. No route rule is required in order to route traffic within the VCN itself.

See the following figure.
Tip:
The scenario uses an IPSec VPN for connectivity. However, you could instead use Oracle Cloud Infrastructure FastConnect.

Prerequisites
To set up the VPN in this scenario, you need to get the following information from a network administrator:

- Public IP address of the customer-premises equipment (CPE) at your end of the VPN
- Static routes for your on-premises network (this scenario uses static routing for the VPN tunnels, but you could instead use BGP dynamic routing)

You will provide Oracle this information and in return receive the information your network administrator must have to configure the CPE at your end of the VPN.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re a member of the Administrators group, you already have the required access to execute Scenario B. Otherwise, you need access to Networking, and you need the ability to launch instances. See IAM Policies for Networking on page 2832.
Setting Up Scenario B

Setup is easy in the Console. Alternatively, you can use the Oracle Cloud Infrastructure API, which lets you execute the individual operations yourself.

**Important:**

Most of this process involves working with the Console or API (whichever you choose) for a short period to set up the desired Networking components. But there's also a critical step that requires a network administrator in your organization to take information you receive from setting up the components and use it to configure the CPE at your end of the VPN. Therefore you can't complete this process in one short session. You'll need to break for an unknown period of time while the network administrator completes the configuration and then return afterward to confirm communication with your instances over the VPN.

Using the Console

**Task 1: Set up the VCN and subnet**

1. Create the VCN:
   
a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   
b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.
   
c. Click Create Virtual Cloud Network.
   
d. Enter the following:

   - **Name:** A descriptive name for the VCN. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in Compartment:** Leave as is.
   - **CIDR Block:** One or more non-overlapping CIDR blocks for the VCN. For example: 172.16.0.0/16. You can add or remove CIDR blocks later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.
   - **Enable IPv6 Address Assignment:** This option is available only if the VCN is in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.
   - **Use DNS Hostnames in this VCN:** Required for assignment of DNS hostnames to hosts in the VCN, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the VCN (<VCN DNS label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - **Tags:** Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   
e. Click Create Virtual Cloud Network.

The VCN is then created and displayed on the Virtual Cloud Networks page in the compartment you chose.
2. Create the regional private subnet:
   a. While still viewing the VCN, click **Create Subnet**.
   b. Enter the following:
      - **Name**: A friendly name for the subnet (for example, *Regional Private Subnet*). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **Regional or Availability Domain-Specific**: Select **Regional** (recommended), which means the subnet spans all availability domains in the region. Later when you launch an instance, you can create it any availability domain in the region. For more information, see *Overview of VCNs and Subnets* on page 2822.
      - **CIDR Block**: A single, contiguous CIDR block within the VCN's CIDR block. For example: 172.16.0.0/24. You cannot change this value later. For reference, here's a [CIDR calculator](#).
      - **Enable IPv6 Address Assignment**: This option is available only if the VCN is in the US Government Cloud. For more information, see *IPv6 Addresses* on page 2889.
      - **Route Table**: Select the default route table.
      - **Private or public subnet**: Select **Private Subnet**, which means instances in the subnet cannot have public IP addresses. For more information, see *Access to the Internet* on page 2752.
      - **Use DNS Hostnames in this Subnet**: This option is available only if you provided a DNS label for the VCN during creation. The option is required for assignment of DNS hostnames to hosts in the subnet, and required if you plan to use the VCN's default DNS feature (called the *Internet and VCN Resolver*). If the check box is selected, you can specify a DNS label for the subnet, or the Console will generate one for you. The dialog box automatically displays the corresponding **DNS Domain Name** for the subnet (<subnet_DNS_label>.<VCN_DNS_label>.oraclevcn.com). For more information, see *DNS in Your Virtual Cloud Network* on page 2910.
      - **DHCP Options**: Select the default set of DHCP options.
      - **Security Lists**: Select the default security list.
      - **Tags**: Leave as is. You can add tags later if you want. For more information, see *Resource Tags* on page 211.
   c. Click **Create Subnet**.

   The subnet is then created and displayed on the **Subnets** page.
3. Update the default security list to include rules to allow the types of connections that your instances in the VCN will need:

a. While still on the page displaying your VCN’s subnets, click Security Lists, and then click the default security list.

b. Under Resources, click either Ingress Rules or Egress Rules depending on the type of rule you want to work with. You can add one rule at a time by clicking either Add Ingress Rule or Add Egress Rule.

c. Add your desired rules. Here are suggested ones to add to the default ones already in the default security list:

Example: Ingress HTTP access

- **Type:** Ingress
- **Stateless:** Unselected (this is a stateful rule)
- **Source Type:** CIDR
- **Source CIDR:** 0.0.0.0/0
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 80
- **Description:** An optional description of the rule.

Example: Ingress HTTPS access

- **Type:** Ingress
- **Stateless:** Unselected (this is a stateful rule)
- **Source Type:** CIDR
- **Source CIDR:** 0.0.0.0/0
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 443
- **Description:** An optional description of the rule.

Example: Ingress SQL*Net access for Oracle databases

- **Type:** Ingress
- **Stateless:** Unselected (this is a stateful rule)
- **Source Type:** CIDR
- **Source CIDR:** 0.0.0.0/0
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 1521
- **Description:** An optional description of the rule.

Example: Ingress RDP access required for Windows instances

- **Type:** Ingress
- **Stateless:** Unselected (this is a stateful rule)
- **Source Type:** CIDR
- **Source CIDR:** 0.0.0.0/0
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 3389
- **Description:** An optional description of the rule.

**Tip:**

For additional security, you could modify all the stateful ingress rules to allow traffic only from within your VCN and your on-premises network. You
Networking

Networking would need to create separate rules for each, one with the VCN's CIDR as the source, and one with the on-premises network's CIDR as the source.

For a production VCN, you typically set up one or more custom security lists for each subnet. You can edit the subnet to use different security lists if you like. If you choose not to use the default security list, do so only after carefully assessing which of its default rules you want to duplicate in your custom security list. For example: the default ICMP rules in the default security list are important for receiving connectivity messages.

**Task 2: Create instances in separate availability domains**

You can now create one or more instances in the subnet (see Launching an Instance). The scenario's diagram shows instances in two different availability domains. When you create the instance, you choose the AD, which VCN and subnet to use, and several other characteristics.

However, you can't yet communicate with the instances because there's no gateway connecting the VCN to your on-premises network. The next procedure walks you through creating an IPSec VPN connection to enable that communication.

**Task 3: Add an IPSec VPN to your VCN**

1. Create a customer-premises equipment (CPE) object:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Customer-Premsises Equipment.
   b. Click Create Customer-Premsises Equipment.
   c. Enter the following:
      - **Create in Compartment**: Leave the default value (the compartment you're currently working in).
      - **Name**: A friendly name for the customer-premises equipment object. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **IP Address**: The public IP address of the CPE at your end of the VPN (see Prerequisites on page 2762).
   d. Click Create.

   The CPE object will be in the "Provisioning" state for a short period.

2. Create a dynamic routing gateway (DRG):
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Dynamic Routing Gateways.
   b. Click Create Dynamic Routing Gateway.
   c. For Create in Compartment: Leave the default value (the compartment you're currently working in).
   d. Enter a friendly name for the DRG. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   e. Click Create.

   The DRG will be in the "Provisioning" state for a short period. Make sure it is done being provisioned before continuing.

3. Attach the DRG to your VCN:
   a. Click the DRG that you just created.
   b. Under Resources, click Virtual Cloud Networks.
   c. Click Attach to Virtual Cloud Network.
   d. Select the VCN. Ignore the section for advanced options, which is only for an advanced routing scenario called transit routing, which is not relevant here.
   e. Click Attach.

   The attachment will be in the "Attaching" state for a short period before it's ready.
4. Update the default route table (which has no rules yet):
   
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
   b. Click your VCN.
   c. Under **Resources**, click **Route Tables**, and then click the default route table.
   d. Click **Add Route Rule**.
   e. Enter the following:
      
      - **Target Type**: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      - **Destination CIDR Block**: 0.0.0.0/0 (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table will go to the target specified in this rule).
      - **Description**: An optional description of the rule.
   
   f. Click **Add Route Rule**.
      
      The VCN's default route table now directs outbound traffic to the DRG and ultimately to your on-premises network.

5. Create an IPSec Connection:
   
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **VPN Connections**.
   b. Click **Create IPSec Connection**.
   c. Enter the following:
      
      - **Create in Compartment**: Leave the default value (the compartment you're currently working in).
      - **Name**: Enter a friendly name for the IPSec connection. It doesn't have to be unique. Avoid entering confidential information.
      - **Customer-Premises Equipment Compartment**: Leave as is (the VCN's compartment).
      - **Customer-Premises Equipment**: Select the CPE object you created earlier.
      - **Dynamic Routing Gateway Compartment**: Leave as is (the VCN's compartment).
      - **Dynamic Routing Gateway**: Select the DRG that you created earlier.
      - **Static Route CIDR**: Enter at least one static route CIDR (see Prerequisites on page 2762). If you need to add another, click **Add Static Route**. You can enter up to 10 static routes, and you can change the static routes later if you like.
   
   d. Click **Show Advanced Options** and optionally provide the following items:
      
      - **CPE IKE Identifier**: Oracle defaults to using the public IP address of the CPE. But if your CPE is behind a NAT device, you might need to enter a different value. You can either enter the new value here, or change the value later.
      - **Tunnel 1** and **Tunnel 2**: Leave as is. Later if you want to use BGP dynamic routing instead of static routing for the VPN tunnels, see Changing from Static Routing to BGP Dynamic Routing on page 3160.
      - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   
   e. Click **Create IPSec Connection**.
      
      The IPSec connection is created and displayed on the page. It will be in the Provisioning state for a short period.
      
      The displayed tunnel information includes the IP address of the VPN headend and the tunnel's IPSec status (possible values are Up, Down, and Down for Maintenance). At this point, the status is Down. To view the tunnel's shared secret, click the Actions icon (three dots), and then click **View Shared Secret**.
   
   f. Copy the Oracle VPN IP address and shared secret for each of the tunnels to an email or other location so you can deliver it to the network engineer who will configure the on-premises router.
      
      For more information, see CPE Configuration on page 2967. You can view this tunnel information here in the Console at any time.
You have now created all the components required for the IPSec VPN. But your network administrator must configure the CPE before network traffic can flow between your on-premises network and VCN.

**Task 4: Configure your CPE**

These instructions are for the network administrator.

1. Make sure you have the tunnel configuration information that Oracle provided during IPSec VPN setup. See **Task 3: Add an IPSec VPN to your VCN** on page 2766.
2. Configure your CPE according to the information in **CPE Configuration** on page 2967.

If there are already instances in the subnet, you can confirm the IPSec connection is up and running by connecting to the instances from your on-premises network.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the following operations:

1. **CreateVcn**: Make sure to include a DNS label for the VCN if you want the instances to have hostnames (see **DNS in Your Virtual Cloud Network** on page 2910).
2. **CreateSubnet**: Create one regional private subnet. Include a DNS label for the subnet if you want the instances to have hostnames. Use the default route table, default security list, and default set of DHCP options.
3. **CreateDrg**: This creates a new dynamic routing gateway (DRG)
4. **CreateDrgAttachment**: This attaches the DRG to the VCN.
5. **CreateCpe**: Here you'll provide the public IP address of the CPE at your end of the VPN (see **Prerequisites** on page 2762).
6. **CreateIPSecConnection**: Here you'll provide the static routes for your on-premises network (see **Prerequisites** on page 2762). In return, you'll receive the configuration information that your network administrator needs in order to configure your CPE. If you need that information later, you can get it with **GetIPSecConnectionDeviceConfig**. For more information about the configuration, see **CPE Configuration** on page 2967.
7. **UpdateRouteTable**: To enable communication via the VPN, update the default route table to include this route: a route rule with destination = 0.0.0.0/0, and destination target = the DRG you created earlier.
8. First call **GetSecurityList** to get the default security list, and then call **UpdateSecurityList** to add rules for the types of connections that your instances in the VCN will need. Be aware that **UpdateSecurityList** overwrites the entire set of rules. Here are some suggested rules to add:

   - **Stateful ingress**: Source type=CIDR, source CIDR=0.0.0.0/0, protocol=TCP, source port = all, destination port=80 (for HTTP).
   - **Stateful ingress**: Source type=CIDR, source CIDR=0.0.0.0/0, protocol=TCP, source port = all, destination port=443 (for HTTPS).
   - **Stateful ingress**: Source type=CIDR, source CIDR=0.0.0.0/0, protocol=TCP, source port = all, destination port=1521 (for SQL*Net access to Oracle databases).
   - **Stateful ingress**: Source type=CIDR, source CIDR=0.0.0.0/0, protocol=TCP, source port=all, destination port=3389 (for RDP; required only if using Windows instances).
9. **LaunchInstance**: Create one or more instances in the subnet. The scenario's diagram shows instances in two different availability domains. When you create the instance, you choose the AD, which VCN and subnet to use, and several other characteristics. For more information, see **Creating an Instance** on page 695.

**Tip:**

For additional security, you could modify all the stateful ingress rules to allow traffic only from within your VCN and your on-premises network. You would need to create separate rules for each, one with the VCN's CIDR as the source, and one with the on-premises network's CIDR as the source.
Important:

Although you can create instances in the subnet, you won't be able to communicate with them from your on-premises network until your network administrator configures your CPE (see CPE Configuration on page 2967). After that, your IPSec connection should be up and running. You can confirm its status by using GetIPSecConnectionDeviceStatus. You can also confirm the IPSec connection is up by connecting to the instances from your on-premises network.

Scenario C: Public and Private Subnets with a VPN

This topic explains how to set up Scenario C, which is a simple example of a multi-tier setup. It consists of a virtual cloud network (VCN) with a regional public subnet to hold public servers (such as web servers), and a regional private subnet to hold private servers (such as database servers). There are servers in separate availability domains for redundancy.

The VCN has a dynamic routing gateway (DRG) and IPSec VPN for connectivity to your on-premises network. Instances in the public subnet have direct access to the internet by way of an internet gateway. Instances in the private subnet can initiate connections to the internet by way of a NAT gateway (for example, to get software updates), but cannot receive inbound connections from the internet through that gateway.

Each subnet uses the default security list, which has default rules that are designed to make it easy to get started with Oracle Cloud Infrastructure. The rules enable typical required access (for example, inbound SSH connections and any type of outbound connections). Remember that security list rules only allow traffic. Any traffic not explicitly covered by a security list rule is denied.

Tip:

Security lists are one way to control traffic in and out of the VCN's resources. You can also use network security groups, which let you apply a set of security rules to a set of resources that all have the same security posture.

Each subnet also has its own custom security list and custom route table with rules specific to the needs of the subnet's instances. In this scenario, the VCN's default route table (which is always empty to start with) is not used.

See the following figure.
Networking

Tip:
The scenario uses an IPSec VPN for connectivity. However, you could instead use Oracle Cloud Infrastructure FastConnect.

Prerequisites
To set up the VPN in this scenario, you need to get the following information from a network administrator:

- Public IP address of the customer-premises equipment (CPE) at your end of the VPN
- Static routes for your on-premises network (this scenario uses static routing for the VPN tunnels, but you could instead use BGP dynamic routing)

You will provide Oracle this information and in return receive the information your network administrator needs in order to configure the on-premises router at your end of the VPN.

Required IAM Policy
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're a member of the Administrators group, you already have the required access to execute Scenario C. Otherwise, you need access to Networking, and you need the ability to launch instances. See IAM Policies for Networking on page 2832.

Setting Up Scenario C
Setup is easy in the Console. Alternatively, you can use the Oracle Cloud Infrastructure API, which lets you execute the individual operations yourself.

Important:
Most of this process involves working with the Console or API (whichever you choose) for a short period to set up the desired Networking components. But there's also a critical step that requires a network administrator in your organization to take information you receive from setting up the components and use it to configure the on-premises router at your end of the VPN. Therefore you can't complete this process in one short session. You'll need to break for an unknown period of time while the network administrator completes the configuration and then return afterward to confirm communication with your instances over the VPN.

Using the Console
Task 1: Set up the VCN and subnets

1. Create the VCN:
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
   b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.
   c. Click **Create Virtual Cloud Network**.
   d. Enter the following:
      - **Name**: A friendly name for the VCN. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **Create in Compartment**: Leave as is.
      - **CIDR Block**: One or more non-overlapping CIDR blocks for the VCN. For example: 172.16.0.0/16. You can add or remove CIDR blocks later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a [CIDR calculator](#).
      - **Enable IPv6 Address Assignment**: This option is available only if the VCN is in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.
      - **Use DNS Hostnames in this VCN**: Required for assignment of DNS hostnames to hosts in the VCN, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding **DNS Domain Name** for the VCN (<VCN DNS label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
      - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   e. Click **Create Virtual Cloud Network**.

   The VCN is then created and displayed on the **Virtual Cloud Networks** page in the compartment you chose.

2. Create an internet gateway for your VCN:
   a. Under **Resources**, click **Internet Gateways**.
   b. Click **Create Internet Gateway**.
   c. Enter the following:
      - **Name**: A friendly name for the internet gateway. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **Create in Compartment**: Leave as is.
      - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   d. Click **Create Internet Gateway**.

   The internet gateway is then created and listed on the page.
3. Create a NAT gateway for your VCN:
   a. Under Resources, click NAT Gateways.
   b. Click Create NAT Gateway.
   c. Enter the following:
      • Name: A friendly name for the NAT gateway. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      • Create in Compartment: Leave as is.
      • Tags: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   d. Click Create NAT Gateway.

   The NAT gateway is then created and listed on the page.

4. Create the custom route table for the public subnet (which you will create later):
   a. Under Resources, click Route Tables.
   b. Click Create Route Table.
   c. Enter the following:
      • Name: A friendly name for the route table (for example, Public Subnet Route Table). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      • Create in Compartment: Leave the default value (the compartment you're currently working in).
      • Click + Additional Route Rule and enter the following:
         • Target Type: Internet Gateway.
         • Destination CIDR Block: 0.0.0.0/0 (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table will go to the target specified in this rule).
         • Compartment: Leave as is.
         • Target: The internet gateway you just created.
         • Description: An optional description of the rule.
   d. Tags: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   e. Click Create Route Table.

   The route table is then created and listed on the page.
5. Create the custom route table for the private subnet (which you will create later):
   a. Click Create Route Table.
   b. Enter the following:
      - **Name**: A friendly name for the route table (for example, *Private Subnet Route Table*). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **Create in Compartment**: Leave the default value (the compartment you're currently working in).
      - **Click + Additional Route Rule** and enter the following:
        - **Target Type**: NAT Gateway.
        - **Destination CIDR Block**: 0.0.0.0/0 (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table will go to the target specified in this rule).
        - **Compartment**: Leave as is.
        - **Target**: The NAT gateway you just created.
        - **Description**: An optional description of the rule.
      c. **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
      d. Click Create Route Table.

   The route table is then created and listed on the page. Later on after you've set up the IPSec VPN, you will update the Private Subnet Route Table so it routes traffic from the private subnet to the on-premises network by way of the DRG.

6. Update the **default security list** to include rules to allow the types of connections that your instances in the VCN will need:
   b. Click the default security list to view its details. By default, you land on the Ingress Rules page.
   c. Edit each of the existing stateful ingress rules so that the **Source CIDR** is the CIDR for your on-premises network (10.0.0.0/16 in this example) and not 0.0.0.0/0. To edit an existing rule, click the Actions icon (three dots) for the rule, and then click **Edit**.
   d. If you plan to launch Windows instances, add a rule to enable RDP access:
7. Create a custom security list for the public subnet:

   a. Return to the Security Lists page for the VCN.
   b. Click Create Security List.
   c. Enter the following:
      
      • **Name:** Enter a friendly name for the list (for example, *Public Subnet Security List*). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      
      • **Create in Compartment:** Leave the default value (the compartment you're currently working in).

d. Add the following ingress rules:

   Example: Ingress HTTP access

   • **Type:** Ingress
   • **Stateless:** Unselected (this is a *stateful rule*)
   • **Source Type:** CIDR
   • **Source CIDR:** 0.0.0.0/0
   • **IP Protocol:** TCP
   • **Source Port Range:** All
   • **Destination Port Range:** 80
   • **Description:** An optional description of the rule.

   Example: Ingress HTTPS access

   • **Type:** Ingress
   • **Stateless:** Unselected (this is a *stateful rule*)
   • **Source Type:** CIDR
   • **Source CIDR:** 0.0.0.0/0
   • **IP Protocol:** TCP
   • **Source Port Range:** All
   • **Destination Port Range:** 443
   • **Description:** An optional description of the rule.

e. Add the following egress rule:

   f. Click Create Security List.

   The custom security list for the public subnet is then created and listed on the page.
8. Create a custom security list for the *private* subnet:
   a. Click **Create Security List**.
   b. Enter the following:
      - **Name**: Enter a friendly name for the list (for example, *Private Subnet Security List*). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **Create in Compartment**: Leave the default value (the compartment you're currently working in).
   c. Add the following ingress rules:
      - Example: Ingress SQL*Net access from clients in the public subnet
         - **Type**: Ingress
         - **Stateless**: Unselected (this is a *stateful rule*)
         - **Source Type**: CIDR
         - **Source CIDR**: CIDR for the public subnet (172.16.2.0/24 in this example)
         - **IP Protocol**: TCP
         - **Source Port Range**: All
         - **Destination Port Range**: 1521
         - **Description**: An optional description of the rule.
      - Example: Ingress SQL*Net access from clients in the private subnet
         - **Type**: Ingress
         - **Stateless**: Unselected (this is a *stateful rule*)
         - **Source Type**: CIDR
         - **Source CIDR**: CIDR for the private subnet (172.16.2.1/24 in this example)
         - **IP Protocol**: TCP
         - **Source Port Range**: All
         - **Destination Port Range**: 1521
         - **Description**: An optional description of the rule.
   d. Add the following egress rules:
   e. Click **Create Security List**.
      - The custom security list for the private subnet is then created and listed on the page.

9. Create the subnets in the VCN:
   a. Under **Resources**, click **Subnets**.
   b. Click **Create Subnet**.
   c. Enter the following:
      - **Name**: A friendly name for the regional public subnet (for example, *Regional Private Subnet*). It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      - **Regional or Availability Domain-Specific**: Select **Regional** (recommended), which means the subnet spans all availability domains in the region. Later when you launch an instance, you can create it any
Networking

availability domain in the region. For more information, see Overview of VCNs and Subnets on page 2822.

- **CIDR Block:** A single, contiguous CIDR block within the VCN's CIDR block. For example: 172.16.1.0/24. You cannot change this value later. For reference, here's a CIDR calculator.
- **Enable IPv6 Address Assignment:** This option is available only if the VCN is in the US Government Cloud. For more information, see **IPv6 Addresses** on page 2889.
- **Route Table:** Select the Private Subnet Route Table you created earlier.
- **Private or public subnet:** Select **Private Subnet**, which means VNICs in the subnet are not allowed to have public IP addresses. For more information, see Access to the Internet on page 2752.
- **Use DNS Hostnames in this Subnet:** This option is available only if you provided a DNS label for the VCN during creation. The option is required for assignment of DNS hostnames to hosts in the subnet, and required if you plan to use the VCN's default DNS feature (called the **Internet and VCN Resolver**). If the check box is selected, you can specify a DNS label for the subnet, or the Console will generate one for you. The dialog box automatically displays the corresponding **DNS Domain Name** for the subnet (<subnet_DNS_label>.<VCN_DNS_label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
- **DHCP Options:** Select the default set of DHCP options.
- **Security Lists:** Select two security lists: Both the default security list and the Private Subnet Security List you created earlier.

d. Click **Create Subnet**.

The private subnet is then created and displayed on the **Subnets** page.

e. Repeat the preceding steps a-d to create the **regional public subnet**. Instead use a name such as **Regional Public Subnet**, select **Public Subnet** instead of **Private Subnet**, use the Public Subnet Route Table, and use both the default security list and Public Subnet Security List you created earlier.

Example: Ingress RDP access required for Windows instances

- **Type:** Ingress
- **Stateless:** Unselected (this is a **stateful rule**)
- **Source Type:** CIDR
- **Source CIDR:** Your on-premises network (10.0.0.0/16 in this example)
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 3389
- **Description:** An optional description of the rule.

Example: Egress SQL*Net access to Oracle databases

- **Type:** Egress
- **Stateless:** Unselected (this is a **stateful rule**)
- **Destination Type:** CIDR
- **Destination CIDR:** CIDR for the private subnet (172.16.1.0/24 in this example)
- **IP Protocol:** TCP
- **Source Port Range:** All
- **Destination Port Range:** 1521
- **Description:** An optional description of the rule.

Example: Egress SQL*Net access to instances in the private subnet

- **Type:** Egress
- **Stateless:** Unselected (this is a **stateful rule**)
- **Destination Type:** CIDR
- **Destination CIDR:** CIDR for the private subnet (172.16.1.0/24 in this example)
- **IP Protocol:** TCP
- **Source Port Range:** All
• **Destination Port Range:** 1521
• **Description:** An optional description of the rule.

**Task 2: Create instances in separate availability domains**

You can now create one or more instances in the subnet (see Launching an Instance). The scenario's diagram shows instances in two different availability domains. When you create the instance, you choose the AD, which VCN and subnet to use, and several other characteristics.

For each instance in the public subnet, make sure to assign the instance a public IP address. Otherwise, you won't be able to reach the instance from your on-premises network.

You can't yet reach the instances in the private subnet because there's no gateway connecting the VCN to your on-premises network. The next procedure walks you through creating an IPSec VPN connection to enable that communication.

**Task 3: Add an IPSec VPN to your VCN**

1. Create a customer-premises equipment object:
   
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Customer-Premises Equipment**.
   
   b. Click **Create Customer-Premises Equipment**.
   
   c. Enter the following:
      
      - **Create in Compartment:** Leave the default value (the compartment you're currently working in).
      
      - **Name:** A friendly name for the customer-premises equipment object. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      
      - **IP Address:** The IP address of the on-premises router at your end of the VPN (see Prerequisites on page 2770).
   
   d. Click **Create**.

   The CPE object is in the "Provisioning" state for a short period.

2. Create a dynamic routing gateway (DRG):

   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.

   b. Click **Create Dynamic Routing Gateway**.

   c. For **Create in Compartment:** Leave the default value (the compartment you're currently working in).

   d. Enter a friendly name for the DRG. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

   e. Click **Create**.

   The DRG will be in the "Provisioning" state for a short period. Make sure it is done being provisioned before continuing.

3. Attach the DRG to your VCN:

   a. Click the DRG that you just created.

   b. Under **Resources**, click **Virtual Cloud Networks**.

   c. Click **Attach to Virtual Cloud Network**.

   d. Select the VCN. Ignore the section for advanced options, which is only for an advanced routing scenario called *transit routing*, which is not relevant here.

   e. Click **Attach**.

   The attachment will be in the "Attaching" state for a short period before it's ready.
4. Update the private subnet's route table (which already has one rule for the NAT gateway):
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click your VCN.
   c. Click Route Tables, and then click the Private Subnet Route Table you created earlier.
   d. Click Add Route Rule.
   e. Enter the following:
      - **Target Type**: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      - **Destination CIDR Block**: 0.0.0.0/0 (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table will go to the target specified in this rule).
      - **Description**: An optional description of the rule.
   f. Click Add Route Rule.
      The table is updated to route any traffic destined for your on-premises network to the DRG. The original rule for 0.0.0.0/0 routes any remaining traffic leaving the subnet to the NAT gateway.

5. Create an IPSec Connection:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.
   b. Click Create IPSec Connection.
   c. Enter the following:
      - **Create in Compartment**: Leave the default value (the compartment you're currently working in).
      - **Name**: Enter a friendly name for the IPSec connection. It doesn't have to be unique. Avoid entering confidential information.
      - **Customer-Premises Equipment Compartment**: Leave as is (the VCN's compartment).
      - **Customer-Premises Equipment**: Select the CPE object you created earlier.
      - **Dynamic Routing Gateway Compartment**: Leave as is (the VCN's compartment).
      - **Dynamic Routing Gateway**: Select the DRG that you created earlier.
      - **Static Route CIDR**: Enter at least one static route CIDR (see Prerequisites on page 2770). If you need to add another, click Add Static Route. You can enter up to 10 static routes, and you can change the static routes later if you like.
   d. Click Show Advanced Options and optionally provide the following items:
      - **CPE IKE Identifier**: Oracle defaults to using the public IP address of the CPE. But if your CPE is behind a NAT device, you might need to enter a different value. You can either enter the new value here, or change the value later.
      - **Tunnel 1** and **Tunnel 2**: Leave as is. Later if you want to use BGP dynamic routing instead of static routing for the VPN tunnels, see Changing from Static Routing to BGP Dynamic Routing on page 3160.
      - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
   e. Click Create IPSec Connection.
      The IPSec connection is created and displayed on the page. It will be in the Provisioning state for a short period.
      The displayed tunnel information includes the IP address of the VPN headend and the tunnel's IPSec status (possible values are Up, Down, and Down for Maintenance). At this point, the status is Down. To view the tunnel's shared secret, click the Actions icon (three dots), and then click View Shared Secret.
   f. Copy the Oracle VPN IP address and shared secret for each of the tunnels to an email or other location so you can deliver it to the network engineer who will configure the on-premises router.
      For more information, see CPE Configuration on page 2967. You can view this tunnel information here in the Console at any time.
You have now created all the components required for the IPSec VPN. But your network administrator must configure the on-premises router before network traffic can flow between your on-premises network and VCN.

**Task 4: Configure your on-premises router (CPE)**

These instructions are for the network administrator.

1. Make sure you have the tunnel configuration information that Oracle provided during VPN setup. See Task 3: Add an IPSec VPN to your VCN on page 2777.
2. Configure your on-premises router according to the information in CPE Configuration on page 2967.

If there are already instances in one of the subnets, you can confirm the IPSec connection is up and running by connecting to the instances from your on-premises network. To connect to instances in the public subnet, you must connect to the instance’s public IP address.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:

1. **CreateVcn**: Make sure to include a DNS label if you want the VCN to use the VCN Resolver (see DNS in Your Virtual Cloud Network on page 2910).
2. **CreateInternetGateway**
3. **CreateNatGateway**
4. **CreateRouteTable**: Call it to create the Public Subnet Route Table. To enable communication by way of the internet gateway, add a route rule with destination = 0.0.0.0/0, and destination target = the internet gateway you created earlier.
5. **CreateRouteTable**: Call it again to create the Private Subnet Route Table. To enable communication by way of the NAT gateway, add a route rule with destination = 0.0.0.0/0, and destination target = the NAT gateway you created earlier.
6. First call **GetSecurityList** to get the default security list, and then call **UpdateSecurityList**:
   - Change the existing stateful ingress rules to use your on-premises network’s CIDR as the source CIDR, instead of 0.0.0.0/0.
   - If you plan to launch Windows instances, add this stateful ingress rule: Source type = CIDR, source CIDR = your on-premises network on TCP, source port = all, destination port = 3389 (for RDP).
7. **CreateSecurityList**: Call it to create the Public Subnet Security List with these rules:
   - Stateful ingress: Source type = CIDR, source 0.0.0.0/0 on TCP, source port = all, destination port = 80 (HTTP)
   - Stateful ingress: Source type = CIDR, source 0.0.0.0/0 on TCP, source port = all, destination port = 443 (HTTPS)
   - Stateful egress: Destination type = CIDR, destination CIDR blocks of private subnets on TCP, source port = all, destination port = 1521 (for Oracle databases)
8. **CreateSecurityList**: Call it again to create the Private Subnet Security List with these rules:
   - Stateful ingress: Source type = CIDR, source CIDR blocks of public subnets on TCP, source port = all, destination port = 1521 (for Oracle databases)
   - Stateful ingress: Source type = CIDR, source CIDR blocks of private subnets on TCP, source port = all, destination port = 1521 (for Oracle databases)
   - Stateful egress: Destination type = CIDR, destination CIDR blocks of private subnets on TCP, source port = all, destination port = 1521 (for Oracle databases)
9. **CreateSubnet**: Call it to create regional public subnet. Include a DNS label for the subnet if you want the VCN Resolver to resolve hostnames for VNICs in the subnet. Use the Public Subnet Route Table you created earlier. Use both the default security list and the Public Subnet Security List that you created earlier. Use the default set of DHCP options.
10. **CreateSubnet**: Call it again to create regional private subnet. Include a DNS label for the subnet if you want the VCN Resolver to resolve hostnames for VNICs in the subnet. Use the Private Subnet Route Table you created
11. **CreateDrg**: This creates a new dynamic routing gateway (DRG).

12. **CreateDrgAttachment**: This attaches the DRG to the VCN.

13. **CreateCpe**: Here you provide the IP address of the router at your end of the VPN (see Prerequisites on page 2770).

14. **CreateIPSecConnection**: Here you provide the static routes for your on-premises network (see Prerequisites on page 2770). In return, you receive the configuration information your network administrator needs in order to configure your router. If you need that information later, you can get it with `GetIPSecConnectionDeviceConfig`. For more information about the configuration, see CPE Configuration on page 2967.

15. First call `GetRouteTable` to get the Private Subnet Route Table. Then call `UpdateRouteTable` to add a route rule with destination = the on-premises network CIDR (10.0.0.0/16 in this example), and destination target = the DRG you created earlier.

16. **LaunchInstance**: Launch at least one instance in each subnet. By default, the instances in the public subnets are assigned public IP addresses. For more information, see Creating an Instance on page 695.

You can now communicate from your on-premises network with the instances in the public subnet over the internet gateway.

---

**Important:**

Although you can launch instances into the private subnets, you can't communicate with them from your on-premises network until your network administrator configures your on-premises router (see CPE Configuration on page 2967). After that, your IPSec connection should be up and running. You can confirm its status by using `GetIPSecConnectionDeviceStatus`. You can also confirm the IPSec connection is up by connecting to the instances from your on-premises network.

---

**Transit Routing: Access to Multiple VCNs in the Same Region**

Transit routing refers to a network topology in which your on-premises network uses a connected virtual cloud network (VCN) to reach Oracle resources or services beyond that VCN. You connect the on-premises network to the VCN with FastConnect or VPN Connect, and then configure the VCN routing so that traffic transits through the VCN to its destination beyond the VCN.

There are two primary transit routing scenarios:

- **Access to multiple VCNs in the same region**: The scenario covered in this topic. This scenario enables communication between your on-premises network and multiple VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect.
- **Private access to Oracle services**: This scenario gives your on-premises network private access to Oracle services, so that your on-premises hosts can use their private IP addresses and the traffic does not go over the internet. See Transit Routing: Private Access to Oracle Services on page 2803.

**Highlights**

- You can use a single FastConnect or IPSec VPN to connect your on-premises network with multiple VCNs in the same region, in a hub-and-spoke topology.
- The VCNs must be in the same region but can be in different tenancies. For accurate routing, the CIDR blocks of the various subnets of interest in the on-premises network and VCNs must not overlap.
- The VCN that acts as the hub uses a dynamic routing gateway (DRG) to communicate with the on-premises network. This hub VCN peers with each VCN that is acting as a spoke (referred to as spoke VCNs in this topic). The hub and spoke VCNs use local peering gateways (LPGs) to communicate.
- To enable the desired traffic from the on-premises network through the hub VCN to a peered spoke VCN, you implement route rules for the hub VCN’s DRG attachment and LPG, and for the spoke VCN’s subnets.
- If you like, you can set up transit routing through a private IP in the hub VCN. For example, you might want to filter or inspect the traffic between the on-premises network and a spoke VCN. In that case, you route the traffic...
Networking

to a private IP on an instance in the hub VCN for inspection, and the resulting traffic continues to its destination. This topic covers both situations: transit routing directly between gateways on the hub VCN, and transit routing through a private IP.

- By configuring route tables that reside in the hub VCN, you can control whether a particular subnet in a peered spoke VCN is advertised to the on-premises network, and whether a particular subnet in the on-premises network is advertised to a peered spoke VCN.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip: There's another scenario that lets you connect your on-premises network to multiple VCNs. Instead of using a single DRG and hub-and-spoke topology, you set up a separate DRG for each VCN and a separate private virtual circuit over a single FastConnect. However, the scenario can be used only with FastConnect through a third-party provider or through colocated with Oracle. The VCNs must be in the same region and same tenancy. For more information, see FastConnect with Multiple DRGs and VCNs on page 2816.</td>
</tr>
</tbody>
</table>

Overview of Transit Routing

A basic networking scenario involves connecting your on-premises network to a VCN with either Oracle Cloud Infrastructure FastConnect or an IPSec VPN. These two basic scenarios illustrate that topology: Scenario B: Private Subnet with a VPN on page 2761 and Scenario C: Public and Private Subnets with a VPN on page 2769.

There's an advanced networking scenario that lets you use your single FastConnect or IPSec VPN to communicate with multiple VCNs from your on-premises network. The VCNs must be in the same region but can be in different tenancies.

Here's a basic example of why you might use transit routing: you have a large organization with different departments, each with their own VCN. Your on-premises network needs access to the different VCNs, but you don't want the administration overhead of maintaining a secure connection from each VCN to the on-premises network. Instead you want to use a single FastConnect or IPSec VPN.

The scenario uses a hub-and-spoke topology, as illustrated in the following diagram. The term hub VCN here means only that a VCN is acting as the hub in this hub-and-spoke design.
One of the VCNs acts as the hub (VCN-H) and connects to your on-premises network by way of FastConnect or an IPSec VPN. The other VCNs are locally peered with the hub VCN. The traffic between the on-premises network and the peered VCNs transits through the hub VCN. The VCNs must be in the same region but can be in different tenancies.

**Gateways Involved in Transit Routing**

The next diagram shows the gateways on the VCNs. The hub VCN has a dynamic routing gateway (DRG), which is the communication path with the on-premises network. For each locally peered spoke VCN, there’s a pair of local peering gateways (LPGs) that anchor the peering connection. One LPG is on the hub VCN, and the other is on the spoke VCN.
Networking

Transit Routing Through a Private IP in the Hub VCN

If you want, you can route all the traffic through a private IP on an instance in the hub VCN. For example, you could set up a firewall or intrusion detection system on the instance in the hub VCN to filter or inspect the traffic between the on-premises network and spoke VCNs. Then you would configure the hub VCN’s routing so that the transit traffic is routed to a private IP on that instance. You must disable the source/destination check for the private IP’s VNIC. The resulting traffic would then travel on to its destination in either the spoke VCN or on-premises network. The following diagram illustrates the idea. Regardless of whether you choose to route through a private IP or not, the same gateways are required. However, you configure the hub VCN’s routing a little differently.
If you're already familiar with the Networking service and local VCN peering, these are the most important new concepts to understand:

- For each spoke VCN subnet that needs to communicate with the on-premises network, you must update the subnet's route table with a rule that sets the target (the next hop) as the spoke VCN's LPG for all traffic destined for the on-premises network.

- You must add a route table to the hub VCN, associate it with the DRG attachment, and add a route rule with a target that depends on your situation:
  - **Transit routing directly through gateways:** Set the target (the next hop) to the hub VCN's LPG (for that spoke) for all traffic destined for that spoke VCN (or a specific subnet in that VCN).
  - **Transit routing through a private IP:** Set the target (the next hop) to a private IP on the instance, for all traffic destined for that spoke VCN (or a specific subnet in that VCN). Make sure to disable the source/destination check for the private IP's VNIC.

---

**Legend:**
- **dynamic routing gateway (DRG)**
- **local peering gateway (LPG)**
- **instance with private IPs**

**Summary of New Concepts for Experienced Networking Service Users**

If you're already familiar with the Networking service and local VCN peering, these are the most important new concepts to understand:

- For each spoke VCN subnet that needs to communicate with the on-premises network, you must update the subnet's route table with a rule that sets the target (the next hop) as the spoke VCN's LPG for all traffic destined for the on-premises network.

- You must add a route table to the hub VCN, associate it with the DRG attachment, and add a route rule with a target that depends on your situation:
  - **Transit routing directly through gateways:** Set the target (the next hop) to the hub VCN's LPG (for that spoke) for all traffic destined for that spoke VCN (or a specific subnet in that VCN).
  - **Transit routing through a private IP:** Set the target (the next hop) to a private IP on the instance, for all traffic destined for that spoke VCN (or a specific subnet in that VCN). Make sure to disable the source/destination check for the private IP's VNIC.
• You must add another route table to the hub VCN, associate it with the hub VCN's LPG (for that spoke), and add a route rule with a target that depends on your situation:

  • **Transit routing directly through gateways:** Set the target (the next hop) as the DRG for all traffic destined for the on-premises network (or a specific subnet in that network).

  • **Transit routing through a private IP:** Set the target (the next hop) to another private IP on that instance, for all traffic destined for the on-premises network (or a specific subnet in that network). Again, make sure to disable the source/destination check for the private IP's VNIC. In the example presented here, the private IP is on a secondary VNIC on the instance, in a different subnet. In the subsequent diagrams, the subnets are referred to as the frontend subnet and backend subnet.

For transit routing directly through gateways, see these specific tasks for more information:

• For routing directly between gateways on page 2791

• Task 6: Set up ingress routing for the DRG and LPG on the hub VCN on page 2794

For transit routing through a private IP: see these specific tasks for more information:

• Task 5: Add a route rule to the spoke VCN's subnet on page 2793

• Task 6: Set up the private IPs on an instance in the hub VCN on page 2799

• Task 7: Set up ingress routing for the DRG and LPG on the hub VCN on page 2800

**Example: Components and Routing for a Hub and Single Spoke**

The examples in this section show a VCN acting as a hub and only a single spoke VCN for simplicity.

---

**Note:**

In a hub-and-spoke model, the hub VCN can have multiple spokes and therefore multiple LPGs (one per spoke). This topic uses the phrase the hub VCN's LPG, which could therefore be ambiguous. When the phrase is used here, it means the hub LPG for the particular spoke of interest. In the following diagrams, it's LPG-H-1. Additional spokes would involve creation of an LPG-H-2, LPG-H-3, and so on.

---

**For transit routing directly through gateways**

The following diagram shows the required Networking service route tables and route rules for transit routing directly through gateways. Although the hub VCN does not require a subnet to make transit routing work, the example presented here includes a subnet called Subnet-H.
The diagram shows four route tables, each associated with a different resource:

- **DRG attachment:**
  - The route table belongs to the hub VCN and is associated with the DRG attachment. Why the attachment and not the DRG itself? Because the DRG is a standalone resource that you can attach to any VCN in the same region and tenancy as the DRG. The attachment itself identifies which VCN.
  - The route table routes the inbound traffic that is from the on-premises network and destined for the spoke VCN (VCN-1). You configure the rule to send that traffic to LPG-H-1.

- **LPG-H-1:**
  - This route table belongs to the hub VCN and is associated with LPG-H-1.
  - The route table routes inbound traffic that is from VCN-1 and destined for the on-premises network. You configure the rule to send that traffic to the DRG.

- **Subnet-H:**
  - This route table belongs to the hub VCN and is associated with Subnet-H.
  - This route table has a rule to route traffic that is destined for the on-premises network to the DRG. It has another rule to route traffic that is destined for the spoke VCN to LPG-H-1.

- **Subnet-1:**
  - This route table belongs to the spoke VCN and is associated with Subnet-1.
  - This route table has rules to route traffic that is destined for the hub VCN or the on-premises network to LPG-1.

**For transit routing through a private IP**

The following diagram shows the required Networking service route tables and route rules for transit routing through a private IP on an instance in the hub VCN. You can choose to implement this scenario with either a single VNIC or multiple VNICs. The diagram and example here shows two VNICs: one in a subnet called Subnet-H-Frontend, and another in a subnet called Subnet-H-Backend. The frontend VNIC has private IP 10.0.4.3, and the backend VNIC has private IP 10.0.8.3.
The diagram shows five route tables, each associated with a different resource:

- **DRG attachment:**
  - The route table belongs to the hub VCN and is associated with the DRG attachment. Why the attachment and not the DRG itself? Because the DRG is a standalone resource that you can attach to any VCN in the same region and tenancy as the DRG. The attachment itself identifies which VCN.
  - The route table routes the inbound traffic that is from the on-premises network and destined for the spoke VCN (VCN-1). You configure the rule to send the traffic to the private IP in the frontend subnet.

- **LPG-H-1:**
  - This route table belongs to the hub VCN and is associated with LPG-H-1.
  - The route table routes inbound traffic that is from VCN-1 and destined for the on-premises network. You configure the rule to send that traffic to the private IP in the backend subnet.

- **Subnet-H-Frontend:**
  - This route table belongs to the hub VCN and is associated with Subnet-H-Frontend.
  - This route table has a rule to route traffic that is destined for the on-premises network to the DRG.
  - Although Oracle does not recommend putting workloads in the hub VCN's subnets, the diagram also shows a route rule to route traffic that is destined for the spoke VCN to the private IP in the frontend subnet (10.0.4.3) for filtering by the instance. The second rule is shown here to give a more complete picture of routing for this example.

- **Subnet-H-Backend:**
  - This route table belongs to the hub VCN and is associated with Subnet-H-Backend.
  - This route table has a rule to route traffic that is destined for the spoke VCN (VCN-1) to LPG-H-1.
  - Although Oracle does not recommend putting workloads in the hub VCN's subnets, the diagram also shows a route rule to route traffic that is destined for the on-premises network to the private IP in the backend subnet (10.0.8.3) for filtering by the instance. The second rule is shown here to give a more complete picture of routing for this example.

- **Subnet-1:**
  - This route table belongs to the spoke VCN and is associated with Subnet-1.
  - This route table has rules to route traffic that is destined for the hub VCN or the on-premises network to LPG-1.

**Important Transit Routing Restrictions to Understand**

This section includes some additional important details about routing:
- **Route table for the DRG attachment:**
  - A route table that is associated with a DRG attachment can have only rules that target an LPG or a private IP.
  - A DRG attachment can exist without a route table associated with it. However, after you associate a route table with a DRG attachment, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

- **Route table for an LPG:**
  - A route table that is associated with an LPG can have only rules that target a DRG or a private IP.
  - An LPG can exist without a route table associated with it. However, after you associate a route table with an LPG, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

- **Traffic through the hub VCN:** The route tables discussed here are intended only for moving traffic through the hub VCN between locations in the on-premises network and locations in the spoke VCN. If you're using a private IP in the hub, you configure those route tables so that the private IP is placed in that traffic path going through the hub.

- **Inbound traffic to the hub VCN:** Even though the preceding statement is true (about traffic through the hub), inbound traffic to subnets within the hub VCN is always allowed. You do not need to set up explicit rules for this inbound traffic in the DRG attachment's route table or hub LPG's route table. When this kind of inbound traffic reaches the DRG or the hub LPG, the traffic is automatically routed to its destination in the hub VCN by the VCN local routing. Because of VCN local routing, for any route table belonging to a given VCN, you can't create a rule that lists that VCN's CIDR (or a sub-section) as the rule's destination.

- **Hub VCN traffic when transit routing through a private IP:** The immediately preceding statement about VCN local routing means that you should use the hub VCN only for transit between the on-premises network and spoke VCNs. Do not set up workloads in the hub VCN itself. More explicitly, if you set up transit routing through a private IP in the hub VCN, you can't also route the hub VCN's traffic through that private IP. For example, in the preceding diagram, if you were to change the route rule in the LPG-H-1 route table so that the destination CIDR is 0.0.0.0/0 instead of 172.16.0.0/12, only traffic coming from VCN-1 and destined for addresses outside the hub VCN's CIDR block would be routed through the private IP. Because of VCN local routing, any traffic destined for addresses within the VCN is automatically routed directly to the destination IP address. The VCN local routing takes precedence over the LPG-H-1 route table (in general, over any of the VCN's route tables).

**About CIDR Overlap**

In this example, the various networks do not have overlapping CIDR blocks (172.16.0.0/12 versus 10.0.0.0/16 versus 192.168.0.0/16). The Networking service does not allow local VCN peering between two VCNs with overlapping CIDRs. That means each spoke must not overlap with the hub.

However, the Networking service does not validate whether the spoke VCNs themselves overlap with each other, or if any of the VCNs overlap with the on-premises network. You must ensure that CIDRs for all the subnets that need to communicate with each other don't overlap. Otherwise, traffic may be dropped.

A Networking service route table cannot contain two rules with the exact same destination CIDR. However, if two rules in the same route table have overlapping destination CIDRs, the most specific rule in the table is used to route the traffic (that is, the rule with the longest prefix match).

**Route Advertisement to the On-Premises Network and Spoke VCNs**

From a security standpoint, you can control route advertisement so that only specific subnets in the on-premises network are advertised to the spoke VCNs. Similarly, you can control which subnets in the spoke VCNs are advertised to the on-premises network.

The routes advertised to the on-premises network consist of:
- The rules listed in the route table associated with the DRG attachment (192.168.0.0/16 in the preceding diagram)
- The individual subnets in the hub VCN

The routes advertised to the spoke VCN consist of:
- The individual subnets in the hub VCN
Networking

- The rules listed in the route table associated with the hub VCN’s LPG for the spoke (172.16.0.0/12 in the preceding diagram)

Therefore, the administrator of the hub VCN alone can control which routes are advertised to the on-premises network and spoke VCNs.

In the preceding example, the relevant routes use the full CIDR block of the on-premises network and spoke VCN as the destination (172.16.0.0/12 and 192.168.0.0/16, respectively), but they could instead use a subnet of those networks to restrict routing to specific subnets.

*Details About Routing for Different Traffic Paths*

To further illustrate how routing takes place in the preceding example, let’s look more closely at different paths of traffic. Here are the same diagrams again.

First, if you are transit routing directly through gateways on the hub VCN:

Second, if you are transit routing through a private IP in the hub VCN:
Traffic from the on-premises network to the spoke VCN

1. Traffic leaves the on-premises network and reaches the DRG. The traffic's destination is in Subnet-1 (for example, 192.168.0.5).

2. The DRG attachment's associated route table has a rule for 192.168.0.0/16. It matches the destination and sends the traffic to the route target:
   - **Transit routing directly through gateways**: The rule's target is LPG-H-1.
   - **Transit routing through a private IP**: The rule's target is the private IP 10.0.4.3. The instance receives and processes the traffic and sends any resulting traffic out of the backend subnet's VNIC. The backend subnet's route table sends that traffic to LPG-H-1.

Remember that you can use the rules in the DRG attachment's route table to control which subnets in the spoke VCN are advertised to the on-premises network. You could instead set up the rule to list only a subnet of the spoke VCN.

3. LPG-H-1 receives the traffic.

4. Egress traffic leaving a VCN through an LPG is automatically routed to the LPG's peered LPG, which is LPG-1 in this situation. That routing occurs automatically because of the peering connection between the two LPGs.

5. LPG-1 receives the traffic.

6. Traffic coming in to a VCN through the LPG is automatically routed to the destination within the VCN because of VCN local routing. No explicit route rules are required.

Traffic from the spoke VCN to the on-premises network

1. Traffic comes from an instance in Subnet-1 in the spoke VCN. The traffic's destination is in the on-premises network (for example, 172.16.0.3).

2. Subnet-1's associated route table has a rule for 172.16.0.0/12. It matches the destination and sends the traffic to the route target, LPG-1.

3. LPG-1 receives the traffic.

4. Egress traffic leaving a VCN through an LPG is automatically routed to the LPG's peered LPG, which is LPG-H-1 in this situation. That routing occurs automatically because of the peering connection between the two LPGs.

5. LPG-H-1 receives the traffic.

6. LPG-H-1's associated route table has a rule for 172.16.0.0/12. It matches the destination and sends the traffic to the route target:
   - **Transit routing directly through gateways**: The rule's target is the DRG.
   - **Transit routing through a private IP**: The rule's target is the private IP 10.0.8.3. The instance receives and processes the traffic and sends any resulting traffic out of the frontend subnet's VNIC. The frontend subnet's route table sends that to the DRG.

Remember that you can use the rules in the LPG's route table to control which subnets in the on-premises network are advertised to the spoke VCN. You could instead set up the rule to list only a subnet of the on-premises network.

7. The DRG receives the traffic.

8. Egress traffic leaving the VCN through the DRG is routed based on the IPSec VPN and FastConnect configuration. No explicit rules in the DRG attachment's route table are required.

Notice that Subnet-1 in the spoke VCN and LPG-H-1 both have route rules with 172.16.0.0/12 as the destination CIDR. Those rules don't have to use the exact same CIDR block. However, make sure both rules cover the traffic you want to route from the spoke to the on-premises network. The rule in Subnet-1's route table controls which traffic is routed from Subnet-1 to LPG-H-1. The rule in LPG-H-1's route table controls which traffic is routed from the spoke VCN to the on-premises network. If LPG-H-1's route rule is more restrictive than Subnet-1's route rule, some traffic leaving the subnet could ultimately be dropped and not reach the DRG.

Traffic from the spoke VCN to a subnet in the hub VCN (routing directly between gateways only)

Depending on your situation, you might want to enable traffic between instances in the hub VCN and a spoke VCN, and not just traffic between the on-premises network and a spoke VCN. You can do this if you're routing...
directly between gateways. **You can't route the traffic from a spoke VCN through the private IP and on to other instances in the hub VCN.** The note at the end of this section explains why.

Here's how traffic would flow from the spoke VCN to a destination with an address in the hub VCN:

1. Traffic comes from an instance in Subnet-1 in the spoke VCN. The traffic's destination is in a subnet in the hub VCN (for example, 10.0.0.3).
2. Subnet-1's associated route table has a rule for 10.0.0.0/16. It matches the destination and sends the traffic to the route target, LPG-1.
3. LPG-1 receives the traffic.
4. Egress traffic leaving a VCN through an LPG is automatically routed to the LPG's peered LPG, which is LPG-H-1 in this situation. That routing occurs automatically because of the peering connection between the two LPGs.
5. LPG-H-1 receives the traffic.
6. Traffic coming in to a VCN through an LPG and destined for an address in the VCN is automatically routed to the destination by VCN local routing. No explicit route rules are required.

A similar series of routing steps occurs for traffic going from Subnet-H to Subnet-1, but in the reverse direction. Subnet-H's route table has a rule that matches the spoke VCN's CIDR (192.168.0.0/16) and sends the traffic to LPG-H-1, which forwards it on to LPG-1.

**Note:**

If you set up transit routing through a private IP in the hub VCN, remember that the LPG-H-1 route table only controls routing of traffic that is destined for addresses *outside the hub VCN*. Traffic destined for addresses within the VCN is instead handled by the hub VCN local routing, which takes precedence and always routes the traffic directly to the packet's destination address. This means that you cannot route traffic that is destined for addresses inside the hub VCN *through the private IP* that is being used for the transit traffic through the hub. Even if the LPG-H-1 route rule uses a destination = 0.0.0.0/0 and target = 10.0.8.3, the hub VCN local routing takes precedence and routes the traffic directly to the destination in the hub VCN instead of the private IP.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

If you’re a member of the Administrators group, you already have the required access to set up transit routing. Otherwise, you need access to the Networking service, and you need the ability to launch instances. See *IAM Policies for Networking* on page 2832.

**Setting Up VCN Transit Routing in the Console**

This section shows how to use the Console to set up transit routing with a VCN to give your on-premises network access to multiple VCNs in the same region.

*For routing directly between gateways*

**Tip:**

You might already have many of the necessary Networking components and connections in this advanced scenario already set up. So you might be able to skip some of the following tasks. **If you already have a network topology with a hub VCN connected to your on-premises network, and spoke VCNs locally peered with the hub VCN, then Task 5 and Task 6 are the most important.** They enable traffic to be routed between your on-premises network and the spoke VCN.
Networking

Task 1: Set up the hub VCN

In this task, you set up the hub VCN. A subnet in the hub VCN is optional. However, this example includes one. The subnet can contain cloud resources that your on-premises network or the spoke VCN need to use.

For more information and instructions:
- VCNs and Subnets on page 2821

Task 2: Connect the hub VCN with your on-premises network

In this task, you set up either FastConnect or VPN Connect between your hub VCN and your on-premises network. As part of this process, you attach a DRG to the hub VCN and set up routing between the hub VCN and your on-premises network. Notice that you do not yet create the route table that will be associated with the DRG attachment. That comes in a later step. For more information and instructions:
- FastConnect on page 3173
- VPN Connect on page 2932
- Dynamic Routing Gateways (DRGs) on page 2927

Task 3: Set up a spoke VCN with at least one subnet
In this task, you set up the spoke VCN with at least one subnet. For more information and instructions:

- [VCNs and Subnets](#) on page 2821

Task 4: Set up a local peering between the hub VCN and the spoke VCN

In this task, you add an LPG to each VCN, establish a connection between the LPGs, and set up routing that enables resources in one VCN to communicate with resources in the other.

**Important:**

When setting up local peering between two VCNs, make sure to establish the connection between the LPGs. It can be easy to overlook that part of the process.

Notice that you do not yet create the route table that will be associated with the LPG on the hub VCN (LPG-H-1). That comes in a later step. For more information and instructions:

- [Setting Up a Local Peering](#) on page 3271

Task 5: Add a route rule to the spoke VCN's subnet
Networking

In this task, you add a rule to the route table associated with the spoke VCN's subnet. This rule routes traffic that is destined for the on-premises network to the spoke VCN's LPG (LPG-1 in the diagram). Prerequisites: You already have an LPG for the spoke VCN, and a route table associated with the subnet (on the spoke VCN) that needs to communicate with the on-premises network.

1. For the spoke VCN, view the list of subnets.
2. For the subnet of interest, look at its details and click the link for its associated route table.
3. Edit the route table to include a rule that sends traffic to the on-premises network:
   a. Click Add Route Rules.
   b. Enter this information for the route rule:
      • **Target Type**: Local Peering Gateway.
      • **Destination CIDR Block**: The on-premises network's CIDR (172.16.0.0/12 in the earlier example).
      • **Compartment**: The compartment where the spoke VCN's LPG is located.
      • **Target Local Peering Gateway**: The spoke VCN's LPG.
      • **Description**: An optional description of the rule.
   c. Click Add Route Rules.

Task 6: Set up ingress routing for the DRG and LPG on the hub VCN
In this task, you set up the route tables for the DRG attachment and hub VCN's LPG for the spoke of interest (LPG-H-1).

Prerequisites:

• You already have a DRG attached to the hub VCN.
• You already have a hub VCN LPG for the spoke of interest.

1. Create a route table for the DRG attachment:
   a. In the Console, view the hub VCN's details.
   b. Under Resources, click Route Tables to view the VCN's route tables.
   c. Click Create Route Table.
   d. Enter the following:
      • Name: A descriptive name for the route table. Example: DRG Route Table. Avoid entering confidential information.
      • Create in Compartment: Leave as is.
   e. Click + Additional Route Rule, and enter this information for the route rule:
      • Target Type: Local Peering Gateway.
      • Destination CIDR Block: This spoke VCN's CIDR (192.168.0.0/16 in the earlier example). Remember that you can use the routes in this table to control which subnets in the spoke VCN are advertised to the on-premises network. You could instead set up the rule to list only a particular subnet of the spoke VCN that the on-premises network.
      • Compartment: The compartment where the hub VCN's LPG is located.
      • Target: The hub VCN's LPG.
      • Description: An optional description of the rule.
   f. Click Create Route Table.

   The route table is created and displayed in the list.
2. Associate the route table (called DRG Route Table in this example) with the hub VCN's DRG attachment:
   a. While still viewing the hub VCN's details, click Dynamic Routing Gateways to view the attached DRG.
   b. Click the Actions icon (three dots), and then click Associate Route Table.
   c. Select the route table.
   d. Click Associate Route Table.
      The route table is associated with the DRG attachment.
3. Create a route table for the hub VCN's LPG for this spoke:
   a. While still viewing the hub VCN's details, click Route Tables.
   b. Click Create Route Table.
   c. Enter the following:
      • Create in Compartment: Leave as is.
      • Name: A descriptive name for the route table. Example: Hub LPG-# Route Table (where # indicates which spoke). Avoid entering confidential information.
   d. Click + Additional Route Rule, and enter this information for the route rule:
      • Target Type: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      • Destination CIDR Block: The on-premises network's CIDR (172.16.0.0/12 in the earlier example). Remember that you can use the routes in this table to control which subnets in the on-premises network are advertised to this spoke VCN. You could instead set up the rule to list only a subnet of the on-premises network that needs to communicate with this spoke.
      • Description: An optional description of the rule.
   e. Click Create Route Table.
      The route table is created and displayed in the list.
4. Associate the route table (called Hub LPG-# Route Table in this example) with the hub VCN's LPG for the spoke of interest:
   a. While still viewing the hub VCN's details, click Local Peering Gateways to view the hub VCN's LPG for this spoke.
   b. For the LPG you're interested in, click the Actions icon (three dots), and then click Associate With Route Table.
   c. Enter the following:
      • Route Table Compartment: Select the compartment of the route table for the LPG.
      • Route Table: Select the route table for the LPG.
   d. Click Associate.
      The route table is associated with the LPG.

Later if you need more spoke VCNs

1. Repeat Tasks 3-5 for the new spoke VCN.
2. Repeat Task 6 with these changes:
   • For Step 1: Instead of creating a new route table for the DRG attachment, update the existing route table to include a new rule for the new spoke VCN. The destination CIDR is the spoke VCN's CIDR (or a subnet within). The target is the hub VCN's LPG for the new spoke.
   • For Step 2: Skip this step entirely because the DRG attachment is already associated with its route table.
   • For Step 3: Repeat as is. Name the new route table according to which spoke the route table is for (for example, Hub LPG-2 Route Table for the second spoke).
   • For Step 4: Repeat as is. Associate the new route table you created in Step 3 with the hub VCN's LPG for the new spoke.
For routing through a private IP

Tip:
You might already have many of the necessary Networking components and connections in this advanced scenario already set up. So you might be able to skip some of the following tasks. **If you already have a network topology with a hub VCN connected to your on-premises network, and spoke VCNs locally peered with the hub VCN, then Tasks 5 through 7 are the most important.** They enable traffic to be routed between your on-premises network and the spoke VCN.

Task 1: Set up the hub VCN

In this task, you set up the hub VCN. The hub VCN must have two subnets: one for the frontend VNIC on the instance, and one for the backend VNIC on the instance. Oracle recommends using regional *private* subnets, unless there will be resources in the frontend subnet that need internet access.

For more information and instructions:
- VCNs and Subnets on page 2821

Task 2: Connect the hub VCN with your on-premises network

In this task, you set up either FastConnect or VPN Connect between your hub VCN and your on-premises network. As part of this process, you attach a DRG to the hub VCN and set up routing between the hub VCN and your on-premises network. Notice that you do not yet create the route table that will be associated with the DRG attachment. That comes in a later step. For more information and instructions:
- FastConnect on page 3173
- VPN Connect on page 2932
- Dynamic Routing Gateways (DRGs) on page 2927

Task 3: Set up a spoke VCN with at least one subnet
In this task, you set up the spoke VCN with at least one subnet. For more information and instructions:

- **VCNs and Subnets** on page 2821

Task 4: Set up a local peering between the hub VCN and the spoke VCN

In this task, you add an LPG to each VCN, establish a connection between the LPGs, and set up routing that enables resources in one VCN to communicate with resources in the other.

**Important:**

When setting up local peering between two VCNs, make sure to establish the connection between the LPGs. It can be easy to overlook that part of the process.

Notice that you do not yet create the route table that will be associated with the LPG on the hub VCN (LPG-H-1). That comes in a later step. For more information and instructions:

- **Setting Up a Local Peering** on page 3271

Task 5: Add a route rule to the spoke VCN's subnet
In this task, you add a rule to the route table associated with the spoke VCN's subnet. This rule routes traffic that is destined for the on-premises network to the spoke VCN's LPG (LPG-1 in the diagram). Prerequisites: You already have an LPG for the spoke VCN, and a route table associated with the subnet (on the spoke VCN) that needs to communicate with the on-premises network.

1. For the spoke VCN, view the list of subnets.
2. For the subnet of interest, look at its details and click the link for its associated route table.
3. Edit the route table to include a rule that sends traffic to the on-premises network:
   a. Click Add Route Rules.
   b. Enter this information for the route rule:
      - **Target Type**: Local Peering Gateway.
      - **Destination CIDR Block**: The on-premises network's CIDR (172.16.0.0/12 in the earlier example).
      - **Compartment**: The compartment where the spoke VCN's LPG is located.
      - **Target Local Peering Gateway**: The spoke VCN's LPG.
      - **Description**: An optional description of the rule.
   c. Click Add Route Rules.

Task 6: Set up the private IPs on an instance in the hub VCN

In this task, you set up the instance to have 2 private IPs.

Prerequisites:
- You already have a hub VCN with a subnet.
- Review this information: Using a Private IP as a Route Target on page 2924.

1. If you haven't already, create the instance in the hub VCN. See Creating an Instance on page 695. The primary VNIC is created in the subnet you specify.
2. Create a secondary VNIC for the other subnet and configure the OS to use it. See Using the Console on page 2858.
3. Disable the source/destination check on each of the VNICs. See Overview of VNICs and Physical NICs on page 2856.

4. For each VNIC, determine which private IP you want to use as the routing target. If you want to use a secondary private IP instead of the VNIC's primary private IP, assign that secondary private IP and configure the OS to use it. See Using the Console on page 2866.

5. For each of the private IPs you created, record the private IP address (for example: 10.0.4.3).

6. Configure the instance as necessary for the job it will perform (for example, configure the firewall or intrusion detection system on the instance).

**Task 7: Set up ingress routing for the DRG and LPG on the hub VCN**

In this task, you set up the route tables for the DRG attachment and hub VCN's LPG for the spoke of interest (LPG-H-1).

**Prerequisites:**
- You already have a DRG attached to the hub VCN.
- You already have a hub VCN LPG for the spoke of interest.
- You already have the two private IPs to use as the routing targets (see the preceding task).

1. Create a route table for the DRG attachment:
   a. In the Console, view the hub VCN's details.
   b. Under Resources, click Route Tables to view the VCN's route tables.
   c. Click Create Route Table.
   d. Enter the following:
      - **Name:** A descriptive name for the route table. Example: DRG Route Table. Avoid entering confidential information.
      - **Create in Compartment:** Leave as is.
   e. Click + Additional Route Rule, and enter this information for the route rule:
      - **Target Type:** Private IP.
      - **Destination CIDR Block:** This spoke VCN's CIDR (192.168.0.0/16 in the earlier example). Remember that you can use the routes in this table to control which subnets in the spoke VCN are advertised to the on-
Networking

premises network. You could instead set up the rule to list only a particular subnet of the spoke VCN that the on-premises network.

- **Compartment**: The compartment where the frontend subnet's private IP is located.
- **Target**: The frontend subnet's private IP, which you recorded in the previous task (10.0.4.3 in the example).
- **Description**: An optional description of the rule.

f. Click **Create Route Table**.

The route table is created and displayed in the list.

2. Associate the route table (called **DRG Route Table** in this example) with the hub VCN's DRG attachment:

a. While still viewing the hub VCN's details, click **Dynamic Routing Gateways** to view the attached DRG.

b. Click the Actions icon (three dots), and then click **Associate With Route Table**.

c. Enter the following:

- **Route Table Compartment**: Select the compartment of the route table for the DRG attachment.
- **Route Table**: Select the route table for the DRG attachment.

d. Click **Associate**.

The route table is associated with the DRG attachment.

3. Create a route table for the hub VCN's LPG for this spoke:

a. While still viewing the hub VCN's details, click **Route Tables**.

b. Click **Create Route Table**.

c. Enter the following:

- **Create in Compartment**: Leave as is.
- **Name**: A descriptive name for the route table. Example: Hub LPG-# Route Table (where # indicates which spoke). Avoid entering confidential information.

d. Click **+ Additional Route Rule**, and enter this information for the route rule:

- **Target Type**: Private IP.
- **Destination CIDR Block**: The on-premises network's CIDR (172.16.0.0/12 in the earlier example). Remember that you can use the routes in this table to control which subnets in the on-premises network are advertised to this spoke VCN. You could instead set up the rule to list only a subnet of the on-premises network that needs to communicate with this spoke.
- **Compartment**: The compartment where the private IP is located.
- **Target**: The backend subnet's private IP, which you recorded in the previous task (10.0.8.3 in the example).
- **Description**: An optional description of the rule.

e. Click **Create Route Table**.

The route table is created and displayed in the list.

4. Associate the route table (called **Hub LPG-# Route Table** in this example) with the hub VCN's LPG for the spoke of interest:

a. While still viewing the hub VCN's details, click **Local Peering Gateways** to view the hub VCN's LPG for this spoke.

b. For the LPG you're interested in, click the Actions icon (three dots), and then click **Associate With Route Table**.

c. Enter the following:

- **Route Table Compartment**: Select the compartment of the route table for the LPG.
- **Route Table**: Select the route table for the LPG.

d. Click **Associate**.

The route table is associated with the LPG.
Although Oracle does not recommend putting workloads in the hub VCN's subnets, to give you a more complete picture of routing in the example, the diagram shows two additional route rules in the hub VCN's subnet route tables. For the frontend subnet, there's a route rule to route traffic that is destined for the spoke VCN to the private IP in the frontend subnet (10.0.4.3) for filtering by the instance. For the backend subnet, there's a route rule to route traffic that is destined for the on-premises network to the private IP in the backend subnet (10.0.8.3) for filtering by the instance. The following procedure adds those two route rules.

1. For the spoke VCN, view the list of subnets.
2. For the frontend subnet, look at its details and click the link for its associated route table.
3. Edit the frontend subnet's route table to include a rule that sends traffic destined for the spoke VCN to the private IP in the frontend subnet:
   a. Click Add Route Rules.
   b. Enter this information for the route rule:
      - **Target Type**: Private IP.
      - **Destination CIDR Block**: This spoke VCN's CIDR (192.168.0.0/16 in the earlier example).
      - **Compartment**: The compartment where the frontend subnet's private IP is located.
      - **Target**: The frontend subnet's private IP, which you recorded in the previous task (10.0.4.3 in the example).
      - **Description**: An optional description of the rule.
   c. Click Add Route Rules.
4. For the backend subnet, look at its details and click the link for its associated route table.
5. Edit the backend subnet's route table to include a rule that sends traffic destined for the on-premises network to the private IP in the backend subnet:
   a. Click Add Route Rules.
   b. Enter this information for the route rule:
      - **Target Type**: Private IP.
      - **Destination CIDR Block**: The on-premises network's CIDR (172.16.0.0/12 in the earlier example).
      - **Compartment**: The compartment where the backend subnet's private IP is located.
      - **Target**: The backend subnet's private IP, which you recorded in the previous task (10.0.8.3 in the example).
      - **Description**: An optional description of the rule.
   c. Click Add Route Rules.

Later if you need more spoke VCNs

1. Repeat Tasks 3-5 for the new spoke VCN.
2. Repeat task 7 with these changes:
   - For Step 1: Instead of creating a new route table for the DRG attachment, update the existing route table to include a new rule for the new spoke VCN. The destination CIDR is the spoke VCN's CIDR (or a subnet within). The target is the frontend subnet private IP 10.0.4.3.
   - For Step 2: Skip this step entirely because the DRG attachment is already associated with its route table.
   - For Step 3: Repeat as is. Name the new route table according to which spoke the route table is for (for example, Hub LPG-2 Route Table for the second spoke).
   - For Step 4: Repeat as is. Associate the new route table you created in Step 3 with the hub VCN's LPG for the new spoke.

**Turning Off Transit Routing**

To turn off transit routing, remove the rules from:

- The route table associated with the DRG attachment.
- The route table associated with each LPG on the hub VCN.

A route table can be associated with a resource but have no rules. Without at least one rule, a route table does nothing.
A DRG attachment or LPG can exist without a route table associated with it. However, after you associate a route table with a DRG attachment or LPG, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table’s rules, or delete some or all of the rules.

Changes to the API

For information about changes to the Networking service API to support transit routing, see the transit routing release notes.

Transit Routing: Private Access to Oracle Services

*Transit routing* refers to a network topology in which your on-premises network uses a connected virtual cloud network (VCN) to reach Oracle resources or services beyond that VCN. You connect the on-premises network to the VCN with FastConnect or VPN Connect, and then configure the VCN routing so that traffic *transits through the VCN* to its destination beyond the VCN.

There are two primary transit routing scenarios:

- **Private access to Oracle services:** The scenario covered in this topic. This scenario gives your on-premises network private access to Oracle services, so that your on-premises hosts can use their private IP addresses and the traffic does not go over the public internet. Instead, the traffic travels over a FastConnect private virtual circuit or VPN Connect, transits through a virtual cloud network (VCN), and then through a *service gateway* to the Oracle service of interest.

- **Access to multiple VCNs in the same region:** This scenario enables communication between an on-premises network and multiple VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect. See Transit Routing: Access to Multiple VCNs in the Same Region on page 2780.

Highlights

- You can set up a VCN so that your on-premises network has private access to Oracle services in the Oracle Services Network by way of the VCN. The hosts in your on-premises network communicate with their private IP addresses.

- The VCN uses a *dynamic routing gateway* (DRG) to communicate with the on-premises network. Access to Oracle services is through a *service gateway* on the VCN. The traffic from the VCN to the Oracle service travels over the Oracle network fabric and never traverses the public internet.

- The service gateway is regional and enables access only to supported Oracle services *in the same region* as the VCN.

- The supported Oracle services are Oracle Cloud Infrastructure Object Storage and others in the Oracle Services Network. For a list, see Service Gateway: Supported Cloud Services in Oracle Services Network.

- The service gateway uses the concept of a *service CIDR label*, which is a string that represents all the regional public IP address ranges for the service or group of services of interest (for example, *OCI PHX Object Storage* is the string for Object Storage in US West (Phoenix)). You use that service CIDR label when you configure the service gateway and related route rules to control traffic to the service. You can optionally use it when configuring security rules. If the service’s public IP addresses change in the future, you don’t have to adjust those rules.

- To enable the desired traffic from the on-premises network through the VCN to Oracle services, you implement route rules for the VCN’s DRG attachment and service gateway.

- If you want, you can set up transit routing through a private IP in the VCN. For example, you might want to filter or inspect the traffic between the on-premises network and the Oracle service. In that case, you route the traffic to a private IP on an instance in the VCN for inspection, and the resulting traffic continues to its destination. This topic covers both situations: transit routing directly between gateways on the VCN, and transit routing through a private IP.

Overview of the Oracle Services Network

The Oracle Services Network is a conceptual network in Oracle Cloud Infrastructure that is reserved for Oracle services. These services have public IP addresses that you typically reach over the public internet. However, you can access the Oracle Services Network *without the traffic going over the public internet*. There are different ways, depending on which of your hosts need the access:
• **Hosts in your on-premises network:**
  - Private access through a VCN with FastConnect private peering or VPN Connect: This is the scenario covered in this topic. The on-premises hosts use private IP addresses and reach the Oracle Services Network by way of the VCN and the VCN’s service gateway.
  - **Public access with FastConnect public peering:** The on-premises hosts use public IP addresses.

• **Hosts in your VCN:**
  - Private access through a service gateway: The VCN’s hosts use private IP addresses.

**Overview of On-Premises Network Private Access to Oracle Services**

The following diagram illustrates the basic layout for giving your on-premises network private access to Oracle services.

![Diagram](image_url)

**Legend:**
- □ dynamic routing gateway (DRG)
- ◊ service gateway

Your on-premises network connects to the VCN by way of a FastConnect private virtual circuit or VPN Connect on page 2932. Each of these types of connections terminates on a dynamic routing gateway (DRG) that is attached to the VCN. The VCN also has a service gateway, which gives the VCN access to the Oracle Services Network. The traffic from your on-premises network transits through the VCN, through the service gateway, and to the Oracle service of interest. The responses return through the service gateway and VCN to your on-premises network.

When you set up a service gateway, you enable a *service CIDR label*, which is a string that represents all the regional public IP address ranges for the service or group of services that you want to access through the service gateway. For example, *All PHX Services in Oracle Services Network* is the service CIDR label for the Oracle services available in US West (Phoenix) through a service gateway. Oracle uses Border Gateway Protocol (BGP) on the DRG to advertise those regional public IP address ranges to the edge device (also called the customer-premises equipment or CPE) in your on-premises network. For a list of those ranges available through the service gateway, see Public IP Addresses for VCNs and the Oracle Services Network on page 193.

**Multiple Connection Paths to Oracle Services**

You can configure your on-premises network with multiple connection paths to Oracle Cloud Infrastructure and Oracle services for redundancy or other reasons. For example, you could use both FastConnect public peering and FastConnect private peering. If you have multiple paths, your edge device receives route advertisement of the Oracle services public IP address ranges over multiple paths. For important information about configuring your edge device correctly, see Routing Details for Connections to Your On-Premises Network on page 2942.

**Multiple VCNs with Private Access to Oracle Services**

Your organization might choose to use multiple VCNs, each with a service gateway to give the VCN's resources access to Oracle services. For example, you might have a different VCN for each department in your organization.

If you *also* want to set up your on-premises network with private access to Oracle services through a VCN with a service gateway, this section describes two different network layouts you could use.
In the first layout, you set up a single DRG, with the VCNs in a hub-and-spoke layout as shown in the next diagram. The VCN that acts as the hub is dedicated to providing the on-premises network with private access to Oracle services. The other VCNs are locally peered with the hub VCN. You configure only the hub VCN according to instructions in Setting Up Private Access to Oracle Services on page 2809. This hub-and-spoke layout is recommended and described further in Transit Routing: Access to Multiple VCNs in the Same Region on page 2780.

In the second layout, there’s a separate DRG for each VCN, with a separate FastConnect private virtual circuit or VPN Connect from your on-premises network to each DRG. You dedicate one DRG and VCN to providing your on-premises network with private access to Oracle services. In the next diagram, it’s the VCN in the center. To configure that VCN, follow the instructions in Setting Up Private Access to Oracle Services on page 2809.

Notice that in both of these layouts, the on-premises network can reach the Oracle services only through a single VCN’s service gateway (the one dedicated for this purpose) and not through the service gateways of the other VCNs. For those other VCNs, only the resources inside those VCNs can reach Oracle services through their VCN’s service gateway.

Regardless of which layout you choose, you can write an IAM policy to restrict access to an Object Storage bucket so that only requests that come through a specific VCN’s service gateway are allowed for that bucket. With either of these layouts, you might want to write the policy to allow requests from multiple VCNs. To restrict access to specific
Networking

VCNs, create a network source to specify the allowed VCN, and then write the policy restricting access to only the network source. One network source can specify multiple VCNs or you can create one network source for each VCN. For information on creating networks sources, see Managing Network Sources on page 2427.

The following example policy assumes you set up one network source for each of your VCNs. The policy lets resources in the example ObjectBackup group write objects to an existing bucket called db-backup that resides in a compartment called ABC. When writing a policy like this one, you can specify one or more network sources. This example shows three.

Allow group ObjectBackup to read buckets in compartment ABC
Allow group ObjectBackup to manage objects in compartment ABC where
   all {target.bucket.name='db-backup',
       any {request.networkSource.name='<hub_VCN_network_source>',
            request.networkSource.name='<spoke_1_VCN_network_source>',
            request.networkSource.name='<spoke_2_VCN_network_source>'},
       any {request.permission='OBJECT_CREATE',
            request.permission='OBJECT_INSPECT'}

For more information, see Setting Up a Service Gateway in the Console on page 3260 in the procedure for setting up a service gateway.

Requests from Oracle Services to Your Clients

The service gateway does not allow incoming connection requests to the VCN or your on-premises network. Any connection requests coming from an Oracle service to your on-premises network must come over a public path such as the internet or FastConnect public peering.

If you use Oracle Analytics Cloud so that it initiates connection requests to clients, and you also want to set up private access to Oracle services for your on-premises network, see this known issue.

Transit Routing Options for Private Access to Oracle Services

There are two options for routing through the VCN for private access to Oracle services:

- **Transit routing directly through gateways:** You route the traffic directly through the VCN, from one gateway to the other.
- **Transit routing through a private IP:** You set up an instance in the VCN to filter or inspect the traffic between the on-premises network and Oracle Services Network, and route traffic through a private IP on the instance.

The examples shown in the following sections assume that the VCN contains no workloads that need to access the on-premises network or Oracle Services Network. The VCN is being used only for transit routing of traffic through the VCN.

**Transit routing directly through gateways**

In this example, you route directly through the two gateways on the VCN: the dynamic routing gateway (DRG) and the service gateway. See the following diagram.
Networking

The diagram shows two route tables, each associated with a different resource:

- **DRG attachment:**
  - The route table belongs to the VCN and is associated with the DRG attachment. Why the attachment and not the DRG itself? Because the DRG is a standalone resource that you can attach to any VCN in the same region and tenancy as the DRG. The attachment itself identifies which VCN.
  - The route table routes the inbound traffic that is from the on-premises network and destined for a supported Oracle service. You configure the rule to send that traffic to the service gateway.

- **Service gateway:**
  - This route table belongs to the VCN and is associated with the service gateway.
  - The route table routes response traffic that is from a supported Oracle service and destined for the on-premises network. You configure the rule to send that traffic to the DRG.

**Transit routing through a private IP in the VCN**

In this example, you set up an instance in the VCN to act as a firewall or intrusion detection system to filter or inspect the traffic between the on-premises network and Oracle Services Network. See the following diagram.
The instance has two VNICs, each with a private IP. One of the VNICs is in a subnet that faces the on-premises network (referred to here as the *frontend subnet*). The other VNIC is in a subnet that faces the Oracle Services Network (referred to here as the *backend subnet*). The frontend VNIC has private IP 10.0.4.3, and the backend VNIC has private IP 10.0.8.3.

The diagram shows four route tables, each associated with a different resource:

- **DRG attachment:**
  - The route table belongs to the VCN and is associated with the DRG attachment. Why the attachment and not the DRG itself? Because the DRG is a standalone resource that you can attach to any VCN in the same region and tenancy as the DRG. The attachment itself identifies which VCN.
  - The route table routes the inbound traffic that is from the on-premises network and destined for a supported Oracle service. You configure the rule to send the traffic to the private IP in the frontend subnet.

- **Service gateway:**
  - This route table belongs to the VCN and is associated with the service gateway.
  - The route table routes response traffic that is from a supported Oracle service and destined for the on-premises network. You configure the rule to send that traffic to the private IP in the backend subnet.

- **Subnet/frontend:**
  - This route table belongs to the VCN and is associated with Subnet/frontend.
  - It includes a rule to enable traffic with the on-premises network.

- **Subnet-backend:**
  - This route table belongs to the VCN and is associated with Subnet-backend.
  - It includes a rule to enable traffic with the regional Oracle Services Network.

**Important Transit Routing Restrictions to Understand**

This section includes some additional important details about routing:

- **Route table for the DRG attachment:**
  - A route table that is associated with a DRG attachment can only have rules that target a service gateway, a private IP, or a local peering gateway.
  - A DRG attachment can exist without a route table associated with it. However, after you associate a route table with a DRG attachment, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

- **Route table for a service gateway:**
  - A route table that is associated with a service gateway can only have rules that target a DRG or a private IP.
  - A service gateway can exist without a route table associated with it. However, after you associate a route table with a service gateway, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

- **Traffic transiting through the VCN:** The route tables discussed here are intended only for moving traffic through the VCN between locations in the on-premises network and the Oracle Services Network. If you're using a private IP in the VCN, you configure the route tables so that the private IP is placed in that traffic path going through the VCN.

- **Inbound traffic to the VCN:** Even though the preceding statement is true (about traffic through the VCN), inbound traffic to subnets within the VCN is always allowed. You do not need to set up explicit rules for this inbound traffic in the DRG attachment's route table or service gateway's route table. When this kind of inbound traffic reaches the DRG or the service gateway, the traffic is automatically routed to its destination in the VCN by the VCN local routing. Because of VCN local routing, for any route table belonging to a given VCN, you can't create a rule that lists that VCN's CIDR (or a subsection) as the rule's destination.

- **VCN traffic when transit routing through a private IP:** The immediately preceding statement about VCN local routing means that you should use the VCN only for transit between the on-premises network and spoke VCNs. You should not set up workloads in the VCN itself. More explicitly, if you set up transit routing through a private IP in the VCN, you can't also route the VCN's traffic through that private IP. For example, in the preceding diagram, if you were to change the route rule in the service gateway's route table so that the destination CIDR...
is 0.0.0.0/0 instead of 172.16.0.0/12, only traffic coming from the Oracle Services Network and destined for addresses outside the VCN's CIDR block would be routed through the private IP. Because of VCN local routing, any traffic destined for addresses within the VCN is automatically routed directly to the destination IP address. The VCN local routing takes precedence over the service gateway’s route table (in general, over any of the VCN’s route tables).

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

If you're a member of the Administrators group, you already have the required access to set up transit routing. Otherwise, you need access to the Networking service, and you need the ability to launch instances. See [IAM Policies for Networking](#) on page 2832.

**Setting Up Private Access to Oracle Services**

This section shows how to use the Console to set up transit routing with a VCN to give your on-premises network private access to Oracle services.

*For routing directly between gateways*

**Tip:**

You might already have many of the necessary Networking components and connections in this advanced scenario already set up. So you might be able to skip some of the following tasks. *If you already have a network layout with a VCN connected to your on-premises network, and a service gateway for that VCN, then Task 4 is the most important.* It enables traffic to be routed between your on-premises network and the Oracle Services Network.

**Task 1: Set up the VCN**

In this task, you set up the VCN. For this example, no subnet is required.

For more information and instructions:

- [VCNs and Subnets](#) on page 2821

**Task 2: Add a service gateway to the VCN**
Networking

In this task, you add a service gateway to the VCN and enable the gateway for the regional Oracle Services Network. Notice that you do not yet create the route table that will be associated with the service gateway. That comes in a later task.

1. In the Console, view the VCN's details.
2. Under Resources, click Service Gateways.
3. Click Create Service Gateway.
4. Enter the following values:
   - **Name**: A descriptive name for the service gateway. It doesn't have to be unique. Avoid entering confidential information.
   - **Create in compartment**: The compartment where you want to create the service gateway, if different from the compartment you're currently working in.
   - **Services**: All <region> Services in Oracle Services Network.
5. Click Create Service Gateway.

The service gateway is then created and displayed on the Service Gateways page in the compartment you chose.

Task 3: Connect the VCN to your on-premises network

In this task, you set up either FastConnect or VPN Connect between your VCN and your on-premises network. As part of this process, you attach a DRG to the VCN and set up routing between the VCN and your on-premises network. Notice that you do not yet create the route table that will be associated with the DRG attachment. That comes in a later task. For more information and instructions:

- FastConnect on page 3173
- VPN Connect on page 2932
- Dynamic Routing Gateways (DRGs) on page 2927
Important:

If you're using VPN Connect with static routing, and you've configured the VCN to give your on-premises network private access to Oracle services, you must configure your edge device with the routes for the Oracle Services Network public IP ranges that are advertised by the DRG over the private path (through the service gateway). For a list of those ranges, see Public IP Addresses for VCNs and the Oracle Services Network on page 193.

Task 4: Set up ingress routing for the DRG and service gateway

In this task, you set up the route tables for the DRG attachment and the service gateway.

Prerequisites:

- You already have a DRG attached to the VCN.
- You already have a service gateway.

1. Create a route table for the DRG attachment:
   
   a. In the Console, view the VCN's details.
   b. Under Resources, click Route Tables to view the VCN's route tables.
   c. Click Create Route Table.
   d. Enter the following:
      
     - **Name**: A descriptive name for the route table. Example: DRG Route Table. Avoid entering confidential information.
     - **Create in Compartment**: Leave as is.
   e. Click + Additional Route Rule, and enter this information for the route rule:
      
     - **Target Type**: Service gateway.
     - **Destination Service**: All `<region>` Services in Oracle Services Network.
     - **Compartment**: The compartment where the service gateway is located.
     - **Target**: The service gateway.
     - **Description**: An optional description of the rule.
   f. Click Create Route Table.

   The route table is created and displayed in the list.
2. Associate the route table (called DRG Route Table in this example) with the VCN's DRG attachment:
   a. While still viewing the VCN's details, click Dynamic Routing Gateways to view the attached DRG.
   b. Click the Actions icon (three dots), and then click Associate With Route Table.
   c. Enter the following:
      • Route Table Compartment: Select the compartment of the route table for the DRG attachment.
      • Route Table: Select the route table for the DRG attachment.
   d. Click Associate.
      The route table is associated with the DRG attachment.

3. Create a route table for the service gateway:
   a. While still viewing the VCN's details, click Route Tables.
   b. Click Create Route Table.
   c. Enter the following:
      • Create in Compartment: Leave as is.
      • Name: A descriptive name for the route table. Example: Service Gateway Route Table. Avoid entering confidential information.
   d. Click + Additional Route Rule, and enter this information for the route rule:
      • Target Type: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      • Destination CIDR Block: The on-premises network's CIDR (172.16.0.0/12 in the earlier example).
      • Description: An optional description of the rule.
   e. Click Create Route Table.
      The route table is created and displayed in the list.

4. Associate the route table (called Service Gateway Route Table in this example) with the service gateway:
   a. While still viewing the VCN's details, click Service Gateways.
   b. For the service gateway, click the Actions icon (three dots), and then click Associate With Route Table.
   c. Enter the following:
      • Route Table Compartment: Select the compartment of the route table for the service gateway.
      • Route Table: Select the route table for the service gateway.
   d. Click Associate.
      The route table is associated with the service gateway.

For routing through a private IP

Tip:
You might already have many of the necessary Networking components and connections in this advanced scenario already set up. So you might be able to skip some of the following tasks. If you already have a network layout with a VCN connected to your on-premises network, and a service gateway for that VCN, then Tasks 4 and 5 are the most important. They enable traffic to be routed between your on-premises network and the spoke VCN.

Task 1: Set up the VCN
Networking

In this task, you set up the VCN. This example also has two subnets: one for the frontend VNIC on the instance, and one for the backend VNIC on the instance. Oracle recommends using regional private subnets.

For more information and instructions:
- VCNs and Subnets on page 2821

Task 2: Add a service gateway to the VCN

1. In the Console, view the VCN's details.
2. Under Resources, click Service Gateways.
3. Click Create Service Gateway.
4. Enter the following values:
   - Name: A descriptive name for the service gateway. It doesn't have to be unique. Avoid entering confidential information.
   - Create in compartment: The compartment where you want to create the service gateway, if different from the compartment you're currently working in.
   - Services: All <region> Services in Oracle Services Network.
5. Click Create Service Gateway.

The service gateway is then created and displayed on the Service Gateways page in the compartment you chose.

Task 3: Connect the VCN to your on-premises network
Networking

In this task, you set up either FastConnect or VPN Connect between your hub VCN and your on-premises network. As part of this process, you attach a DRG to the hub VCN and set up routing between the hub VCN and your on-premises network. Notice that you do not yet create the route table that will be associated with the DRG attachment. That comes in a later step. For more information and instructions:

- FastConnect on page 3173
- VPN Connect on page 2932
- Dynamic Routing Gateways (DRGs) on page 2927

**Important:**

If you're using VPN Connect with static routing, and you've configured the VCN to give your on-premises network private access to Oracle services, you must configure your edge device with the routes for the Oracle Services Network public IP ranges that are advertised by the DRG over the private path (through the service gateway). For a list of those ranges, see Public IP Addresses for VCNs and the Oracle Services Network on page 193.

Task 4: Set up the private IPs on an instance in the VCN

In this task, you set up the instance to have 2 private IPs. Prerequisites:

- You already have a VCN with two subnets.
- Review this information: Using a Private IP as a Route Target on page 2924.

1. If you haven't already, create the instance in the VCN. See Creating an Instance on page 695. The primary VNIC is created in the subnet you specify.
2. Create a secondary VNIC for the other subnet and configure the OS to use it. See Using the Console on page 2858.
3. Disable the source/destination check on each of the VNICs. See Overview of VNICs and Physical NICs on page 2856.
4. For each VNIC, determine which private IP you want to use as the routing target. If you want to use a secondary private IP instead of the VNIC's primary private IP, assign that secondary private IP and configure the OS to use it. See Using the Console on page 2866.

5. For each of the private IPs you created, record the private IP address (for example: 10.0.4.3).

6. Configure the instance as necessary for the job it will perform (for example, configure the firewall or intrusion detection system on the instance).

Task 5: Set up ingress routing for the DRG and service gateway

In this task, you set up the route tables for the DRG attachment and service gateway.

Prerequisites:
- You already have a DRG attached to the VCN.
- You already have a service gateway.
- You already have the 2 private IPs to use as the routing targets (see the preceding task).

1. Create a route table for the DRG attachment:
   a. In the Console, view the VCN's details.
   b. Under Resources, click Route Tables to view the VCN's route tables.
   c. Click Create Route Table.
   d. Enter the following:
      - Name: A descriptive name for the route table. Example: DRG Route Table. Avoid entering confidential information.
      - Create in Compartment: Leave as is.
   e. Click + Additional Route Rule, and enter this information for the route rule:
      - Target Type: Private IP.
      - Destination: Service.
      - Destination Service: All <region> Services in Oracle Services Network
      - Compartment: The compartment where the frontend subnet's private IP is located.
      - Target: The frontend subnet's private IP, which you recorded in the previous task (10.0.4.3 in the example).
      - Description: An optional description of the rule.
   f. Click Create Route Table.

The route table is created and displayed in the list.
2. Associate the route table (called DRG Route Table in this example) with the VCN's DRG attachment:
   a. While still viewing the VCN's details, click Dynamic Routing Gateways to view the attached DRG.
   b. Click the Actions icon (three dots), and then click Associate Route Table.
   c. Select the route table.
   d. Click Associate Route Table.

   The route table is associated with the DRG attachment.

3. Create a route table for the service gateway:
   a. While still viewing the VCN's details, click Route Tables.
   b. Click Create Route Table.
   c. Enter the following:
      • Create in Compartment: Leave as is.
      • Name: A descriptive name for the route table. Example: Service Gateway Route Table. Avoid entering confidential information.
   d. Click + Additional Route Rule, and enter this information for the route rule:
      • Target Type: Private IP.
      • Destination: CIDR Block.
      • Destination CIDR Block: The on-premises network's CIDR (172.16.0.0/12 in the earlier example).
      • Compartment: The compartment where the private IP is located.
      • Target: The backend subnet's private IP, which you recorded in the previous task (10.0.8.3 in the example).
      • Description: An optional description of the rule.
   e. Click Create Route Table.

   The route table is created and displayed in the list.

4. Associate the route table (called Service Gateway Route Table in this example) with the service gateway:
   a. While still viewing the VCN's details, click Service Gateways.
   b. For the service gateway, click the Actions icon (three dots), and then click Associate With Route Table.
   c. Enter the following:
      • Route Table Compartment: Select the compartment of the route table for the service gateway.
      • Route Table: Select the route table for the service gateway.
   d. Click Associate.

   The route table is associated with the service gateway.

Turning Off Transit Routing

To turn off transit routing, remove the rules from:

• The route table associated with the DRG attachment.
• The route table associated with service gateway.

A route table can be associated with a resource but have no rules. Without at least one rule, a route table does nothing.

A DRG attachment or service gateway can exist without a route table associated with it. However, after you associate a route table with a DRG attachment or service gateway, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

FastConnect with Multiple DRGs and VCNs

This topic summarizes an advanced networking scenario that enables communication between an on-premises network and multiple virtual cloud networks (VCNs) over a single Oracle Cloud Infrastructure FastConnect. Each VCN has its own dynamic routing gateway (DRG), and you set up a separate FastConnect private virtual circuit to each DRG.
This scenario is supported for only certain FastConnect setups:

- Using a third-party provider or a Colocation with Oracle in a FastConnect location is fully supported.
- Using multiple DRGs and VCNs with an Oracle partner depends on your partner's support of this feature. Some partners also provide alternative solutions to achieve the same goal, so check with your chosen Oracle partner for details.

There's a scenario called transit routing that also involves using multiple VCNs, but only a single DRG. It can be used with VPN Connect or FastConnect. It involves setting up the VCNs in a hub-and-spoke layout and using the hub VCN for transit routing of traffic to the other VCNs. You might use this scenario if you need multiple VCNs for different parts of your organization, but you want to use one VCN for centralized services that all parts of the organization need. For more information, see Transit Routing: Access to Multiple VCNs in the Same Region on page 2780.

Highlights

- You can use a single FastConnect to connect your on-premises network with multiple VCNs in the same region. The scenario is supported only for FastConnect through a third-party provider or through colocation with Oracle. You need at least one physical connection (cross-connect) in your connection.
- The VCNs must be in the same region and same tenancy. The VCNs can be in the same compartment or different ones in the tenancy. For accurate routing, the CIDR blocks of the various subnets of interest in the on-premises network and VCNs must not overlap.
- Each VCN has its own dynamic routing gateway (DRG) and private virtual circuit. You must use a different VLAN and different set of BGP IP addresses for each private virtual circuit.
- You can also use FastConnect public peering to give your on-premises network access to public endpoints of Oracle services. In this case, you set up a single public virtual circuit, which covers all the VCNs. With public peering, configure your edge device (also known as your customer-premises equipment or CPE) to prefer FastConnect over your ISP for the Oracle Cloud Infrastructure public IP prefixes. Or, if you plan to also set up private access to Oracle services through one of the VCNs, see the important routing details in Routing Details for Connections to Your On-Premises Network on page 2942.

Overview of the Scenario

In this scenario, you have a single FastConnect that connects your existing on-premises network to Oracle Cloud Infrastructure. That FastConnect has at least one physical connection, or cross-connect.

In Oracle Cloud Infrastructure, you have multiple VCNs, all in the same region. Each VCN has its own DRG. For each VCN, there's a private virtual circuit that runs on the FastConnect and terminates at your CPE on one end, and on the VCN's DRG on the other end. The private virtual circuit enables communication that uses private IP addresses between the VCN and the on-premises network. See the following diagram.
For example, imagine that each department in your organization has its own subnet in your on-premises network and a corresponding departmental VCN in Oracle Cloud Infrastructure. You want to enable private communication between each department's subnet and VCN over the FastConnect.

Or, perhaps all the departments need to communicate with all the VCNs. For example, instead perhaps the VCNs are for separate development, test, and production environments, and each department needs access to all three VCNs.

The FastConnect and virtual circuits give you the general private connection where none of the traffic traverses the internet. You can separately control which on-premises subnets and VCNs can communicate by configuring route rules in your on-premises network and VCN route tables. You can optionally configure VCN security rules and other firewalls that you maintain to allow only certain types of traffic (such as SSH) between your on-premises network and VCN.

Public Peering

You can also set up public peering on that same FastConnect by creating a public virtual circuit. In the following diagram, the public virtual circuit is shown separate from the private virtual circuits. It terminates at Oracle's edge. The public virtual circuit enables communication that uses public IP addresses but does not traverse the internet. If a given VCN happens to also have an internet gateway, Oracle's edge prefers the FastConnect route over the VCN's internet gateway. For other important details about how you can control route preferences when you have multiple connections between your on-premises network and Oracle, see Routing Details for Connections to Your On-Premises Network on page 2942.
When you set up public peering for your FastConnect, the public IP prefixes that you designate for the public virtual circuit are advertised to all the VCNs in your tenancy. The routes advertised to your on-premises network are all the Oracle Cloud Infrastructure public IP addresses (including the CIDRs for each of the VCNs in the tenancy).

**Important:**

Your network receives Oracle's public IP addresses through both FastConnect and your Internet Service Provider (ISP). When configuring your edge, give higher preference to FastConnect over your ISP, or you will not receive the benefits of FastConnect. If you plan to also set up private access to Oracle services through one of the VCNs, see the important routing details in Routing Details for Connections to Your On-Premises Network on page 2942.

For more information, see Basic Network Diagrams on page 3176.

**General Setup Process**

The setup process and instructions are in these topics, based on your particular FastConnect setup:

- FastConnect: With a Third-Party Provider on page 3200
- FastConnect: Colocation with Oracle on page 3210

However, remember that:
• You set up a separate DRG for each VCN. A DRG can be attached to only a single VCN, and each VCN can be attached to only a single DRG.
• You set up a separate private virtual circuit for each DRG.
• For each private virtual circuit, you must specify a different VLAN and a different set of BGP IP addresses.
• When you configure your CPE, you can advertise the same on-premises routes to each VCN, or different ones, based on your own requirements.

Virtual Networking Quickstart

To make it easier to set up a virtual cloud network (VCN) and connect to it, the Console has the following wizards that walk you through network setup.

VCN with Internet Connectivity

What this wizard does:

• Creates a VCN.
• Creates an internet gateway, NAT gateway, and service gateway for the VCN.
• Creates a regional public subnet with routing to the internet gateway. Instances in a public subnet may optionally have public IP addresses.
• Creates a regional private subnet with routing to the NAT gateway and service gateway (and therefore the Oracle Services Network). Instances in a private subnet cannot have public IP addresses.
• Sets up basic security list rules for the two subnets, including SSH access.

Notice that this wizard does not support the creation of a VCN with IPv6 addresses. Also be aware that IPv6 addressing is currently supported only in the US Government Cloud. See For All US Government Cloud Customers on page 148.

Where to access this wizard:

Option 1:
1. In the Console, click the Oracle Cloud icon at the top of the page to go to the Console home page. The page has a Quick Actions section to take you directly to common tasks.
2. Click the quick action for Networking: Set up a network with a wizard.
3. Select VCN with Internet Connectivity, and then click Start Workflow.

Option 2:
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click Networking Quickstart.
3. Select VCN with Internet Connectivity, and then click Start Workflow.

VCN with VPN Connect and Internet Connectivity

What this wizard does:

• Creates a VCN.
• Creates an internet gateway for the VCN.
• Creates a regional public subnet with access to the internet gateway. Instances in a public subnet may optionally have public IP addresses.
• Sets up basic security list rules for the subnet, including SSH access.
• Sets up all the Networking service resources required for a VPN Connect between the VCN and your on-premises network.

Notice that this wizard does not support the creation of a VCN with IPv6 addresses. Also be aware that IPv6 addressing is currently supported only in the Government Cloud. See For All US Government Cloud Customers on page 148.
Networking

**Note:**

For the IPSec connection to work, your network engineer must also configure the customer-premises equipment (CPE) in your edge network.

More information about this wizard: VPN Connect Quickstart on page 2939

Where to access this wizard:

Option 1:

1. In the Console, click the **Oracle Cloud** icon at the top of the page to go to the Console home page.
   
   The page has a **Quick Actions** section to take you directly to common tasks.
2. Click the quick action for **Networking: Set up a network with a wizard**.
3. Select **VCN with VPN Connect and Internet Connectivity**, and then click **Start Workflow**.

Option 2:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click **Networking Quickstart**.
3. Select **VCN with VPN Connect and Internet Connectivity**, and then click **Start Workflow**.

**VCNs and Subnets**

A virtual cloud network (VCN) is a customizable and private network set up in Oracle Cloud Infrastructure.

Create a service request Ask the community

VCN and Subnet Overview

- Get a high-level overview of VCNs and subnets.

Create a peering connection

- Connect multiple VCNs to each other.

Enable transit routing

- Connect your on-premises network to Oracle resources.

Troubleshoot VCN issues

- Troubleshoot common issues and error messages.
Networking

Features

Customizable Virtual Cloud Networks
Fully configurable IP addresses, subnets, routing, and firewalls support new or existing private networks.

End-to-End Security
Multiple security layers, encryption, and private connectivity to other networks and critical Oracle services.

Highest Performance
High bandwidth, microsecond latency network enables high performance and big data applications with networked storage.

Highest Availability
Active and passive logical and physical network redundancy, including default redundant IPSec VPN connectivity.

Overview of VCNs and Subnets

This topic describes how to manage virtual cloud networks (VCNs) and the subnets in them. This topic uses the terms virtual cloud network, VCN, and cloud network interchangeably. The Console uses the term Virtual Cloud Network, whereas for brevity the API uses VCN.

A VCN is a software-defined network that you set up in the Oracle Cloud Infrastructure data centers in a particular region. A subnet is a subdivision of a VCN. For an overview of VCNs, allowed size, default VCN components, and scenarios for using a VCN, see Networking Overview on page 2748.

A VCN can have multiple non-overlapping CIDR blocks that you can change after you create the VCN. Regardless of the number of CIDR blocks, the max number of private IPs you can create within the VCN is 64,000.

You can privately connect a VCN to another VCN so that the traffic does not traverse the internet. The CIDRs for the two VCNs must not overlap. For more information, see Access to Other VCNs: Peering on page 3265. For an example of an advanced routing scenario that involves the peering of multiple VCNs, see Transit Routing: Access to Multiple VCNs in the Same Region on page 2780.

Each subnet in a VCN consists of a contiguous range of IPv4 addresses that do not overlap with other subnets in the VCN. Example: 172.16.1.0/24. The first two IPv4 addresses and the last in the subnet's CIDR are reserved by the Networking service. You can change the size of the subnet after creation.

Subnets act as a unit of configuration: all instances in a given subnet use the same route table, security lists, and DHCP options. For more information, see Default Components that Come With Your VCN on page 2751.

Subnets can be either public or private (see Public vs. Private Subnets on page 2752). The choice of public or private happens during subnet creation, and you can't change it later.

You can think of each Compute instance as residing in a subnet. But to be precise, each instance is attached to a virtual network interface card (VNIC), which in turn resides in the subnet and enables a network connection for that instance.

IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

About Regional Subnets

Originally subnets were designed to cover only one availability domain (AD) in a region. They were all AD-specific, which means the subnet's resources were required to reside in a particular availability domain. Now subnets can be either AD-specific or regional. You choose the type when you create the subnet. Both types of subnets can co-exist in the same VCN. In the following diagram, subnets 1-3 are AD-specific, and subnet 4 is regional.
Aside from the removal of the AD constraint, regional subnets behave the same as AD-specific subnets. **Oracle recommends using regional subnets** because they're more flexible. They make it easier to efficiently divide your VCN into subnets while also designing for availability domain failure.

When you create a resource such as a Compute instance, you choose which availability domain the resource will be in. From a virtual networking standpoint, you must also choose which VCN and subnet the instance will be in. You can either choose a regional subnet, or choose an AD-specific subnet that matches the AD you chose for the instance.

**Caution:**

If anyone in your organization implements a regional subnet, be aware that you **may need to update any client code that works with Networking service subnets and private IPs**. There are possible breaking API changes. For more information, see the [regional subnet release note](#).
Working with VCNs and Subnets

One of the first things you do when working with Oracle Cloud Infrastructure resources is create a VCN with one or more subnets. You can easily get started in the Console with a simple VCN and some related resources that enable you to launch and connect to an instance. See Tutorial - Launching Your First Linux Instance on page 61 or Tutorial - Launching Your First Windows Instance on page 73.

For the purposes of access control, when you create a VCN or subnet, you must specify the compartment where you want the resource to reside. Consult an administrator in your organization if you're not sure which compartment to use.

You may optionally assign descriptive names to the VCN and its subnets. The names don't have to be unique, and you can change them later. Oracle automatically assigns each resource a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

You can also add a DNS label for the VCN and each subnet, which are required if you want the instances to use the Internet and VCN Resolver feature for DNS in the VCN. For more information, see DNS in Your Virtual Cloud Network on page 2910.

When you create a subnet, you may optionally specify a route table for the subnet to use. If you don't, the subnet uses the cloud network's default route table. You can change which route table the subnet uses at any time.

Also, you may optionally specify one or more security lists for the subnet to use (up to five). If you don't specify any, the subnet uses the cloud network's default security list. You can change which security list the subnet uses at any time. Remember that the security rules are enforced at the instance level, even though the list is associated at the subnet level. Network security groups are an alternative to security lists and let you apply a set of security rules to a set of resources that all have the same security posture, instead of all the resources in a particular subnet.

You may optionally specify a set of DHCP options for the subnet to use. All instances in the subnet receive the configuration specified in that set of DHCP options. If you don't specify a set, the subnet uses the cloud network's default set of DHCP options. You can change which set of DHCP options the subnet uses at any time.

To delete a subnet, it must contain no resources (no instances, load balancers, DB systems, and orphaned mount targets). For more details, see Subnet or VCN Deletion on page 3334.

To delete a VCN, its subnets must contain no resources. Also, the VCN must have no attached gateways. If you're using the Console, there's a “Delete All” process you can use after first ensuring the subnets are empty. See To delete a VCN on page 2828.

For information about the number of VCNs and subnets you can have, see Service Limits on page 215.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

Security Zones

Security Zones ensure that your cloud resources comply with Oracle security principles. If any operation on a resource in a security zone compartment violates a policy for that security zone, then the operation is denied.

The following security zone policies affect your ability to manage VCNs and subnets:

- Subnets in a security zone can’t be public. All subnets must be private.
- You can’t move a subnet from a security zone to a standard compartment.

Using the Console
To create a VCN

**Note:**
The following procedure creates a VCN without any subnets or gateways for access. You must manually create the subnets and other resources before you can use the VCN. For a quick procedure that creates a VCN that you can try out immediately (that is, with subnets and an internet gateway), see the information about the "VCN with Internet Connectivity" wizard in Virtual Networking Quickstart on page 2820. Or see Scenario A: Public Subnet on page 2756.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.
3. Click Create Virtual Cloud Network.
4. Enter the following:
   - **Name:** A descriptive name for the VCN. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in Compartment:** Leave as is.
   - **CIDR Blocks:** One or more non-overlapping CIDR blocks for the VCN. For example: 172.16.0.0/16. You can add or remove CIDR blocks later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a [CIDR calculator](#).
   - **Enable IPv6 Address Assignment:** This option is available only if the VCN is in the Government Cloud. For more information, see IPv6 Addresses on page 2889.
   - **Use DNS Hostnames in this VCN:** Required for assignment of DNS hostnames to hosts in the VCN, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the VCN (VCN DNS label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click Create Virtual Cloud Network.

The VCN is then created and displayed on the Virtual Cloud Networks page in the compartment you chose.

Next you'll typically want to create one or more subnets in the cloud network.

To create a subnet

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click Create Subnet.
4. In the Create Subnet dialog box, you specify the resources to associate with the subnet (for example, a route table). By default, the subnet is created in the current compartment, and you choose the resources from the same
Networking

compartment. Click the click here link in the dialog box if you want to enable compartment selection for the subnet and each of those resources.

Enter the following:

- **Create in Compartment:** If you've enabled compartment selection, specify the compartment where you want to put the subnet.
- **Name:** A friendly name for the subnet. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
- **Regional or AD-specific subnet:** Oracle recommends creating only regional subnets, which means that the subnet can contain resources in any of the region's availability domains. If you instead choose Availability Domain-Specific (the only type of subnet that Oracle originally offered), you must also specify an availability domain. This choice means that any instances or other resources later created in this subnet must also be in that availability domain.
- **CIDR Block:** A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). Ensure that it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You can change the size of this CIDR block later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.
- **Enable IPv6 Address Assignment:** This option is available only if the VCN is in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.
- **Route Table:** The route table to associate with the subnet. If you've enabled compartment selection, under Route Table Compartment, you must specify the compartment that contains the route table.
- **Private or public subnet:** This controls whether VNICs in the subnet can have public IP addresses. For more information, see Access to the Internet on page 2752.
- **Use DNS Hostnames in this Subnet:** This option is available only if you provided a DNS label for the VCN during creation. The option is required for assignment of DNS hostnames to hosts in the subnet, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the subnet, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the subnet (<subnet_DNS_label>.<VCN_DNS_label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.
- **DHCP Options:** The set of DHCP options to associate with the subnet. If you've enabled compartment selection, under DHCP Options Compartment, you must specify the compartment that contains the set of DHCP options.
- **Security Lists:** One or more security lists to associate with the subnet. If you've enabled compartment selection, you must specify the compartment that contains the security list.
- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Create. The subnet is then created and displayed on the Subnets page in the compartment you chose.

*To edit a subnet*

You can change these characteristics of a subnet:

- **Name**
- **Size of the CIDR block**

**Note:**

- The CIDR block IP range you specify must be completely within one of the VCN's CIDR block ranges.
- The new range must use the same network address as the previous range. For example, the previous and new ranges could be 10.0.0.0/25 and 10.0.0.0/24.
• If you are reducing the CIDR range, ensure that no IP addresses outside of the reduced range are in use.
• The new CIDR range's broadcast address (last IP address of CIDR range) must not be an IP address in use in the previous CIDR range.
• You cannot create VNICs or private IPs for this subnet while a CIDR block update is in progress.
• After the CIDR block update is complete, the DHCP lease for each host within the subnet must be renewed. Renewal happens automatically within 24 hours. To renew the lease immediately, refer to the applicable operating system documentation for guidance on how to renew the lease manually.
• Ensure that you adjust your secondary VNICs and secondary IPs as applicable to match your updated VCN configuration.

- Which set of DHCP options the subnet uses
- Which route table the subnet uses
- Which security lists the subnet uses

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click **Subnets**.
4. Click the subnet you're interested in.
5. Click **Edit**.
7. Click **Save Changes**.

   The changes take effect within a few seconds.

To delete a subnet

Prerequisite: The subnet must have no instances, load balancers, DB systems, and orphaned mount targets in it. For more information, see **Subnet or VCN Deletion** on page 3334.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click **Subnets**.
4. Click the subnet you're interested in.
5. Click **Terminate**.
6. Confirm when prompted.

If the subnet is empty, its state changes to TERMINATING briefly and then TERMINATED. If the subnet is not empty, you get an error indicating that there are still instances or other resources in it that you must delete first.

To add a CIDR block to a VCN

- The CIDR block you add must not overlap with any other CIDR block in the VCN or in a peered VCN.
- The new CIDR block must not include an IP address used in an existing route rule.
- You cannot create or update the VCN's subnets, VLANs, LPGs, or route tables while this VCN update is in progress.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click **CIDR Blocks**.
4. Click **Add CIDR Block**.
5. Enter the value of the CIDR block you want to add to the VCN.
6. Click **Add CIDR Block**.

   The VCN's state changes to UPDATING. The time to completion can take a few minutes. You can view work requests to monitor the status of the update.
To change a VCN CIDR block

- The CIDR block range you specify must not overlap with any other CIDR block in this VCN or in a peered VCN.
- You cannot change the CIDR block to a range that excludes an IP address in use in the current CIDR block range.
- You cannot create or update the VCN's subnets, VLANs, LPGs, or route tables while this VCN update is in progress.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click CIDR Blocks.
4. Find the CIDR block in the list, click the Actions icon (three dots), and then click Edit CIDR Block.
5. Make the applicable change.
6. Click Save Changes.

The VCN’s state changes to UPDATING. The time to completion can vary depending on the size of your network. Updating a small network could take about a minute, and updating a large network could take up to an hour. You can view work requests to monitor the status of the update.

To remove a CIDR block from a VCN

- You cannot remove a CIDR block if an IP address in that range is in use.
- You cannot create or update the VCN's subnets, VLANs, LPGs, or route tables while this VCN update is in progress.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click CIDR Blocks.
4. Find the CIDR block in the list, click the Actions icon (three dots), and then click Remove CIDR Block.
5. Click Remove CIDR Block.

The VCN’s state changes to UPDATING. The time to completion can vary depending on the size of your network. Updating a small network could take about a minute, and updating a large network could take up to an hour. You can view work requests to monitor the status of the update.

To delete a VCN

Important:

The Console has an easy "Delete all" process that deletes a VCN and its related Networking resources (subnets, route tables, security lists, sets of DHCP options, internet gateway, and so on). If the VCN is attached to a dynamic routing gateway (DRG), the attachment is deleted, but the DRG remains.

The "Delete All" process deletes one resource at a time and takes a minute or two. A progress report is displayed to show you what's been deleted so far.

Before using the "Delete All" process, verify there are no instances, load balancers, DB systems, or orphaned mount targets in any of the subnets. For more information, see Subnet or VCN Deletion on page 3334.

If there are still resources in any subnet, or if you don't have permission to delete a particular Networking resource, the "Delete All" process stops and an error message is displayed. Any resources deleted up to that point cannot be restored. You might need to contact your tenancy administrator to help you delete any remaining resources.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click **Terminate**.
   The resulting dialog box displays a list of the resources to be deleted. The list doesn't include the default components that come with the VCN, but they are deleted along with the VCN.

4. Click **Delete All**.
   The process begins. The progress is displayed as each resource is deleted.

5. When the process is complete, click **Close**.

---

### To manage tags for a VCN

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click the **Tags** tab to view or edit the existing tags. Or click **Apply tag(s)** to add new ones.

For more information, see **Resource Tags** on page 211.

### To manage tags for a subnet

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click the subnet you're interested in.
4. Click the **Tags** tab to view or edit the existing tags. Or click **Apply tag(s)** to add new ones.

For more information, see **Resource Tags** on page 211.

### To move a VCN to a different compartment

You can move a VCN from one compartment to another. When you move a VCN, its associated VNICs, private IPs, and ephemeral IPs move with it to the new compartment. For more information, see **To move a resource to a different compartment** on page 2444.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Find the VCN in the list, click the Actions icon (three dots), and then click **Move Resource**.
3. Choose the destination compartment from the list.
4. Click **Move Resource**.
5. If there are alarms monitoring the VCN, update the alarms to reference the new compartment. See **To update an alarm after moving a resource** on page 2737 for more information.

### To move a subnet to a different compartment

You can move a subnet from one compartment to another. For more information, see **Working with Compartments** on page 2432.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Find the subnet in the list, click the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

### Using the API

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

To manage your VCNs, use these operations:

- `ListVcns`
- `CreateVcn`
- `GetVcn`
- `UpdateVcn`
- `AddVcnCidr`
- `ModifyVcnCidr`
Networking

- **RemoveVcnCidr**
- **DeleteVcn**: Deletes only the VCN and not its related resources. For more information, see Subnet or VCN Deletion on page 3334. Note that the Console offers a “Delete All” process that makes it easy to delete the VCN and its related resources. See To delete a VCN on page 2828.
- **ChangeVcnCompartment**

To manage a VCN's subnets, use these operations:

- ListSubnets
- CreateSubnet
- GetSubnet
- UpdateSubnet
- DeleteSubnet
- ChangeSubnetCompartment

Access and Security

See these topics for more information about access and security in your cloud network:

- **Ways to Secure Your Network** on page 2830
- **Access Control** on page 2831
- **Virtual firewall for your VCN**:
  - **Security Rules** on page 2833
  - **Network Security Groups** on page 2841
  - **Security Lists** on page 2850

**Ways to Secure Your Network**

There are several ways you can control security for your cloud network and compute instances:

- **Public versus private subnets**: You can designate a subnet to be private, which means instances in the subnet cannot have public IP addresses. For more information, see Public vs. Private Subnets on page 2752.
- **Security rules**: To control packet-level traffic in and out of an instance. You configure security rules in the Oracle Cloud Infrastructure API or Console. To implement security rules, you can use network security groups or security lists. For more information, see Security Rules on page 2833.
- **Firewall rules**: To control packet-level traffic in/out of an instance. You configure firewall rules directly on the instance itself. Notice that Oracle Cloud Infrastructure images that run Oracle Linux automatically include default rules that allow ingress on TCP port 22 for SSH traffic. Also, the Windows images include default rules that allow ingress on TCP port 3389 for Remote Desktop access. For more information, see Oracle-Provided Images on page 629.

**Important:**

Firewall rules and security rules both operate at the instance level. However, you configure security lists at the subnet level, which means all resources in a given subnet have the same set of security list rules. Also, the security rules in a network security group apply only to the resources in the group. When troubleshooting access to an instance, ensure that all the following items are set correctly: the network security groups that the instance is in, the security lists associated with the instance's subnet, and the instance's firewall rules.

If your instance is running Oracle Autonomous Linux 7, Oracle Linux 8, or Oracle Linux 7, you need to use `firewalld` to interact with the `iptables` rules.
Networking rules. For your reference, here are commands for opening a port (1521 in this example):

```
sudo firewall-cmd --zone=public --permanent --add-port=1521/tcp
sudo firewall-cmd --reload
```

For instances with an iSCSI boot volume, the preceding `--reload` command can cause problems. For details and a workaround, see Instances experience system hang after running firewall-cmd --reload.

- **Gateways and route tables**: To control general traffic flow from your cloud network to outside destinations (the internet, your on-premises network, or another VCN). You configure your cloud network's gateways and route tables in the Oracle Cloud Infrastructure API or Console. For more information about the gateways, see Networking Components on page 2748. For more information about route tables, see Route Tables on page 2921.

- **IAM policies**: To control who has access to the Oracle Cloud Infrastructure API or Console itself. You can control the type of access, and which cloud resources can be accessed. For example, you can control who can set up your network and subnets, or who can update route tables, network security groups, or security lists. You configure policies in the Oracle Cloud Infrastructure API or Console. For more information, see Access Control on page 2831.

- **Security zones**: To ensure that your network and other cloud resources comply with Oracle security principles and best practices, you can create them in a security zone. A security zone is associated with a compartment and checks all network management operations against security zone policies. For example, a security zone does not permit the use of public IP addresses and can contain only private subnets. For more information, see Security Zones.

## Access Control

This topic gives basic information about using **compartments** and IAM **policies** to control access to your cloud network.

### Compartments and Your Cloud Network

Anytime you create a cloud resource such as a virtual cloud network (VCN) or compute instance, you must specify which IAM **compartment** you want the resource in. A compartment is a collection of related resources that can only be accessed by certain groups that have been given permission by an administrator in your organization. The administrator creates compartments and corresponding IAM policies to control which users in your organization access which compartments. Ultimately, the goal is to ensure that each person can only access the resources they need.

If your company is starting to try out Oracle Cloud Infrastructure, only a few people need to create and manage the VCN and its components, launch instances into the VCN, and attach block storage volumes to those instances. Those few people need access to **all** these resources, so all those resources could be in the same compartment.

In an enterprise production environment with a VCN, your company can use multiple compartments to more easily control access to certain types of resources. For example, your administrator could create Compartment_A for your VCN and other networking components. The administrator could then create Compartment_B for all the compute instances and block storage volumes that the HR organization uses, and Compartment_C for all the instances and block storage volumes that the Marketing organization uses. The administrator would then create IAM policies that give users only the level of access they need in each compartment. For example, the HR instance administrator is not entitled to modify the existing cloud network. So they would have full permissions for Compartment_B, but limited access to Compartment_A (just what's required to launch instances into the network). If they tried to modify other resources in Compartment_A, the request would be denied.

Network resources such as VCNs, subnets, route tables, security lists, service gateways, NAT gateways, VPNs, and FastConnect connections can be moved from one compartment to another. When you move a resource to a new compartment, inherent policies apply immediately.
For more information about compartments and how to control access to your cloud resources, see "Setting Up Your Tenancy" in the Oracle Cloud Infrastructure Getting Started Guide and Overview of Oracle Cloud Infrastructure Identity and Access Management on page 2124.

IAM Policies for Networking

The simplest approach to granting access to Networking is the policy listed in Let network admins manage a cloud network on page 2143. It covers the cloud network and all the other Networking components (subnets, security lists, route tables, gateways, and so on). To also give network admins the ability to launch instances (to test network connectivity), see Let users launch compute instances on page 2143.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For reference material for writing more detailed policies for Networking, see Details for the Core Services on page 2181.

Individual Resource-Types

If you'd like, you can write policies that focus on individual resource-types (for example, security lists only) instead of the broader virtual-network-family. The instance-family resource-type also includes several permissions for VNICS, which reside in a subnet but attach to an instance. For more information, see Details for Verb + Resource-Type Combinations on page 2183 and Virtual Network Interface Cards (VNICS) on page 2855.

There's a resource-type called local-peering-gateways that is included within virtual-network-family and includes two other resource-types related to local VCN peering (within region):

- local-peering-from
- local-peering-to

The local-peering-gateways resource-type covers all permissions related to local peering gateways (LPGs). The local-peering-from and local-peering-to resource-types are for granting permission to connect two LPGs and define a peering relationship within a single region. For more information, see Local VCN Peering (Within Region) on page 3267.

Similarly, there's a resource-type called remote-peering-connections that is included within virtual-network-family and includes two other resource-types related to remote VCN peering (across regions):

- remote-peering-from
- remote-peering-to

The remote-peering-connections resource-type covers all permissions related to remote peering connections (RPCs). The remote-peering-from and remote-peering-to resource-types are for granting permission to connect two RPCs and define a peering relationship across regions. For more information, see Remote VCN Peering (Across Regions) on page 3280.

Nuances of Different Verbs

If you'd like, you can write policies that limit the level of access by using a different policy verb (manage versus use, and so on). If you do, there are some nuances to understand about the policy verbs for Networking.

Be aware that the inspect verb not only returns general information about the cloud network's components (for example, the name and OCID of a security list, or of a route table). It also includes the contents of the component (for example, the actual rules in the security list, the routes in the route table, and so on).

Also, the following types of abilities are available only with the manage verb, not the use verb:

- Update (enable/disable) internet-gateways
- Update security-lists
- Update route-tables
- Update dhcp-options
- Attach a dynamic routing gateway (DRG) to a virtual cloud network (VCN)
- Create an IPSec connection between a DRG and customer-premises equipment (CPE)
• Peer VCNs

**Important:**

Each VCN has various components that directly affect the behavior of the network (route tables, security lists, DHCP options, Internet Gateway, and so on). When you create one of these components, you establish a relationship between that component and the VCN, which means you must be allowed in a policy to both create the component and manage the VCN itself. However, the ability to update that component (to change the route rules, security list rules, and so on) does NOT require permission to manage the VCN itself, even though changing that component can directly affect the behavior of the network. This discrepancy is designed to give you flexibility in granting least privilege to users, and not require you to grant excessive access to the VCN just so the user can manage other components of the network. Be aware that by giving someone the ability to update a particular type of component, you're implicitly trusting them with controlling the network's behavior.

For more information about policy verbs, see [Policy Basics on page 2137](#).

**Security Rules**

The Networking service offers two virtual firewall features that both use *security rules* to control traffic at the packet level. The two features are:

- **Security lists**: The original virtual firewall feature from the Networking service.
- **Network security groups (NSGs)**: A subsequent feature designed for application components that have different security postures. NSGs are supported only for specific services.

These two features offer different ways to apply security rules to a set of *virtual network interface cards (VNICs)* in the virtual cloud network (VCN).

This topic summarizes basic differences between the two features. It also explains important security rule concepts that you need to understand. How you create, manage, and apply security rules varies between security lists and network security groups. For implementation details, see these related topics:

- [Security Lists on page 2850](#)
- [Network Security Groups on page 2841](#)

**Comparison of Security Lists and Network Security Groups**

*Security lists* let you define a set of security rules that applies to all the VNICs in an entire subnet. To use a given security list with a particular subnet, you *associate* the security list with the subnet either during subnet creation or later. A subnet can be associated with a maximum of five security lists. Any VNICs that are created in that subnet are subject to the security lists associated with the subnet.

*Network security groups* (NSGs) let you define a set of security rules that applies to a *group of VNICs of your choice* (or the VNICs' parent resources such as load balancers or DB systems). For example: the VNICs that belong to a set of Compute instances that all have the same security posture. To use a given NSG, you add the VNICs of interest to the group. Any VNICs added to that group are subject to that group's security rules. A VNIC can be added to a maximum of five NSGs.

The following diagram illustrates the concept.
Oracle recommends using NSGs instead of security lists because NSGs let you separate the VCN's subnet architecture from your application security requirements.

However, you can use both security lists and NSGs together if you want. For more information, see If You Use Both Security Lists and Network Security Groups on page 2837.

About VNICs and Parent Resources

A VNIC is a Networking service component that enables a networked resource such as a Compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN.

When you create a Compute instance, a VNIC is automatically created for the instance in the instance's subnet. The instance is considered to be the parent resource for the VNIC. You can add more (secondary) VNICs to a Compute instance. For this reason, an instance's VNICs are displayed prominently as part of a Compute instance's related resources in the Console.

There are other types of parent resources that you can create that also result in a VNIC automatically being created. For example: when you create a load balancer, the Load Balancing service automatically creates VNICs for balancing traffic across the backend set. Also, when you create a DB system, the Database service automatically creates VNICs as DB system nodes. Those services create and manage those VNICs for you. For this reason, those VNICs are not readily apparent in the Console the same way VNICs are for Compute instances.

To use an NSG, you put VNICs of your choice into the group. However, you typically work with the parent resource when you add a VNIC to the group, not the VNIC itself. For example, when you create a Compute instance, you can optionally specify an NSG for the instance. Although you conceptually put the instance in the group, you're actually putting the instance's primary VNIC in the network security group. The group's security rules apply to that VNIC, not the instance. Also, if you add a secondary VNIC to the instance, you can optionally specify an NSG for that VNIC, and the rules apply to that VNIC, not the instance. Note that all the VNICs in a given NSG must be in the VCN that the NSG belongs to.

Likewise, when you put a load balancer in a network security group, you conceptually put the load balancer in the group. But you're actually putting VNICs managed by the Load Balancing service into the network security group.

You manage the VNIC membership of an NSG at the parent resource, and not at the NSG itself. In other words, to add a parent resource to an NSG, you execute the action on the parent resource (by specifying which NSGs the parent resource should be added to). You do not execute the action on the NSG (by specifying which VNICs or parent resources should be added to the NSG). Similarly, to remove a VNIC from an NSG, you execute that action by updating the parent resource, not the NSG. For example, to add an existing Compute instance's VNIC to an NSG, you update that VNIC's properties and specify the NSG. For example, with the REST API, you call UpdateVnic. In the Console, you view the instance and then the VNIC of interest, and then edit the VNIC's properties there.

For a list of parent resources that support the use of NSGs, see Support for Network Security Groups on page 2842.
**Network Security Group as Source or Destination of a Rule**

There's an important difference in how you can write security rules for NSGs compared to security lists.

When writing rules for an NSG, you can specify an *NSG* as the source of traffic (for ingress rules) or the traffic's destination (for egress rules). Contrast this with security list rules, where you specify a *CIDR* as the source or destination.

The ability to specify an NSG means that you can easily write rules to control traffic between two different NSGs. The NSGs must be in the same VCN.

Also, if you want to control traffic between *VNICS in a specific NSG*, you can write rules that specify the *rule's own NSG* as the source (for ingress rules) or destination (for egress rules).

For more information, see [Overview of Network Security Groups](#) on page 2842.

**REST API Differences**

There are a few basic differences in the REST API model for NSGs compared to security lists. For more information, see [Using the API](#) on page 2849.

**Default Rules**

Your VCN automatically comes with a *default security list* that contains several default security rules to help you get started using the Networking service. When you create a subnet, the default security list is associated with the subnet unless you specify a custom security list that you've already created in the VCN. For comparison, the VCN does NOT have a default network security group.

**Limits**

The two features have different limits.

**Security List Limits**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security lists</td>
<td>VCN</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>Security lists</td>
<td>Subnet</td>
<td>5*</td>
<td>5*</td>
</tr>
<tr>
<td>Security rules</td>
<td>Security list</td>
<td>200 ingress rules* and 200 egress rules*</td>
<td>200 ingress rules* and 200 egress rules*</td>
</tr>
</tbody>
</table>

* Limit for this resource cannot be increased

**Network Security Group Limits**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Scope</th>
<th>Monthly or Annual Universal Credits</th>
<th>Pay-as-You-Go or Promo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network security groups</td>
<td>VCN</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Resource</td>
<td>Scope</td>
<td>Monthly or Annual Universal Credits</td>
<td>Pay-as-You-Go or Promo</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>VNICS</td>
<td>Network security group</td>
<td>A given network security group can have as many VNICS as are in the VCN. A given VNIC can belong to a maximum of 5 network security groups.*</td>
<td>A given network security group can have as many VNICS as are in the VCN. A given VNIC can belong to a maximum of 5 network security groups.*</td>
</tr>
<tr>
<td>Security rules</td>
<td>Network security group</td>
<td>120 (total ingress plus egress)</td>
<td>120 (total ingress plus egress)</td>
</tr>
</tbody>
</table>

* Limit for this resource cannot be increased

**Best Practices for Security Rules**

**Use Network Security Groups**

Oracle recommends using NSGs for components that all have the same security posture. For example, in a multi-tier architecture, you would have a separate NSG for each tier. A given tier's VNICS would all belong to that tier's NSG. Within a given tier, you might have a particular subset of the tier's VNICS that have additional, special security requirements. Therefore you would create another NSG for those additional rules, and place that subset of VNICS into both the tier's NSG and the additional NSG.

Oracle also recommends using NSGs because Oracle will prioritize NSGs over security lists when implementing future enhancements.

**Get Familiar with the Default Security List Rules**

Your VCN automatically comes with a default security list that contains several default security rules to help you get started using the Networking service. Those rules exist because they enable basic connectivity. Even if you choose not to use security lists or the default security list, get familiar with the rules so you better understand the types of traffic that your networked cloud resources require. You might want to use those rules in your NSGs or any custom security lists that you set up.

The default security list does not include rules to enable ping. If you need to use ping, see Rules to Enable Ping on page 2841.

**Don't Delete Default Security Rules Indiscriminately**

Your VCN might have subnets that use the default security list by default. Do not delete any of the list's default security rules unless you've first confirmed that resources in your VCN do not require them. Otherwise, you might disrupt your VCN's connectivity.

**Confirm That Your OS Firewall Rules Align with Your Security Rules**

Your instances running Oracle-provided Linux images or Windows images also have OS firewall rules that control access to the instance. When troubleshooting access to an instance, make sure that all of the following items are set correctly:

- The rules in the network security groups that the instance is in
- The rules in the security lists associated with the instance's subnet
- The instance's OS firewall rules

For more information, see Oracle-Provided Images on page 629.
If your instance is running Oracle Autonomous Linux 7, Oracle Linux 8, or Oracle Linux 7, you need to use `firewalld` to interact with the `iptables` rules. For your reference, here are commands for opening a port (1521 in this example):

```
sudo firewall-cmd --zone=public --permanent --add-port=1521/tcp
sudo firewall-cmd --reload
```

For instances with an iSCSI boot volume, the preceding `--reload` command can cause problems. For details and a workaround, see [Instances experience system hang after running firewall-cmd --reload](#).

**Use VNIC Metrics to Troubleshoot Packets Dropped Because of Security Rules**

The Networking service offers metrics for VNICs, which show the levels of VNIC traffic (packets and bytes). Two of the metrics are for ingress and egress packets that violate security rules and are therefore dropped. You can use these metrics to help you troubleshoot issues related to security rules and whether your VNICs are receiving the desired traffic.

**If You Use Both Security Lists and Network Security Groups**

You can use security lists alone, network security groups alone, or both together. It depends on your particular security needs.

If you have security rules that you want to enforce for all VNICs in a VCN: the easiest solution is to put the rules in one security list, and then associate that security list with all subnets in the VCN. This way you can ensure that the rules are applied, regardless of who in your organization creates a VNIC in the VCN. If you like, you can use the VCN's default security list, which automatically comes with the VCN and contains a set of essential rules by default.

If you choose to use both security lists and network security groups, the set of rules that applies to a given VNIC is the union of these items:

- The security rules in the security lists associated with the VNIC's subnet
- The security rules in all NSGs that the VNIC is in

The following diagram is a simple illustration of the idea.

![Diagram](#)

A packet in question is allowed if *any rule in any of the relevant lists and groups* allows the traffic (or if the traffic is part of an existing connection being tracked). There's a caveat if the lists happen to contain both stateful and stateless rules that cover the same traffic. For more information, see [Stateful Versus Stateless Rules](#) on page 2839.

**Parts of a Security Rule**

A security rule allows a particular type of traffic in or out of a VNIC. For example, a commonly used security rule allows ingress TCP port 22 traffic for establishing SSH connections to the instance (more specifically to the instance's VNICs). Without security rules, no traffic is allowed in and out of VNICs in the VCN.

**Note:**

Security rules are not enforced for traffic involving the 169.254.0.0/16 CIDR block, which includes services such as iSCSI and instance metadata.
Each security rule specifies the following items:

- **Direction (ingress or egress):** Ingress is inbound traffic to the VNIC, and egress is outbound traffic from the VNIC. The REST API model for security lists is different from network security groups. With security lists, there is an `IngressSecurityRule` object and a separate `EgressSecurityRule` object. With network security groups, there is only a `SecurityRule` object, and the object's `direction` attribute determines whether the rule is for ingress or egress traffic.

- **Stateful or stateless:** If stateful, connection tracking is used for traffic matching the rule. If stateless, no connection tracking is used. See Stateful Versus Stateless Rules on page 2839.

- **Source type and source (ingress rules only):** The source you provide for an ingress rule depends on the source type you choose.

  **Allowed source types**

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Allowed Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>The CIDR block where the traffic originates from. Use 0.0.0.0/0 to indicate all IP addresses. The prefix is required (for example, include the /32 if specifying an individual IP address).</td>
</tr>
<tr>
<td>Network Security Group</td>
<td>An NSG that is in the same VCN as this rule's NSG.</td>
</tr>
<tr>
<td></td>
<td>This source type is available only if the rule belongs to an NSG and not a security list.</td>
</tr>
<tr>
<td>Service</td>
<td>Only for packets coming from an Oracle service through a service gateway.</td>
</tr>
<tr>
<td></td>
<td>The source service is the service CIDR label that you're interested in.</td>
</tr>
</tbody>
</table>

- **Destination type and destination (egress rules only):** The destination you provide for an egress rule depends on the destination type you choose.

  **Allowed destination types**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Allowed Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>The CIDR block where the traffic is destined to. Use 0.0.0.0/0 to indicate all IP addresses. The prefix is required (for example, include the /32 if specifying an individual IP address).</td>
</tr>
<tr>
<td>Network Security Group</td>
<td>An NSG that is in the same VCN as this rule's NSG.</td>
</tr>
<tr>
<td></td>
<td>This destination type is available only if the rule belongs to an NSG and not a security list.</td>
</tr>
<tr>
<td>Service</td>
<td>Only for packets going to an Oracle service through a service gateway.</td>
</tr>
<tr>
<td></td>
<td>The destination service is the service CIDR label that you're interested in.</td>
</tr>
</tbody>
</table>

- **IP Protocol:** Either a single IPv4 protocol or "all" to cover all protocols.

- **Source port:** The port where the traffic originates from. For TCP or UDP, you can specify all source ports, or optionally specify a single source port number, or a range.

- **Destination port:** The port where the traffic is destined to. For TCP or UDP, you can specify all destination ports, or optionally specify a single destination port number, or a range.

- **ICMP type and code:** For ICMP, you can specify all types and codes, or optionally specify a single type with an optional code. If the type has multiple codes, create a separate rule for each code you want to allow.

- **Description** (NSG rules only): NSG security rules include an optional attribute where you can provide a friendly description of the rule. This is currently not supported for security list rules.

For examples of security rules, see Networking Scenarios on page 2756.

For the limit on the number of rules you can have, see Comparison of Security Lists and Network Security Groups on page 2833.
Note:

If you're using NSGs, and two VNICs that are in the same VCN need to communicate using their public IP addresses, you must use the VNIC's public IP address and not the VNIC's NSG as the source (for ingress) or destination (for egress) in the relevant security rules. The packet is routed to the VCN's internet gateway, and at that point, the VNIC's NSG information is not available. Therefore a security rule that specifies the NSG as the source or destination will be ineffective in allowing that specific type of traffic.

Stateful Versus Stateless Rules

When you create a security rule, you choose whether it's stateful or stateless. The difference is described in the next sections. The default is stateful. Stateless rules are recommended if you have a high-volume internet-facing website (for the HTTP/HTTPS traffic).

This section refers specifically to Compute instances and their traffic. However, the discussion is applicable to all types of resources with VNICs. See Comparison of Security Lists and Network Security Groups on page 2833.

Stateful Rules

Marking a security rule as stateful indicates that you want to use connection tracking for any traffic that matches that rule. This means that when an instance receives traffic matching the stateful ingress rule, the response is tracked and automatically allowed back to the originating host, regardless of any egress rules applicable to the instance. And when an instance sends traffic that matches a stateful egress rule, the incoming response is automatically allowed, regardless of any ingress rules. For more details, see Stateful Versus Stateless Rules on page 2839.

The figure below illustrates a stateful ingress rule for an instance that needs to receive and respond to HTTP traffic. Instance A and Host B are communicating (Host B could be any host, whether an instance or not). The stateful ingress rule allows traffic from any source IP address (0.0.0.0/0) to destination port 80 only (TCP protocol). No egress rule is required to allow the response traffic.

Stateful Security Rule: Receive HTTP Traffic

![Diagram showing stateful ingress rule](attachment://diagram.stateful_ingress.png)

Stateless Rules

Marking a security rule as stateless indicates that you do NOT want to use connection tracking for any traffic that matches that rule. This means that response traffic is not automatically allowed. To allow the response traffic for a stateless ingress rule, you must create a corresponding stateless egress rule.

![Diagram showing stateless rule](attachment://diagram.stateless.png)
The next figure shows Instance A and Host B as before, but now with stateless security rules. As with the stateful rule in the preceding section, the stateless ingress rule allows traffic from all IP addresses and any ports, on destination port 80 only (using the TCP protocol). To allow the response traffic, there needs to be a corresponding stateless egress rule that allows traffic to any destination IP address (0.0.0.0/0) and any ports, from source port 80 only (using the TCP protocol).

**Stateless Security Rule: Receive HTTP Traffic**

![Diagram showing stateless security rules for receiving HTTP traffic]

If Instance A needs instead to *initiate* HTTP traffic and get the response, then a different set of stateless rules are required. As the next figure shows, the egress rule would have source port = all and destination port = 80 (HTTP). The ingress rule would then have source port 80 and destination port = all.

**Stateless Security Rule: Initiate HTTP Traffic**

![Diagram showing stateless security rules for initiating HTTP traffic]

If you were to use port binding on Instance A to specify exactly which port the HTTP traffic would come from, you could specify that as the source port in the egress rule and the destination port in the ingress rule.
Note:
If for some reason you use both stateful and stateless rules, and there's traffic that matches both a stateful and stateless rule in a particular direction (for example, ingress), the stateless rule takes precedence and the connection is not tracked. You would need a corresponding rule in the other direction (for example, egress, either stateless or stateful) for the response traffic to be allowed.

Connection Tracking Details for Stateful Rules
Oracle uses connection tracking to allow responses for traffic that matches stateful rules (see Stateful Versus Stateless Rules on page 2839). Each instance has a maximum number of concurrent connections that can be tracked, based on the instance's shape.

To determine response traffic for TCP, UDP, and ICMP, Oracle performs connection tracking on these items for the packet:
- Protocol
- Source and destination IP addresses
- Source and destination ports (for TCP and UDP only)

Note:
For other protocols, Oracle tracks only the protocol and IP addresses, and not the ports. This means that when an instance initiates traffic to another host and that traffic is allowed by egress security rules, any traffic that the instance receives later from that host for a period is considered response traffic and is allowed.

Enabling Path MTU Discovery Messages for Stateless Rules
If you decide to use stateless security rules to allow traffic to/from endpoints outside the VCN, it's important to add a security rule that allows ingress ICMP traffic type 3 code 4 from source 0.0.0.0/0 and any source port. This rule enables your instances to receive Path MTU Discovery fragmentation messages. This rule is critical for establishing a connection to your instances. Without it, you can experience connectivity issues. For more information, see Hanging Connection on page 3327.

Rules to Enable Ping
The VCN's default security list contains several default rules, but not one to allow ping requests. If you want to ping an instance, ensure that the instance's applicable security lists or NSGs include an additional stateful ingress rule to specifically allow ICMP traffic type 8 from the source network you plan to ping from. To allow ping access from the internet, use 0.0.0.0/0 for the source. Note that this rule for pinging is separate from the default ICMP-related rules in the default security list. Do not remove those rules.

Rules to Handle Fragmented UDP Packets
Instances can send or receive UDP traffic. If a UDP packet is too large for the connection, it is fragmented. However, only the first fragment from the packet contains the protocol and port information. If the security rules that allow this ingress or egress traffic specify a particular port number (source or destination), the fragments after the first one are dropped. If you expect your instances to send or receive large UDP packets, set both the source and destination ports for the applicable security rules to ALL (instead of a particular port number).

Network Security Groups
The Networking service offers two virtual firewall features to control traffic at the packet level:
- **Network security groups**: Covered in this topic. Network security groups are supported only for specific services.
Networking

- **Security lists**: The original type of virtual firewall offered by the Networking service. See Security Lists on page 2850.

Both of these features use security rules. For important information about how security rules work, and a general comparison of security lists and network security groups, see Security Rules on page 2833.

**Highlights**

- Network security groups (NSGs) act as a virtual firewall for your Compute instances and other kinds of resources. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice in a single VCN (for example: all the Compute instances that act as web servers in the web tier of a multi-tier application in your VCN).
- Compared to security lists, NSGs let you separate your VCN's subnet architecture from your application security requirements. See Comparison of Security Lists and Network Security Groups on page 2833.
- You can use NSGs with certain resource types. For more information, see Support for Network Security Groups on page 2842.
- NSG security rules function the same as security list rules. However, for an NSG security rule's source (for ingress rules) or destination (for egress rules), you can specify an NSG instead of a CIDR. This means you can easily write security rules to control traffic between two NSGs in the same VCN, or traffic within a single NSG. See Parts of a Security Rule on page 2837.
- Unlike with security lists, the VCN does not have a default NSG. Also, each NSG you create is initially empty. It has no default security rules.
- Network security groups have separate and different limits compared to security lists. See Security List Limits on page 2835.

**Support for Network Security Groups**

NSGs are available for you to create and use. However, they are not yet supported by all the relevant Oracle Cloud Infrastructure services.

Currently, the following types of parent resources support the use of NSGs:

- **Compute instances**: When you create an instance, you can specify one or more NSGs for the instance's primary VNIC. If you add a secondary VNIC to an instance, you can specify one or more NSGs for that VNIC. You can also update existing VNICs on an instance so that they are in one or more NSGs.
- **Load balancers**: When you create a load balancer, you can specify one or more NSGs for the load balancer (not the backend set). You can also update an existing load balancer to use one or more NSGs.
- **DB systems**: When you create a DB system, you can specify one or more NSGs. You can also update an existing DB system to use one or more NSGs.
- **Autonomous Databases**: When you create an Autonomous Database on dedicated Exadata infrastructure, you can specify one or more NSGs for the infrastructure resource. You can also update an existing dedicated Exadata infrastructure instance to use NSGs.
- **Mount targets**: When you create a mount target for a file system, you can specify one or more NSGs. You can also update an existing mount target to use one or more NSGs.
- **DNS resolver endpoint**: When you create an endpoint for a private DNS resolver, you can specify one or more NSGs. You can also update an existing endpoint to use one or more NSGs.

For resource types that do not yet support NSGs, continue to use security lists to control traffic in and out of those parent resources.

**Overview of Network Security Groups**

A network security group (NSG) provides a virtual firewall for a set of cloud resources that all have the same security posture. For example: a group of Compute instances that all perform the same tasks and thus all need to use the same set of ports.

An NSG consists of two types of items (as illustrated in the following diagram):

- **VNICs**: One or more VNICs (for example, the VNICs attached to the set of Compute instances that all have the same security posture). All the VNICs must be in the VCN that the NSG belongs to. Also see Comparison of Security Lists and Network Security Groups on page 2833.
**Security rules:** Security rules that define the types of traffic allowed in and out of the VNICs in the group. For example: ingress TCP port 22 SSH traffic from a particular source.

If you have resources with different security postures in the same VCN, you can write NSG security rules to control traffic between the resources with one posture versus another. For example, in the following diagram, NSG1 has VNICs running in one tier of a multi-tier architecture application. NSG2 has VNICs running in a second tier. Both NSGs must belong to the same VCN. The assumption is that both NSGs need to initiate connections to the other NSG.

For NSG1, you set up egress security rules that specify NSG2 as the destination, and ingress security rules that specify NSG2 as the source. Likewise for NSG2, you set up egress security rules that specify NSG1 as the destination, and ingress security rules that specify NSG1 as the source. The rules are assumed to be stateful in this example.

The preceding diagram assumes that each NSG needs to initiate connections to the other NSG.

The next diagram assumes that you instead want to only allow connections initiated from NSG1 to NSG2. To do that, remove the ingress rule from NSG1 and the egress rule from NSG2. The remaining rules do not allow connections initiated from NSG2 to NSG1.
Networking

The next diagram assumes that you want to control traffic between VNICs in the same NSG. To do that, set the rule's source (for ingress) or destination (for egress) as the rule's own NSG.

A VNIC can be in a maximum of five NSGs. A packet in question is allowed if any rule in any of the VNIC's NSGs allows the traffic (or if the traffic is part of an existing connection being tracked). There's a caveat if the lists happen to contain both stateful and stateless security rules that cover the same traffic. For more information, see Stateful Versus Stateless Rules on page 2839.

Network security groups are regional entities. For limits related to network security groups, see Comparison of Security Lists and Network Security Groups on page 2833.

Security Rules

If you're not yet familiar with the basics of NSG security rules, see these sections in the security rules topic:

- Parts of a Security Rule on page 2837
Networking

- Stateful Versus Stateless Rules on page 2839

Working with Network Security Groups

General Process for Working with NSGs

1. Create an NSG.
2. Add security rules to the NSG.
3. Add parent resources (or more specifically, VNICs) to the NSG. You can do this when you create the parent resource, or you can update the parent resource and add it to one or more NSGs. When you create a Compute instance and add it to an NSG, the instance's primary VNIC is added to the NSG. Separately, you can create secondary VNICs and optionally add them to NSGs.

Before deleting an NSG, you must remove all VNICs from it.

See the next sections for more details.

Creating NSGs

Each VCN comes with a default security list that has default security rules in it to enable basic connectivity. However, there is no default NSG in the VCN.

When you create an NSG, it is initially empty, without any security rules or VNICs. If you're using the Console, you can add security rules to the NSG during creation.

You may optionally assign a friendly name to the NSG during creation. It doesn't have to be unique, and you can change it later. Oracle automatically assigns the NSG a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers on page 197.

For the purposes of access control, you must specify the compartment where you want the NSG to reside. Consult an administrator in your organization if you're not sure which compartment to use. For more information, see Access Control on page 2831.

Updating Security Rules and Group Membership

After the NSG is created, you can add or remove security rules to allow the types of ingress and egress traffic that the VNICs in the group require.

If you're familiar with security lists and use the REST API, note that the model for updating existing security rules is different between security lists and NSGs. With NSGs, each rule in a given group has a unique Oracle-assigned identifier (example: 04ABEC). When you call UpdateNetworkSecurityGroupSecurityRules, you provide the IDs of the specific rules that you want to update. For comparison, with security lists, the rules have no unique identifier. When you call UpdateSecurityList, you must pass in the entire list of rules, including rules that are not being updated in the call.

When you manage an NSG's VNIC membership, you do it as part of working with the parent resource, not the NSG itself. For more information, see Comparison of Security Lists and Network Security Groups on page 2833.

Specifying an NSG in a Security Rule

As mentioned earlier in Overview of Network Security Groups on page 2842, you can specify an NSG as the source (for ingress rules) or destination (for egress rules) in a given NSG's security rule. The two NSGs must be in the same VCN. For example, if both NSG1 and NSG2 belong to the same VCN, you could add an ingress rule to NSG1 that lists NSG2 as the source. If someone deletes NSG2, the rule becomes invalid. The REST API uses an isValid Boolean in the SecurityRule object to convey that status.

Deleting NSGs

To delete an NSG, it must not contain any VNICs or parent resources. When a parent resource (or a Compute instance VNIC) is deleted, it is automatically removed from the NSGs it was in. You might not have permission to delete a particular parent resource. Contact your administrator to determine who owns a given resource.
The Console displays a list of parent resources that are in an NSG, with a link to each parent resource. If the parent resource is a Compute instance, the Console also displays the instance's VNIC or VNICs that are in the NSG.

To remove a parent resource from its NSGs without deleting the resource, first view the parent resource's details in the Console. There you can see a list of the NSGs that the resource belongs to. From there, you can click Edit and remove the resource from all NSGs. If you're instead working with a Compute instance, view the details of the specific VNIC that you want to remove from the NSGs.

If you're using the REST API: the `ListNetworkSecurityGroupVnics` lists the parent resources and VNICs in an NSG. Use the resource's Update operation to remove the resource from NSGs. For example, for a Compute instance, use the `UpdateVnic` operation. For a load balancer, use the `UpdateNetworkSecurityGroups` operation, and so on.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a `policy` by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which `compartment` you should work in.

For administrators: The policy in Let network admins manage a cloud network on page 2143 covers management of all Networking components, including NSGs.

If you have security admins who need to manage NSGs but not other components in the Networking service, you could write a more restrictive policy:

```plaintext
Allow group NSGAdmins to manage network-security-groups in tenancy
Allow group NSGAdmins to manage vcns in tenancy
  where ANY {request.operation = 'CreateNetworkSecurityGroup',
               request_operation = 'DeleteNetworkSecurityGroup'}
Allow group NSGAdmins to read vcns in tenancy
Allow group NSGAdmins to use VNICs in tenancy
```

The first statement lets the NSGAdmins group create and manage NSGs and their security rules.

The second statement is required because the creation or deletion of an NSG affects the VCN that the NSG is in. The statement restricts the VCN-related permissions to only those required to create or delete an NSG. The statement does not allow the NSGAdmins group to create or delete VCNs, or work with any resources in a VCN except NSGs.

The third statement is required for listing the VCNs, which is a prerequisite for creating or deleting an NSG in a VCN. For information about why both the second and third statements are required, see Conditions on page 2160.

The fourth statement is required if the NSGAdmins need to put VNICs into an NSG. Whoever creates the parent resource of the VNIC (for example, a Compute instance) must already have this level of permission to create the parent resource.

For more information about Networking service policies, see IAM Policies for Networking on page 2832.

**Using the Console**

*To view the security rules and resources in an NSG*

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the NSG you're interested in to view its details.

The NSG's security rules are displayed on the page. From there you can add, edit, or remove rules.
Networking

5. Under Resources, click VNICs to see the parent resources that belong to the NSG.

   If the parent resource is a Compute instance, the corresponding VNICs from that instance are also listed on the page.

   For other types of parent resources, the relevant service manages the VNICs on your behalf. Therefore only the parent resource (and not its corresponding VNICs) is listed on the page.

To create an NSG

Prerequisite: Become familiar with the parts of security rules.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
5. Enter the following:

   a. Name: A descriptive name for the network security group. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.

   b. Create in Compartment: The compartment where you want to create the network security group, if different from the compartment you're currently working in.

   c. Show Tagging Options: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. Click Next.

   If you want to create the NSG without any rules yet, click Create and you're done. Otherwise proceed to the next step.

7. For the first security rule, enter the following items (for examples of rules, see Networking Scenarios on page 2756):

   • Stateful or stateless: If stateful, connection tracking is used for traffic matching the rule. If stateless, no connection tracking is used. By default, rules are stateful unless you specify otherwise. See Stateful Versus Stateless Rules on page 2839.

   • Direction (ingress or egress): Ingress is inbound traffic to the VNIC, and egress is outbound traffic from the VNIC.

   • Source Type and Source (for ingress rules only):

     Allowed source types

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Allowed Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>The CIDR block where the traffic originates from. Use 0.0.0.0/0 to indicate all IP addresses. The prefix is required (for example, include the /32 if specifying an individual IP address).</td>
</tr>
<tr>
<td>Service</td>
<td>Only for packets coming from an Oracle service through a service gateway. The source service is the service CIDR label that you're interested in.</td>
</tr>
</tbody>
</table>
### Source Type

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Allowed Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Group</td>
<td>An NSG that is in the same VCN as this rule's NSG.</td>
</tr>
</tbody>
</table>

**Destination Type** and **Destination** (for egress rules only):

Allowed destination types

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Allowed Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>The CIDR block where the traffic is destined to. Use 0.0.0.0/0 to indicate all IP addresses. The prefix is required (for example, include the /32 if specifying an individual IP address).</td>
</tr>
<tr>
<td>Service</td>
<td>Only for packets going to an Oracle service through a service gateway. The destination service is the service CIDR label that you're interested in.</td>
</tr>
<tr>
<td>Network Security Group</td>
<td>An NSG that is in the same VCN as this rule's NSG.</td>
</tr>
</tbody>
</table>

- **IP Protocol**: Either a single IPv4 protocol (for example, TCP or ICMP) or "all" to cover all protocols.
- **Source port range**: The port where the traffic originates from. For TCP or UDP, you can specify all source ports, or optionally specify a single source port number, or a range.
- **Destination port range**: The port where the traffic is destined to. For TCP or UDP, you can specify all destination ports, or optionally specify a single destination port number, or a range.
- **ICMP type and code**: For ICMP, you can specify all types and codes, or optionally specify a single type with an optional code. If the type has multiple codes, create a separate rule for each code you want to allow.

8. To add another security rule, click + Another Rule and enter the rule's information. Repeat for each rule you want to add.

9. When you're done, click Create.

The NSG is created and then displayed on the Network Security Group page in the compartment you chose. You can now specify this NSG when creating or managing instances or other types of parent resources.

When you view all the security rules in an NSG, you can filter the list by ingress or egress.

#### To add or remove a resource from an NSG

In general, you manage the resource membership of an NSG at the parent resource, and not at the NSG itself. In other words, to add a parent resource to an NSG, you execute the action on the parent resource (by specifying which NSGs the parent resource should be added to). You do not execute the action on the NSG (by specifying which VNICs or parent resources should be added to the NSG). Similarly, to remove a VNIC from an NSG, you execute that action by updating the parent resource, not the NSG. For a list of the parent resources that support the use of NSG, see Support for Network Security Groups on page 2842.

Example: Compute instances

- **When creating an instance**: In the Configure networking section, select the check box for Use network security groups to control traffic, and then specify one or more NSGs. The instance's primary VNIC is added to the NSGs. See the procedure in Creating an Instance on page 695.

- **For an existing instance**: Adding an existing instance to an NSG means adding its primary VNIC to the NSG. You can also add a secondary VNIC to an NSG. See To add or remove a VNIC from a network security group on page 2859.

Example: Exadata DB systems

- **When creating an Exadata DB system**: In the Network Information section, you set up the client network and backup network. For each network, select the check box for Use network security groups to control traffic, and then specify one or more NSGs for the specific network. See To create an X7 or X8 Exadata DB system on page 1248. Also see Network Setup for Exadata Cloud Service Instances on page 1232.
For an existing Exadata DB system: An Exadata's details include a list of the NSGs that the client network belongs to (if any), and a list of the NSGs that the backup network belongs to (if any). Next to the relevant Network Security Groups, click Edit to change that list. See To edit the network security groups (NSGs) for your client or backup network on page 1261.

To delete an NSG

Prerequisite: To delete a security list, it must not be associated with a subnet. You can't delete the default security list in a VCN.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the security list you want to delete, click the Actions icon (three dots), and then click Terminate.
5. Confirm when prompted.

To manage security rules for an NSG

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the NSG you're interested in to view its details.
5. The NSG's security rules are displayed on the page. From there you can add, edit, or remove rules.

To manage tags for an NSG

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the NSG you're interested in.
5. Click the Tags tab to view or edit the existing tags. Or click Add tags to add new ones.

For more information, see Resource Tags on page 211.

To move an NSG to a different compartment

You can move an NSG from one compartment to another. When you move an NSG to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the NSG you're interested in.
5. Click the the Actions icon (three dots) for the NSG, and then click Move Resource.
6. Choose the destination compartment from the list.
7. Click Move Resource.

For more information about using compartments and policies to control access to your cloud network, see Access Control on page 2831. For general information about compartments, see Managing Compartments on page 2431.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage a VCN's network security groups, use these operations:

- ListNetworkSecurityGroups
- GetNetworkSecurityGroup
- UpdateNetworkSecurityGroup
- CreateNetworkSecurityGroup
- DeleteNetworkSecurityGroup
• ChangeNetworkSecurityGroupCompartment
• ListNetworkSecurityGroupVnics
• ListNetworkSecurityGroupSecurityRules
• AddNetworkSecurityGroupSecurityRules
• RemoveNetworkSecurityGroupSecurityRules
• UpdateNetworkSecurityGroupSecurityRules

There are some differences in the REST API model for NSGs compared to security lists:

• With security lists, there is an `IngressSecurityRule` object and a separate `EgressSecurityRule` object. With network security groups, there is only a `SecurityRule` object, and the object's `direction` attribute determines whether the rule is for ingress or egress traffic.

• With security lists, the rules are part of the `SecurityList` object, and you work with the rules by calling the security list operations (such as `UpdateSecurityList`). With NSGs, the rules are not part of the `NetworkSecurityGroup` object. Instead you use separate operations to work with the rules for a given NSG (example: `UpdateNetworkSecurityGroupSecurityRules`).

• The model for updating existing security rules is different between security lists and NSGs. With NSGs, each rule in a given group has a unique Oracle-assigned identifier (example: 04ABEC). When you call `UpdateNetworkSecurityGroupSecurityRules`, you provide the IDs of the specific rules that you want to update. For comparison, with security lists, the rules have no unique identifier. When you call `UpdateSecurityList`, you must pass in the `entire` list of rules, including rules that are not being updated in the call.

• There is a limit of 25 rules when calling the operations to add, remove, or update security rules.

**Security Lists**

The Networking service offers two virtual firewall features to control traffic at the packet level:

• **Security lists**: Covered in this topic. This is the original type of virtual firewall offered by the Networking service.

• **Network security groups**: Another type of virtual firewall that Oracle recommends over security lists. See Network Security Groups on page 2841.

Both of these features use security rules. For important information about how security rules work, and a general comparison of security lists and network security groups, see Security Rules on page 2833.

**Highlights**

• Security lists act as virtual firewalls for your Compute instances and other kinds of resources. A security list consists of a set of ingress and egress security rules that apply to all the VNICs in any subnet that the security list is associated with. This means that all the VNICs in a given subnet are subject to the same set of security lists. See Comparison of Security Lists and Network Security Groups on page 2833.

• Security list rules function the same as network security group rules. For a discussion of rule parameters, see Parts of a Security Rule on page 2837.

• Each VCN comes with a default security list that has several default rules for essential traffic. If you don’t specify a custom security list for a subnet, the default security list is automatically used with that subnet. You can add and remove rules from the default security list.

• Security lists have separate and different limits compared to network security groups. See Comparison of Security Lists and Network Security Groups on page 2833.

**Overview of Security Lists**

A security list acts as a virtual firewall for an instance, with ingress and egress rules that specify the types of traffic allowed in and out. Each security list is enforced at the VNIC level. However, you configure your security lists at the subnet level, which means that all VNICs in a given subnet are subject to the same set of security lists. The security lists apply to a given VNIC whether it’s communicating with another instance in the VCN or a host outside the VCN.

Each subnet can have multiple security lists associated with it, and each list can have multiple rules (for the maximum number, see Comparison of Security Lists and Network Security Groups on page 2833). A packet in question is allowed if any rule in any of the lists allows the traffic (or if the traffic is part of an existing connection being
Networking

There's a caveat if the lists happen to contain both stateful and stateless rules that cover the same traffic. For more information, see Stateful Versus Stateless Rules on page 2839.

Security lists are regional entities. For limits related to security lists, see Comparison of Security Lists and Network Security Groups on page 2833.

Security lists can control both IPv4 and IPv6 traffic. However, IPv6 addressing and related security list rules are currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

**Default Security List**

Unlike other security lists, the default security list comes with an initial set of stateful rules, which should in most cases be changed to only allow inbound traffic from authorized subnets relevant to the region that homes that VCN or subnet. A list of authorized subnet ranges relevant to each region can be found at https://docs.cloud.oracle.com/iaas/tools/public_ip_ranges.json.

- **Stateful ingress**: Allow TCP traffic on destination port 22 (SSH) from authorized source IP addresses and any source port. This rule makes it easy for you to create a new cloud network and public subnet, launch a Linux instance, and then immediately use SSH to connect to that instance without needing to write any security list rules yourself.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The default security list does not include a rule to allow Remote Desktop Protocol (RDP) access. If you're using Windows images, make sure to add a stateful ingress rule for TCP traffic on destination port 3389 from authorized source IP addresses and any source port. See To enable RDP access for more information.</td>
</tr>
</tbody>
</table>

- **Stateful ingress**: Allow ICMP traffic type 3 code 4 from authorized source IP addresses. This rule enables your instances to receive Path MTU Discovery fragmentation messages.

- **Stateful ingress**: Allow ICMP traffic type 3 (all codes) from your VCN's CIDR block. This rule makes it easy for your instances to receive connectivity error messages from other instances within the VCN.

- **Stateful egress**: Allow all traffic. This allows instances to initiate traffic of any kind to any destination. Notice that this means the instances with public IP addresses can talk to any internet IP address if the VCN has a configured internet gateway. And because stateful security rules use connection tracking, the response traffic is automatically allowed regardless of any ingress rules. For more information, see Stateful Versus Stateless Rules on page 2839.

The default security list comes with no stateless rules. However, you can always add or remove rules from the default security list.

If your VCN is enabled for IPv6 addressing (which is currently supported in only the Government Cloud), the default security list contains some default rules for IPv6 traffic. For more information, see IPv6 Addresses on page 2889.

**Enabling Ping**

The default security list does not include a rule to allow ping requests. If you plan to ping an instance, see Rules to Handle Fragmented UDP Packets on page 2841.

**Security Rules**

If you're not yet familiar with the basics of security rules, see these sections in the security rules topic:

- Parts of a Security Rule on page 2837
- Stateful Versus Stateless Rules on page 2839

**Working with Security Lists**

**General Process for Working with Security Lists**

1. Create a security list.
2. Add security rules to the security list.
3. Associate the security list with one or more subnets.
4. Create resources in the subnet (for example, create Compute instances in the subnet). The security rules apply to all the VNICs in that subnet. See Comparison of Security Lists and Network Security Groups on page 2833.

**Additional Details**

When you create a subnet, you must associate at least one security list with it. It can be either the VCN's default security list or one or more other security lists that you've already created (for the maximum number, see Service Limits on page 215). You can change which security lists the subnet uses at any time.

You may optionally assign a friendly name to the security list during creation. It doesn't have to be unique, and you can change it later. Oracle automatically assigns the security list a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers on page 197.

For the purposes of access control, you must specify the compartment where you want the security list to reside. Consult an administrator in your organization if you're not sure which compartment to use. For more information, see Access Control on page 2831.

You can move security lists from one compartment to another. Moving a security list doesn’t affect its attachment to a subnet. When you move a security list to a new compartment, inherent policies apply immediately and affect access to the security list. For more information, see Managing Compartments on page 2431.

You can add and remove rules from the security list. A security list can have no rules. Notice that when you update a security list in the API, the new set of rules replaces the entire existing set of rules.

To delete a security list, it must not be associated with a subnet. You can't delete a VCN's default security list.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let network admins manage a cloud network on page 2143 covers management of all Networking components, including security lists.

If you have security admins who need to manage security lists but not other components in Networking, you could write a more restrictive policy:

```
Allow group SecListAdmins to manage security-lists in tenancy
Allow group SecListAdmins to manage vcns in tenancy
```

Both statements are needed because the creation of a security list affects the VCN the security list is in. The scope of the second statement also allows the SecListAdmins group to create VCNs. However, the group can't create subnets or manage any other components related to any of those VCNs (except for the security lists), because other permissions would be required for those resources. The group also can't delete any existing VCNs that already have subnets in them, because that action would require permissions related to subnets.

For more information, see IAM Policies for Networking on page 2832.

**Using the Console**

*To view a VCN's default security list*

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the default security list to view its details.

Under Resources, you can click Ingress Rules or Egress Rules to switch between the different types of rules.
**To update rules in an existing security list**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the security list you're interested in.
5. Under Resources, click either Ingress Rules or Egress Rules depending on the type of rule you want to work with.
6. If you want to add a rule, click Add Ingress Rule (or Add Egress Rule). See details of adding a rule in To create a security list on page 2853.
7. If you want to delete an existing rule, click the Actions icon (three dots), and then click Remove.
8. If you wanted to edit an existing rule, click the Actions icon (three dots), and then click Edit.

---

**To create a security list**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click Create Security List.
5. Enter the following:
   a. **Name**: A descriptive name for the security list. The name doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   b. **Create in Compartment**: The compartment where you want to create the security list, if different from the compartment you're currently working in.
6. Add either an ingress rule or egress rule (for examples of rules, see Networking Scenarios on page 2756):
   a. Click either Add Ingress Rule or Add Egress Rule.
   b. Choose whether it's a stateful or stateless rule (see Stateful Versus Stateless Rules on page 2839). By default, rules are stateful unless you specify otherwise.
   c. Enter either the source CIDR (for ingress) or destination CIDR (for egress). For example, use 0.0.0.0/0 to indicate all IP addresses. Other typical CIDRs you might specify in a rule are the CIDR block for your on-premises network, or for a particular subnet. If you're setting up a security list rule to allow traffic with a service gateway, instead see Task 3: (Optional) Update security rules on page 3261.
   d. Select the IP protocol (for example, TCP, UDP, ICMP, "All protocols", and so on).
   e. Enter further details depending on the protocol:
      - If you chose TCP or UDP, enter a source port range and destination port range. You can enter "All" to cover all ports. If you want to allow a specific port, enter the port number (for example, 22 for SSH or 3389 for RDP) or a port range (for example, 20–22).
      - If you chose ICMP, you can enter "All" to cover all types and codes. If you want to allow a specific ICMP type, enter the type and an optional code separated by a comma (for example, 3,4). If the type has multiple codes you want to allow, create a separate rule for each code.
   f. Enter an optional description of the rule to help manage your security list rules.
7. Repeat the preceding step for each rule you want to add to the list.
8. **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
9. When you're done, click Create Security List.

The security list is created and then displayed on the Security Lists page in the compartment you chose. You can now specify this security list when creating or updating a subnet.

When you view all the rules in a security list, notice that any stateless rules in the list are shown above any stateful rules. Stateless rules in the list take precedence over stateful rules. In other words: If there's traffic that matches
both a stateless rule and a stateful rule across all the security lists associated with the subnet, the stateless rule takes precedence and the connection is not tracked.

To change which security lists a subnet uses

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click Subnets.
4. Click the subnet you're interested in.
6. If you want to add a security list, click Add Security List, and select the new security list you want the subnet to use.
7. If you want to remove a security list, click the Actions icon (three dots), and then click Remove. Remember that a subnet must always have at least one security list associated with it.

The changes take effect within a few seconds.

To move a security list to a different compartment

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Find the security list, click the the Actions icon (three dots), and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To delete a security list

Prerequisite: To delete a security list, it must not be associated with a subnet. You can't delete the default security list in a VCN.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the security list you want to delete, click the Actions icon (three dots), and then click Terminate.
5. Confirm when prompted.

To manage tags for a security list

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. Click the security list you're interested in.
5. Click the Tags tab to view or edit the existing tags. Or click Add tags to add new ones.

For more information, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage a VCN's security lists, use these operations:

- ListSecurityLists
- GetSecurityList
- UpdateSecurityList
- CreateSecurityList
- DeleteSecurityList
- ChangeSecurityListCompartment
**VCN Flow Logs**

This topic describes the contents of VCN flow logs and how to set up flow logs for resources in your VCN.

**Highlights**

- VCN flow logs shows details about traffic that passes through your VCN.
- VCN flow logs help you audit traffic and troubleshoot your security lists.
- Flow logs are enabled and managed using the Logging service. For more information, see Overview of the Logging Service.
- Flow logs can be generated from VNICS, PEs, and RCEs. For PEs and RCEs, they appear as from the VNIC associated with the PE/RCE.

**Overview of Flow Logs**

Each instance in a VCN has one or more Virtual Network Interface Cards (VNICS) on page 2855. The Networking service uses Security Lists on page 2850 to determine what traffic is allowed through a given VNIC. The VNIC is subject to all rules in all security lists associated with the VNIC's subnet.

To help you troubleshoot your security lists or audit the traffic in and out of your VNICS, you can set up VCN flow logs. Flow logs record details about traffic that has been accepted or rejected based on the security list rules.

**How Flow Logs Are Enabled and Delivered**

Flow logs are enabled and managed using the Logging service. You can enable flow logs for a given subnet, which means traffic is logged for all the existing and future VNICS in that subnet. Each flow log record contains information about traffic for a single VNIC. Here are the general steps for setting up flow logs:

1. **Enable flow logs for the subnet**: VCN flow logs are enabled for a subnet using the Logging service.
2. **View the subnet’s flow logs**: Assuming there is traffic for the given subnet, it can take up to 10 minutes for the first flow logs to be delivered. Then you receive batches of flow logs every minute.

After flow logs are enabled for a subnet, a batch of flow logs for each VNIC is collected in one-minute capture windows. It takes under eight minutes to process a batch, after which the flow logs are available for viewing.

**Flow Log Contents**

Each flow log record reflects logged traffic in one direction of a connection between two endpoints. For example, for a single TCP connection, you may have two records in the capture window: one for ingress traffic, and the other for egress traffic.

For more information about flow log contents, examples, and limitations and other considerations, see Details for VCN Flow Logs on page 2612.

**Setting Up Flow Logs for a Subnet**

See Enabling Logging for a Resource on page 2591 for instructions on setting up logging.

**Managing Flow Logs**

Flow log management tasks such as disabling logs, deleting logs, and editing logs are performed using the Logging service. For more information on log management, see Managing Logs and Log Groups on page 2577.

**Use VCN Flow Logs to Audit Traffic and Troubleshoot Security Lists**

To list details about traffic that passes to and from destinations in your VCN, enable flow logs for a given subnet. After you have them enabled, flow logs record traffic for all existing and future VNICS attached to compute instances in that subnet.

Flow logs are enabled and managed using the Logging service. For more information, see Overview of the Logging Service.

**Virtual Network Interface Cards (VNICS)**

This topic describes how to manage the virtual network interface cards (VNICS) in a virtual cloud network (VCN).
Overview of VNICs and Physical NICs

The servers in Oracle Cloud Infrastructure data centers have physical network interface cards (NICs). When you launch an instance on one of these servers, the instance communicates using Networking service virtual NICs (VNICs) associated with the physical NICs. The next sections talk about VNICs and NICs, and how they're related.

About VNICs

A VNIC enables an instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN and includes these items:

- One primary private IPv4 address from the subnet the VNIC is in, chosen by either you or Oracle.
- Up to 31 optional secondary private IPv4 addresses from the same subnet the VNIC is in, chosen by either you or Oracle.
- An optional public IPv4 address for each private IP, chosen by Oracle but assigned by you at your discretion.
- An optional hostname for DNS for each private IP address (see DNS in Your Virtual Cloud Network on page 2910).
- A MAC address.
- A VLAN tag assigned by Oracle and available when attachment of the VNIC to the instance is complete (relevant only for bare metal instances).
- A flag to enable or disable the source/destination check on the VNIC’s network traffic (see Overview of VNICs and Physical NICs on page 2856).
- Optional membership in one or more network security groups (NSGs) of your choice. NSGs have security rules that apply only to the VNICs in that NSG.
- Up to 32 optional IPv6 addresses. IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

Each VNIC also has a friendly name you can assign, and an Oracle-assigned OCID (see Resource Identifiers).

Each instance has a primary VNIC that is automatically created and attached during launch. That VNIC resides in the subnet you specify during launch. The primary VNIC cannot be removed from the instance.

How VNICs and Physical NICs Are Related

This section is relevant to bare metal instances.

The OS on a bare metal instance recognizes two physical network devices and configures them as two physical NICs, 0 and 1. Whether they're both active depends on the underlying hardware. You can determine which NICs are active for a shape by reviewing the network bandwidth specifications for bare metal shapes. If the network bandwidth is listed as "2 x <bandwidth> Gbps," it means that both NIC 0 and NIC 1 are active, and each physical NIC has the indicated amount of bandwidth. If the network bandwidth is listed as "1 x <bandwidth> Gbps," it means that only NIC 0 is active. On current generation Standard and DenseIO shapes, typically both NIC 0 and NIC 1 are active.

NIC 0 is automatically configured with the primary VNIC's IP configuration (the IP addresses, DNS hostname, and so on).

If you add a secondary VNIC to an instance, you must specify which physical NIC the secondary VNIC should use. You must also configure the OS so that the physical NIC has the secondary VNIC's IP configuration. For Linux instances, see Linux: Configuring the OS for Secondary VNICs on page 2861. For Windows instances, see Windows: Configuring the OS for Secondary VNICs on page 2862.

About Secondary VNICs

You can add secondary VNICs to an instance after it's launched. Each secondary VNIC can be in a subnet in the same VCN as the primary VNIC, or in a different subnet that is either in the same VCN or a different one. However, all the VNICs must be in the same availability domain as the instance.
Here are some reasons why you might use secondary VNICs:

- **Use your own hypervisor on a bare metal instance:** The virtual machines on the bare metal instance each have their own secondary VNIC, giving direct connectivity to other instances and services in the VNIC's VCN. For more information, see *Installing and Configuring KVM on Bare Metal Instances with Multi-VNIC*.

- **Connect an instance to subnets in multiple VCNs:** For example, you might set up your own firewall to protect traffic between VCNs, so the instance needs to connect to subnets in different VCNs.

Here are more details about secondary VNICs:

- They're supported for these types of instances:
  - **Linux:** Both VM and bare metal instances. Also see *Linux: Configuring the OS for Secondary VNICs* on page 2861.
  - **Windows:** Both VM and bare metal instances (except for instances that use previous generation Standard1 and StandardB1 shapes). For bare metal instances, secondary VNICs are supported only on the second physical NIC. Remember that the first physical NIC is NIC 0, and the second is NIC 1. Also see *Windows: Configuring the OS for Secondary VNICs* on page 2862.

- There's a limit to how many VNICs can be attached to an instance, and it varies by shape. For those limits, see *Compute Shapes* on page 655.

- They can be added only after the instance is launched.

- They must always be attached to an instance and cannot be moved. The process of creating a secondary VNIC automatically attaches it to the instance. The process of detaching a secondary VNIC automatically deletes it.

- They are automatically detached and deleted when you terminate the instance.

- They are automatically detached and deleted when you terminate the instance.

- There's a limit to how many VNICs can be attached to an instance, and it varies by shape. For those limits, see *Compute Shapes* on page 655.

- They can be added only after the instance is launched.

- They must always be attached to an instance and cannot be moved. The process of creating a secondary VNIC automatically attaches it to the instance. The process of detaching a secondary VNIC automatically deletes it.

- They are automatically detached and deleted when you terminate the instance.

- The instance's bandwidth is fixed regardless of the number of VNICs attached. You can't specify a bandwidth limit for a particular VNIC on an instance.

- Attaching multiple VNICs from the same subnet CIDR block to an instance can introduce asymmetric routing, especially on instances using a variant of Linux. If you need this type of configuration, Oracle recommends assigning multiple private IP addresses to one VNIC, or using policy-based routing as shown in the script later in this topic.

### Source/Destination Check

By default, every VNIC performs the source/destination check on its network traffic. The VNIC looks at the source and destination listed in the header of each network packet. If the VNIC is not the source or destination, then the packet is dropped.

If the VNIC needs to forward traffic (for example, if it needs to perform Network Address Translation (NAT)), you must disable the source/destination check on the VNIC. For instructions, see *To update an existing VNIC* on page 2859. For information about the general scenario, see *Using a Private IP as a Route Target* on page 2924.

### VNIC Information in the Instance Metadata

The instance metadata service (IMDS) includes information about the VNICs at these URLs:

- IMDS version 2:

  ```
  ```

- Legacy IMDS version 1:

  ```
  ```

Here's an example response that shows the VNICs that are attached to an instance:

```json
[
  {
    "vnicId" : "ocid1.vnic.oc1.phx.exampleuniqueID",
    "privateIp" : "10.0.3.6",
    "vlanTag" : 11,
```
Networking

```
{"macAddr" : "00:00:00:00:00:01",
"virtualRouterIp" : "10.0.3.1",
"subnetCidrBlock" : "10.0.3.0/24",
"nicIndex" : 0 },
{
"vnicId" : "ocid1.vnic.oc1.phx.exampleuniqueID",
"privateIp" : "10.0.4.3",
"vlanTag" : 12,
"macAddr" : "00:00:00:00:00:02",
"virtualRouterIp" : "10.0.4.1",
"subnetCidrBlock" : "10.0.4.0/24",
"nicIndex" : 0
}
```

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

VNICs reside in a subnet but attach to an instance. The VNIC’s *attachment to the instance* is a separate object from the VNIC or the instance itself. Be aware that the VNIC and subnet always exist together in the same compartment, but the VNIC’s *attachment to the instance* always exists in the instance's compartment. This distinction isn't important if you have a simple access control scenario where all the cloud resources are in the same compartment (for example, for a proof-of-concept). When you move to a production implementation, you might decide to have network administrators manage the network, and other personnel administer instances. That means you might put instances in a different compartment than the subnet.

For administrators: see [IAM Policies for Networking](#) on page 2832.

**Monitoring VNICs**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see [Monitoring Overview](#) on page 2660 and [Notifications Overview](#) on page 3350.

For information about monitoring the traffic coming in and out of VNICs, see [VNIC Metrics](#) on page 3321.

**Using the Console**

**To view an instance's VNICs**

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under *Core Infrastructure*, go to *Compute* and click *Instances*.
3. Click the instance to view its details.
4. Under *Resources*, click *Attached VNICs*.

   The primary VNIC and any secondary VNICs attached to the instance are displayed. If the instance has two active physical NICs, the VNICs are grouped by NIC 0 and NIC 1.

**To create and attach a secondary VNIC**

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under *Core Infrastructure*, go to *Compute* and click *Instances*.
3. Click the instance to view its details.
4. Under *Resources*, click *Attached VNICs*.

   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. Click *Create VNIC*.  

Oracle Cloud Infrastructure User Guide 2858
6. In the **Create VNIC** dialog box, you specify which VCN and subnet to put the VNIC in. By default, the VNIC will be created in the current compartment. You can choose a VCN and subnet from the same compartment or a different compartment.

Enter the following:

- **Name**: A friendly name for the secondary VNIC. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.
- **Virtual cloud network**: The VCN that contains the subnet of interest.
- **Network**: Select **Normal Setup: Subnet**.
- **Subnet**: The subnet of interest. The secondary VNIC must be in the same availability domain as the instance's primary VNIC, so the subnet list includes any regional subnets or AD-specific subnets in the primary VNIC's availability domain.
- **Physical NIC**: Only relevant if this is a bare metal instance with two active physical NICs. Select which one you want the secondary VNIC to use. When you later view the instance's details and the list of VNICs attached to the instance, they'll be grouped by NIC 0 and NIC 1.
- **Use network security groups to control traffic**: Select this check box to add the secondary VNIC to at least one network security group (NSG) of your choice. NSGs have security rules that apply only to the VNICs in that NSG.
- **Skip source/destination check**: By default, this check box is NOT selected, which means the VNIC performs the source/destination check. Only select this check box if you want the VNIC to be able to forward traffic. See **Overview of VNICs and Physical NICs** on page 2856.
- **Private IP Address**: Optional. An available private IP address of your choice from the subnet's CIDR (otherwise the private IP address is automatically assigned).
- **Assign a public IPv4 address**: Whether to assign a public IP address to the VNIC's primary private IP. Available only if the subnet is public. Choose this option to specify an existing reserved public IP address by name, or to create a new reserved IP address by assigning a name and selecting a source IP pool for the address. If you don't select an IP pool you've created, the default Oracle IP pool is used.
- **Hostname**: Optional. A hostname to be used for DNS within the cloud network. Available only if the VCN and subnet both have DNS labels. For more information, see **DNS in Your Virtual Cloud Network** on page 2910.
- **Show Tagging Options**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

7. Click **Submit**. The secondary VNIC is created and then displayed on the **Attached VNICs** page for the instance. It can take several seconds before the secondary VNIC appears on the page.

8. Configure the OS to use the VNIC. See **Linux: Configuring the OS for Secondary VNICs** on page 2861 or **Windows: Configuring the OS for Secondary VNICs** on page 2862.

### To update an existing VNIC

You can update the VNIC's friendly name or hostname, or whether the VNIC performs the source/destination check.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICs**.

   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. For the VNIC you want to edit, click the Actions icon (three dots), and then click **Edit VNIC**.
6. Make your changes. Avoid entering confidential information. Then, click **Save Changes**.

### To add or remove a VNIC from a network security group

You can change which network security groups (NSGs) a VNIC belongs to, or remove a VNIC from all NSGs.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICs**.
   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. Click the VNIC you’re interested in.
   Each VNIC's details page includes a list of the NSGs that the VNIC belongs to (if any).
6. Next to **Network Security Groups**, click **Edit**.
7. Make your changes and click **Save Changes**.

### To delete a secondary VNIC

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the VNIC has a private IP that is the target of a route rule, deleting the VNIC causes the route rule to blackhole and traffic will be dropped.</td>
</tr>
</tbody>
</table>

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICs**.
   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. For the VNIC you want to delete, click the Actions icon (three dots), and then click **Delete VNIC**.
6. Confirm when prompted.

It takes typically a few seconds before the VNIC is deleted.

If the secondary VNIC is on a Linux instance: If you then run the provided script in [Linux: Configuring the OS for Secondary VNICs](page 2861), it removes the secondary VNIC from the OS configuration.

### To manage tags for a VNIC

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICs**.
   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Click the **Tags** tab to view or edit the existing tags. Or click **Add Tags** to add new ones.

For more information, see [Resource Tags](page 211).

### Using the API

For information about using the API and signing requests, see [REST APIs](page 4368) and [Security Credentials](page 179). For information about SDKs, see [Software Development Kits and Command Line Interface](page 4225).

To manage VNICs on an instance, use these operations:

- **ListVnicAttachments**: Use this to list the VNICs attached to an instance.
- **GetVnicAttachment**: Use this to get the VNIC’s VLAN tag and other properties.
- **GetVnic**: Use this to get the VNIC’s private IP address, MAC address, optional public IP address, optional DNS hostname, and other properties.
- **AttachVnic**
- **DetachVnic**
- **UpdateVnic**
Linux: Configuring the OS for Secondary VNICs

This section gives details about OS configuration that is required for secondary VNICs on instances that run a variant of Linux.

At the end of the section is a script that you can use to configure secondary VNICs on either VM instances or bare metal instances.

Linux VM Instances

When you add a secondary VNIC to a Linux VM instance, a new interface (that is, an Ethernet device) is added to the instance and automatically recognized by the OS. However, DHCP is not active for the secondary VNIC, and you must configure the interface with the static IP address and default route. The script provided here handles that configuration for you.

Linux Bare Metal Instances

When you add a secondary VNIC to a Linux bare metal instance, the OS does not automatically recognize the secondary VNIC, so you must configure it in the OS. Depending on your requirements, you can configure it as either:

• An SR-IOV virtual function (see Installing and Configuring KVM on Bare Metal Instances with Multi-VNIC).
• A VLAN-tagged interface (see the script in the following section).

Configuration Script for Either Linux VM Instances or Linux Bare Metal Instances

The following script works for both VM instances and bare metal instances. It looks at the secondary VNIC information in the instance metadata and configures the OS accordingly. You could run the script periodically to bring the OS configuration up to date with the instance metadata.

For VM instances in particular, the OS automatically recognizes the secondary VNIC's interface, and the script just needs to configure the static IP address and default route.

For bare metal instances in particular, the script creates the interface for the secondary VNIC and configures it with the relevant information. If the instance has two active physical NICs (NIC 0 and NIC 1), the script configures the secondary VNIC to use whichever physical NIC you chose when you added the VNIC to the instance. Note that for NIC 1, if a secondary VNIC has VLAN tag 0, it uses the NIC's interface. The script doesn't create an interface for that secondary VNIC.

Here are some additional notes about how the script works for both VM instances and bare metal instances:

• Default namespace and policy-based routing: By default, this script configures the secondary VNIC in the default namespace and with policy-based routing so applications can communicate through the VNIC with hosts outside the VNIC's subnet. This policy-based routing has effect only if the packets are sourced from the IP address of the secondary VNIC. The ability to bind to a specific source IP address or source interface exists in most tools (such as ssh, ping, and wget) and libraries that initiate connections. For example, the ssh -b <secondary_VNIC_IP_address> <destination_IP_address> lets you bind to the private IP address of the secondary VNIC.

Be aware that if traffic comes in to a service on the instance through a secondary VNIC's interface and the service replies, the reply packets automatically have the VNIC's interface IP address as the source IP address. Policy-based routing is required for that reply to go back out on the same interface and find the correct default gateway.

• A separate namespace: If you're familiar with namespaces, you can instead configure the secondary VNIC in another namespace of your choice by running the script with the -n option. A separate namespace is required when an instance has secondary VNICs that are attached to subnets in different VCNs, and those subnets have overlapping CIDR blocks.

• Secondary private IPs: The instance metadata does not include information about any secondary private IPs assigned to the instance. To include that as part of the script's OS configuration, you must provide the secondary private IP address and OCID at the command line when you run the script.
• **Removal of a secondary VNIC:** After deleting a secondary VNIC from an instance, running the script removes the VNIC's information from the OS configuration.

**Important:**

The script uses a simple configuration process that does not persist if you reboot the instance. If you use the script, make sure to rerun it after each reboot.

Here are basic examples of how to run the script:

• `<script_name> -c`: Configure (adds or deletes) secondary VNIC host IP configuration
• `<script_name> -c -n`: Same but uses separate namespaces
• `<script_name> -d`: Force removes all secondary VNIC host IP configuration

See the script's help for more information.

**Important:**

This script is intended for use in situations where non-hypervisor compute instances need to be assigned an additional VNIC and IP address.

For Kernel-based Virtual Machine (KVM) applications on a bare metal instance, refer to the white paper "Installing and Configuring KVM on Bare Metal Instances with Multi-VNIC."

**Tip:**

Download the script from the online version of this user guide at https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/managingVNICs.htm#linux.

### Windows: Configuring the OS for Secondary VNICS

Secondary VNICS are supported on VM and bare metal instances (except for instances that use previous generation Standard1 and StandardB1 shapes). For bare metal instances, secondary VNICS are supported only on the second physical NIC.

**Tip:**

The first physical NIC is NIC 0, and the second is NIC 1.

You must configure the secondary VNIC within the OS. There's an Oracle-provided PowerShell script that performs configuration. When running the script, you can optionally provide the secondary VNIC's OCID (which you can get from the instance's VNIC metadata):

```
.\secondary_vnic_windows_configure.ps1 "<secondary_VNIC OCID>"
```

Otherwise, the script shows a list of the secondary VNICS on the instance and asks you to choose the one you want to configure. Here's generally what the script does:

1. The script checks if the network interface has an IP address and a default route.
2. To enable the OS to recognize the secondary VNIC, the script must overwrite the IP address and default route with static settings (which effectively disables DHCP). The script prompts you with a choice: to overwrite with the static settings, or exit.

**Tip:**

Download the script from the online version of this user guide at https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/managingVNICs.htm#windows.
The overall process for configuration varies slightly depending on the type of instance (VM or bare metal) and how many secondary VNICs you add to the instance.

**Windows VM instances**

Here's the overall process:

1. **Add one or more secondary VNICs** to the instance. Keep each VNIC's OCID handy so you can provide it later when you run the configuration script. You can also get the OCID from the instance's VNIC metadata.
2. **Connect to the instance** with Remote Desktop.
3. **Run the script**:
   a. Open PowerShell as an administrator.
   b. Run the script with the secondary VNIC's OCID:
      ```
      .\secondary_vnic_windows_configure.ps1 "<secondary_VNIC_OCID>"
      ```
4. Repeat the preceding step for each additional secondary VNIC.

**Windows bare metal instances: adding the first secondary VNIC**

If you're adding only a single secondary VNIC to the bare metal instance, here's the overall process:

1. **Add the secondary VNIC** to your instance. Keep the VNIC's OCID handy so you can provide it when later running the configuration script. You can also get the OCID from the instance's VNIC metadata.
2. **Connect to the instance** with Remote Desktop.
3. **Enable the second physical NIC** on the instance:
   a. Open the Device Manager, and then click **Network adapters**.
   b. Right-click the adapter that corresponds to the instance's second physical NIC, and click **Enable**.
4. **Run the script**:
   a. Open PowerShell as an administrator.
   b. Run the script with the secondary VNIC's OCID:
      ```
      .\secondary_vnic_windows_configure.ps1 "<secondary_VNIC_OCID>"
      ```
   c. When the script prompts you to overwrite the network interface's settings, say yes.

**Windows bare metal instances: adding additional secondary VNICs**

If you have one secondary VNIC on the second physical NIC of a bare metal instance, and you want to one or more additional VNICs, here's the overall process. It includes a task for setting up NIC teaming, which is required if the instance has more than one VNIC on the second physical NIC.

1. **Add one or more additional secondary VNICs** to your instance. Keep each VNIC's OCID and VLAN tag handy so you can provide them when later running the configuration script. You can also get the values from the instance's VNIC metadata.
2. **Connect to the instance** with Remote Desktop.
Networking

3. Set up NIC teaming on the instance:
   a. Open the Server manager, and then click **Local Server**.
   b. In the list of properties, locate **NIC Teaming**, and then click **Disabled** to enable and set up NIC teaming.
   c. In the **Teams** section on the lower-left side of the screen, click **Tasks**, and then click **New Team**.
   d. Enter a name for the team, select the check box for the second physical NIC on the instance, and click **OK**.
      The new team is created and appears in the list of teams in the **Teams** section.
   e. Click the new team so it's selected, and then in the **Adapters and Interfaces** section on the right side of the screen, click the **Team Interfaces** tab.
   f. Click **Tasks**, and then click **Add Interface** (you will create a separate interface for each secondary VNIC on the second physical NIC).
   g. Click the radio button for **Specific VLAN**, and then enter the Oracle-assigned VLAN tag number for the VLAN (for example, 1). You can get the VLAN tag from the Console or the instance's **VNIC metadata**.
   h. Click **OK**.
   i. Repeat the four preceding steps (e-h) for each of the other secondary VNICs. You create a separate interface for each secondary VNIC.

4. Run the script:
   a. Open PowerShell as an administrator.
   b. For the first secondary VNIC, run the script with the secondary VNIC's OCID:

   ```powershell
   .\secondary_vnic_windows_configure.ps1 "<secondary_VNIC_OCID>"
   ```
   c. When the script prompts you to overwrite the network interface's settings, say yes.
   d. Repeat the preceding two steps (b and c) for each of the additional secondary VNICs.

**IP Addresses and DNS in Your VCN**

These topics cover how your instances are assigned private and public IP addresses, and the use of DNS within your cloud network.

- **Private IP Addresses** on page 2864
- **Public IP Addresses** on page 2875
- **Bring Your Own IP** on page 2882
- **IP Pools** on page 2887
- **IPv6 Addresses** on page 2889
- **DNS in Your Virtual Cloud Network** on page 2910

**Private IP Addresses**

This topic describes how to manage the IPv4 addresses assigned to an instance in a virtual cloud network (VCN).

IPv6 addressing is currently supported only in the US Government Cloud. For more information, see **IPv6 Addresses** on page 2889.

**Overview of IP Addresses**

Instances use IP addresses for communication. Each instance has at least one private IP address and optionally one or more public IP addresses. A private IP address enables the instance to communicate with other instances inside the VCN, or with hosts in your on-premises network (via an IPSec VPN or Oracle Cloud Infrastructure FastConnect). A public IP address enables the instance to communicate with hosts on the internet. For more information, see these related topics:

- **Public vs. Private Subnets** on page 2752
- **How IP Addresses Are Assigned** on page 2752
- **Public IP Addresses** on page 2875
About the Private IP Object

The Networking service defines an object called a private IP, which consists of:

- Private IPv4 address, assigned by either you or Oracle.
- Optional hostname for DNS (see DNS in Your Virtual Cloud Network on page 2910).

Each private IP object has an Oracle-assigned OCID (see Resource Identifiers). If you're using the API, you can also assign each private IP object a friendly name.

Each instance receives a primary private IP object during launch. The Networking service uses the Dynamic Host Configuration Protocol (DHCP) to pass the object's private IP address to the instance. This address does not change during the instance's lifetime and cannot be removed from the instance. The private IP object is terminated when the instance is terminated.

If an instance has any secondary VNICs attached, each of those VNICs also has a primary private IP.

A private IP can have a public IP assigned to it at your discretion.

A private IP can be the target of a route rule in your VCN. For more information, see Using a Private IP as a Route Target on page 2924.

About Secondary Private IP Addresses

You can add a secondary private IP to an instance after it's launched. You can add it to either the primary VNIC or a secondary VNIC on the instance. The secondary private IP address must come from the CIDR of the VNIC's subnet.

You can move a secondary private IP from a VNIC on one instance to a VNIC on another instance if both VNICs belong to the same subnet.

Here are a few reasons why you might use secondary private IPs:

- **Instance failover:** You assign a secondary private IP to an instance. Then if the instance has problems, you can easily reassign that secondary private IP to a standby instance in the same subnet. If the secondary private IP has a public IP assigned to it, that public IP moves along with the private IP.
- **Running multiple services or endpoints on a single instance:** For example, you could have multiple container pods running on a single instance, and each uses an IP address from the VCN's CIDR. The containers have direct connectivity to other instances and services in the VCN. Another example: you could run multiple SSL websites with each one using its own IP address.

Here are more details about secondary private IP addresses:

- They're supported for all shapes and OS types, for both bare metal and VM instances.
- A VNIC can have a maximum of 31 secondary private IPs.
- They can be assigned only after the instance is launched (or the secondary VNIC is created/attached).
- A secondary private IP that is assigned to a VNIC in a regional subnet has a null availability domain attribute. Compare this with the VNIC's primary private IP, which always has its availability domain attribute set to the instance's availability domain, regardless of whether the instance's subnet is regional or AD-specific.
- Deleting a secondary private IP from a VNIC returns the address to the pool of available addresses in the subnet.
- They are automatically deleted when you terminate the instance (or detach/delete the secondary VNIC).
- The instance's bandwidth is fixed regardless of the number of private IP addresses attached. You can't specify a bandwidth limit for a particular IP address on an instance.
- A secondary private IP can have a reserved public IP assigned to it at your discretion.

IP Address Information in the Instance Metadata

The instance metadata includes information about the private IP addresses at this URL:

Here's an example response:

```json
[
  {
    "vnicId": "ocid1.vnic.oc1.sea.<unique_ID>",
    "privateIp": "10.0.3.6",
    "vlanTag": 11,
    "macAddr": "00:00:00:00:00:01",
    "virtualRouterIp": "10.0.3.1",
    "subnetCidrBlock": "10.0.3.0/24"
  },
  {
    "vnicId": "ocid1.vnic.oc1.sea.<unique_ID>",
    "privateIp": "10.0.4.3",
    "vlanTag": 12,
    "macAddr": "00:00:00:00:00:01",
    "virtualRouterIp": "10.0.4.1",
    "subnetCidrBlock": "10.0.4.0/24"
  }
]
```

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

For administrators: see [IAM Policies for Networking](#) on page 2832.

**Using the Console**

*To view an instance's private IPs*

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under *Core Infrastructure*, go to *Compute* and click *Instances*.
3. Click the instance to view its details.
4. Under *Resources*, click *Attached VNICS*.
   
   The primary VNIC and any secondary VNICS assigned to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under *Resources*, click *IP Addresses*.

   The VNIC's primary private IP and any secondary private IPs are displayed.

*To assign a new secondary private IP to a VNIC*

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under *Core Infrastructure*, go to *Compute* and click *Instances*.
3. Click the instance to view its details.
4. Under *Resources*, click *Attached VNICS*.

   The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under *Resources*, click *IP Addresses*.

   The VNIC's primary private IP and any secondary private IPs are displayed.
7. Click *Assign Secondary Private IP Address*. 

Networking

8. Enter the following:
   - **Private IP Address**: Optional. An available private IP address of your choice from the subnet's CIDR (otherwise the private IP address is automatically assigned).
   - **Unassign if already assigned to another VNIC**: Select this check box to force reassignment of the IP address if it's already assigned to another VNIC in the subnet. Relevant only if you specify a private IP address in the preceding field.
   - **Hostname**: Optional. A hostname to be used for DNS within the cloud network. Available only if the VCN and subnet both have DNS labels. See *DNS in Your Virtual Cloud Network* on page 2910.
   - **Public IP Type**: Whether to assign a public IP address. Available only if the VNIC is in a public subnet. See *Public IP Addresses* on page 2875.

9. Click Assign.

The secondary private IP is created and then displayed on the **IP Addresses** page for the VNIC.

10. Configure the IP address:
   - For instances running a variant of Linux, see *Linux: Details about Secondary IP Addresses* on page 2868.
   - For Windows instances, see *Windows: Details about Secondary IP Addresses* on page 2870.

**To move a secondary private IP to another VNIC in the same subnet**

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICS**.
   
The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under **Resources**, click **IP Addresses**.
   
The VNIC's primary private IP and any secondary private IPs are displayed.
7. Click **Assign Secondary Private IP Address**.
8. Enter the following:
   - **Private IP Address**: The secondary private IP address you want to move.
   - **Unassign if already assigned to another VNIC**: Select this check box to move the secondary IP address from the VNIC it's currently assigned to.
   - **Hostname**: Optional. The hostname to be used for DNS within the cloud network. Available only if the VCN and subnet both have DNS labels. See *DNS in Your Virtual Cloud Network* on page 2910.
   - **Public IP Type**: Whether to assign a public IP address. Available only if the VNIC is in a public subnet. See *Public IP Addresses* on page 2875.
9. Click Assign.

The private IP address is moved from the original VNIC to the new VNIC.

**To update the hostname for an existing private IP**

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICS**.
   
The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under **Resources**, click **IP Addresses**.
   
The VNIC's primary private IP and any secondary private IPs are displayed.
7. For the IP address you're interested in, click the Actions icon (three dots), and then click **Edit**.
8. Make your changes and click **Update**.
To delete a secondary private IP from a VNIC

**Caution:**
If the private IP is the target of a route rule, deleting it from the VNIC causes the route rule to blackhole and the traffic will be dropped.

Prerequisite: Oracle recommends removing the IP address from the OS configuration before deleting it from the VNIC. See Linux: Details about Secondary IP Addresses on page 2868 or Windows: Details about Secondary IP Addresses on page 2870.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICS.
   - The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under Resources, click IP Addresses.
   - The VNIC’s primary private IP and any secondary private IPs are displayed.
7. For the private IP you want to delete, click the Actions icon (three dots), and then click Delete Private IP.
8. Confirm when prompted.

The private IP address is returned to the pool of available addresses in the subnet.

To manage tags for a private IP

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICS.
   - The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under Resources, click IP Addresses.
   - The VNIC's primary private IP and any secondary private IPs are displayed.
7. For the private IP you're interested in, click the Actions icon (three dots), and then click View Tags. From there you can view the existing tags, edit them, and apply new ones.

For more information, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage private IPs on a VNIC, use these operations:

- **GetPrivateIp**: Use this to get a single `privateIp` object by specifying its OCID.
- **ListPrivateIps**: Use this to get a single `privateIp` object by specifying the private IP address (for example, 10.0.3.3) and the subnet's OCID. Or you can list all the `privateIp` objects in a given subnet, or just the ones assigned to a given VNIC.
- **CreatePrivateIp**: Use this to assign a new secondary private IP to a VNIC.
- **UpdatePrivateIp**: Use this to reassign a secondary private IP to a different VNIC in the same subnet, or to update the hostname or display name of a secondary private IP.
- **DeletePrivateIp**: Use this to delete a secondary private IP from a VNIC. The private IP address is returned to the subnet's pool of available addresses.

**Linux: Details about Secondary IP Addresses**

After assigning a secondary private IP to a VNIC, you must configure the OS to use it.
**Basic Commands (Not Persistent Through a Reboot)**

On the instance, run the following command. It works on all variants of Linux, for both bare metal and VM instances:

```
ip addr add <address>/<subnet_prefix_len> dev <phys_dev> label <phys_dev>:<addr_seq_num>
```

where:
- `<address>`: The secondary private IP address.
- `<subnet_prefix_len>`: The subnet's prefix length. For example, if the subnet is 192.168.20.0/24, the subnet prefix length is 24.
- `<phys_dev>`: The interface to add the address to (for example, ens2f0).
- `<addr_seq_num>`: The sequential number in the stack of addresses on the device (for example, 0).

For example:

```
ip addr add 192.168.20.50/24 dev ens2f0 label ens2f0:0
```

Later if you want to delete the address, you can use:

```
ip addr del 192.168.20.50/24 dev ens2f0:0
```

Also make sure to delete the secondary IP from the VNIC. You can do that before or after executing the above command to delete the address from the OS configuration.

**Note:**
If you've assigned a secondary IP to a secondary VNIC, and you're using policy-based routing for the secondary VNIC, make sure to configure the route rules to look up the same route table for the secondary IP address.

**Configuration File (Persistent Through a Reboot)**

You can make the configuration persistent through a reboot by adding the information to a configuration file.

**For Oracle Linux and CentOS**

Create an `ifcfg` file named `/etc/sysconfig/network-scripts/ifcfg-<phys_dev>:<addr_seq_num>`. To continue with the preceding example, the file name would be `/etc/sysconfig/network-scripts/ifcfg-ens2f0:0`, and the contents would be:

```
DEVICE="ens2f0:0"
BOOTPROTO=static
IPADDR=192.168.0.50
NETMASK=255.255.255.0
ONBOOT=yes
```

**Note:**
If you've assigned a secondary IP to a secondary VNIC, and you're using policy-based routing for the secondary VNIC, make sure to configure the route rules to look up the same route table for the secondary IP address.

**For Ubuntu**

```
auto <phys_dev>:<addr_seq_num>
iface <phys_dev>:<addr_seq_num> inet static
    address <address>
    netmask <address_netmask>
```
Networking

Where the netmask is not the prefix but the 255.255.x.x. address.

To continue with the earlier example:

```
auto ens2f0:0
iface ens2f0:0 inet static
address 192.168.0.50
netmask 255.255.255.0
```

**Note:**

If you've assigned a secondary IP to a secondary VNIC, and you're using policy-based routing for the secondary VNIC, make sure to configure the route rules to look up the same route table for the secondary IP address.

**Windows: Details about Secondary IP Addresses**

After assigning a secondary private IP to a VNIC, you must configure the OS to use it. Here are instructions for using a PowerShell script or the Network and Sharing Center UI.

**Using a PowerShell Script**

You must run PowerShell as an administrator. The script configures two things: static IP addressing on the instance and the secondary private IP. The configuration persists through a reboot of the instance.

1. In your browser, go to the Console, and note the secondary private IP address that you want to configure on the instance.
2. Connect to the instance, and run the following command at a command prompt:

   ```
ipconfig /all
   ```

3. Note the values for the following items so you can enter them into the script in the next step:
   - Default Gateway
   - DNS Servers
4. Replace the variables in the following PowerShell script with your own values:

   ```powershell
   netadapter = Get-NetAdapter -Name Ethernet
   $netadapter | Set-NetIPInterface -DHCP Disabled
   $netadapter | New-NetIPAddress -AddressFamily IPv4 -IPAddress <secondary_IP_address> -PrefixLength <subnet_prefix_length> -Type Unicast -DefaultGateway <default_gateway>
   Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses <DNS_server>
   ```

   For example:

   ```powershell
   netadapter = Get-NetAdapter -Name Ethernet
   $netadapter | Set-NetIPInterface -DHCP Disabled
   $netadapter | New-NetIPAddress -AddressFamily IPv4 -IPAddress 192.168.0.14 -PrefixLength 24 -Type Unicast -DefaultGateway 192.168.0.1
   Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 203.0.113.254
   ```
5. Save the script with the name of your choice and a `.ps1` extension, and run it on the instance.

If you run `ipconfig /all` again, you'll see that DHCP has been disabled and the secondary private IP address is included in the list of IP addresses.

Later if you want to delete the address, you can use this command:

```
Remove-NetIPAddress -IPAddress 192.168.11.14 -InterfaceAlias Ethernet
```

Also make sure to delete the secondary IP from the VNIC. You can do that before or after executing the above command to delete the address from the OS configuration.

**Using the Network and Sharing Center UI**

The following instructions configure two things: static IP addressing on the instance and the secondary private IP. The configuration persists through a reboot of the instance.

1. In your browser, go to the Console, and note the secondary private IP address that you want to configure on the instance.
2. Connect to the instance, and run the following command at a command prompt:

   `ipconfig /all`

3. Note the values for the following items so you can enter them elsewhere in a later step:
   - IPv4 Address
   - Subnet Mask
   - Default Gateway
   - DNS Servers

4. In the instance's Control Panel, open the Network and Sharing Center (see the image below for the set of dialog boxes you'll see in these steps).
5. For the active networks, click the connection (Ethernet).
6. Click Properties.
7. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties.
8. Select the radio button for **Use the following IP address**, and then enter the values you noted earlier for the IP address, subnet mask, default gateway, and DNS servers.

9. Click **Advanced....**

10. Under **IP addresses**, click **Add....**
11. Enter the secondary private IP address and the subnet mask you used earlier and click **Add**.

12. Click **OK** until the Network and Sharing Center is closed.
13. Verify the changes by returning to the command prompt and running `ipconfig /all`.

You should now see that DHCP is disabled (static IP addressing is enabled), and the secondary private IP address is in the list of addresses displayed. The address is now configured on the instance and available to use.

![Windows PowerShell](image.png)

**Note:**

You might not see the primary private IP address when you again view the properties for Internet Protocol Version 4 (TCP/IPv4) in the Network and Sharing Center UI. The best way to confirm your changes is to use `ipconfig /all` at the command line.

**Public IP Addresses**

This topic describes how to manage public IPv4 addresses on instances in a virtual cloud network (VCN).

IPv6 addressing is currently supported only in the US Government Cloud. For more information, see [IPv6 Addresses](#) on page 2889.

**Overview of Public IP Addresses**

A public IP address is an IPv4 address that is reachable from the internet. If a resource in your tenancy needs to be directly reachable from the internet, it must have a public IP address. Depending on the type of resource, there might be other requirements.

Certain types of resources in your tenancy are designed to be directly reachable from the internet and therefore automatically come with a public IP address. For example: a NAT gateway or a public load balancer. Other types of resources are directly reachable only if you configure them to be. For example: instances in your VCN.

This topic focuses on these subjects:

- The types of public IP addresses and their characteristics
- How to control whether an instance has a public IP address
For more information about resources that automatically get a public IP address, see Overview of Public IP Addresses on page 2875.

**Instances and Public IP Addresses**

You can assign a public IP address to an instance to enable communication with the internet. The instance is assigned a public IP address from the Oracle Cloud Infrastructure address pool.

The assignment is actually to a private IP object on the instance. The VNIC that the private IP is assigned to must be in a public subnet. A given instance can have multiple secondary VNICs, and a given VNIC can have multiple secondary private IPs. So you can assign a given instance multiple public IPs across one or more VNICs if you like.

For an instance to communicate directly with the internet, all of the following are required:

- The instance must be in a public subnet.
- The instance must have a public IP address.
- The instance's VCN must have an internet gateway.
- The public subnet must have route tables and security lists configured accordingly.

**Tip:**

Oracle Cloud Infrastructure FastConnect public peering lets your on-premises network access the public IP addresses of resources in Oracle Cloud Infrastructure without the traffic traversing the internet. For more information, see FastConnect on page 3173.

**The Public IP Object**

The Networking service defines an object called a public IP, which consists of these items:

- Public IPv4 address (chosen by Oracle)
- Properties that further define the public IP's type and behavior

Each public IP object has an Oracle-assigned OCID (see Resource Identifiers). If you're using the API, you can also assign each public IP object a friendly name.

**Types of Public IPs**

There are two types of public IPs:

- **Ephemeral**: Think of it as temporary and existing for the lifetime of the instance.
- **Reserved**: Think of it as persistent and existing beyond the lifetime of the instance it's assigned to. You can unassign it and then reassign it to another instance whenever you like. Exception: reserved public IPs on public load balancers. See Overview of Public IP Addresses on page 2875.

The following table summarizes the differences between the two types.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Ephemeral Public IPs</th>
<th>Reserved Public IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allowed assignment</strong></td>
<td>To a VNIC's primary private IP only</td>
<td>To either a primary or secondary private IP</td>
</tr>
<tr>
<td></td>
<td>Limits:</td>
<td>Limit: 32 per VNIC</td>
</tr>
<tr>
<td></td>
<td>• One per VNIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Two per VM instance, and 16 per bare metal instance</td>
<td></td>
</tr>
</tbody>
</table>

---

Oracle Cloud Infrastructure User Guide 2876
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Ephemeral Public IPs</th>
<th>Reserved Public IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation</td>
<td>Optionally created and assigned during instance launch or secondary VNIC creation. You can create and assign one later if the VNIC doesn't already have one.</td>
<td>You create one at any time. You can then assign it when you like. Limit: You can create 50 per region</td>
</tr>
<tr>
<td>Unassignment</td>
<td>You can unassign it at any time, which deletes it. You might do this if whoever launched the instance included a public IP, but you don't want the instance to have one. When you stop an instance, its ephemeral public IPs remain assigned to the instance.</td>
<td>You can unassign it at any time, which returns it to your tenancy's pool of reserved public IPs.</td>
</tr>
<tr>
<td>Moving to a different resource</td>
<td>You cannot move an ephemeral public IP to a different private IP.</td>
<td>If assigned to a secondary private IP: If you move the private IP to a different VNIC (must be in the same subnet), the reserved public IP goes with it. You can move it (unassign and then reassign it) at any time to another private IP in the same region. Can be in a different VCN or availability domain.</td>
</tr>
<tr>
<td>Automatic deletion</td>
<td>Its lifetime is tied to the private IP's lifetime. Automatically unassigned and deleted when: • Its private IP is deleted • Its VNIC is detached or terminated • Its instance is terminated</td>
<td>Never. Exists until you delete it.</td>
</tr>
<tr>
<td>Scope</td>
<td>Availability domain</td>
<td>Regional (can be assigned to a private IP in any availability domain in the region)</td>
</tr>
<tr>
<td>Compartment and availability domain</td>
<td>Same as the private IPs</td>
<td>Can be different from the private IPs</td>
</tr>
</tbody>
</table>

When you launch an instance in a public subnet, by default, the instance gets a public IP unless you say otherwise. See To choose whether an ephemeral public IP is assigned when launching an instance on page 2878.

After you create a given public IP, you can't change which type it is. For example, if you launch an instance that is assigned an ephemeral public IP with address 203.0.113.2, you can't convert the ephemeral public IP to a reserved public IP with address 203.0.113.2.

The preceding table notes the public IP limits per VNIC and instance. If you try to perform any operation that assigns or moves a public IP to a VNIC or instance that has already reached its public IP limit, an error is returned. The operations include:

- Assigning a public IP
Networking

- Creating a new secondary VNIC with a public IP
- Moving a private IP with a public IP to another VNIC
- Moving a public IP to another private IP

**Resources That Always Get a Public IP**

As mentioned earlier, certain types of resources are designed to be directly reachable from the internet. Examples: a NAT gateway or a public load balancer. These resources automatically get a public IP address upon creation. Oracle chooses the public IP address from the Oracle pool. You can't remove or change the address.

For public load balancers, the address is a regional reserved public IP that is assigned to a private IP on the load balancer. This public IP appears in the list of your tenancy's reserved public IPs, which you can view in the Console. However, unlike other reserved public IPs that you create, you have no control over this public IP. You can't edit it or unassign it from the load balancer yourself. It's automatically unassigned and deleted from your tenancy when you terminate the load balancer.

For NAT gateways, the address is a regional ephemeral public IP that is assigned to the NAT gateway. Like other ephemeral public IPs, it's automatically unassigned and deleted when you terminate its assigned resource (the NAT gateway). However, unlike other ephemeral public IPs, you can't edit it or unassign it yourself.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

**Ephemeral Public IPs: Using the Console**

To choose whether an ephemeral public IP is assigned when launching an instance

When you launch an instance into a public subnet, there's an Assign a public IPv4 address check box on the Create Compute Instance page. By default, the check box is selected, which means the instance gets an ephemeral public IP.

If you do NOT want an ephemeral public IP assigned, you can either:

- Select the Do not assign a public IPv4 address option
- Delete the ephemeral public IP after instance launch

To assign an ephemeral public IP when creating a secondary VNIC

When you add a secondary VNIC to an instance, you choose whether the primary private IP on the new VNIC gets an ephemeral public IP. This choice is available only if the secondary VNIC is in a public subnet.

In the Create VNIC dialog box, there's an Assign a public IPv4 address check box. By default, the check box is NOT selected, which means the secondary VNIC does not get an ephemeral public IP. You must select the check box.

For instructions, see Connectivity Choices on page 2752.

To assign an ephemeral public IP to an existing primary private IP

Prerequisite: The primary private IP must not have a reserved or ephemeral public IP already assigned to it. If it does, first delete the ephemeral public IP, or unassign the reserved public IP.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICS.
   - The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under **Resources**, click **IP Addresses**.

   The VNIC's primary private IP and any secondary private IPs are displayed.

7. For the VNIC's primary private IP, click the Actions icon (three dots), and then click **Edit**.

8. In the **Public IP Address** section, for **Public IP type**, select the radio button for **Ephemeral Public IP**.

9. In the **Ephemeral Public IP Name** field, enter an optional friendly name for the public IP. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.

10. Click **Update**.

**To delete an ephemeral public IP from an instance**

Deleting an ephemeral public IP automatically unassigns it from its private IP.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICs**.

   The primary VNIC and any secondary VNICs attached to the instance are displayed.

5. Click the VNIC you're interested in.
6. Under **Resources**, click **IP Addresses**.

   The VNIC's primary private IP and any secondary private IPs are displayed.

7. For the VNIC's primary private IP, click the Actions icon (three dots), and then click **Edit**.

8. In the **Public IP Address** section, for **Public IP Type**, select the radio button for **No Public IP**.

9. Click **Update**.

**To change the display name for an ephemeral public IP**

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICs**.

   The primary VNIC and any secondary VNICs attached to the instance are displayed.

5. Click the VNIC you're interested in.
6. Under **Resources**, click **IP Addresses**.

   The VNIC’s primary private IP and any secondary private IPs are displayed.

7. For the VNIC’s primary private IP, click the Actions icon (three dots), and then click **Edit**.

8. In the **Public IP Address** section, edit the **Ephemeral Public IP Name**. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.

9. Click **Update**.

**Reserved Public IPs: Using the Console**

**To view your reserved public IPs**

1. Confirm you're viewing the region and compartment you're interested in.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking**, go to **IP Management**, and click **Public IPs**.

   The details of the reserved public IPs in the selected region and compartment are displayed. If the reserved public IP is assigned, there's a link to the relevant VNIC.

**To create a new reserved public IP in your pool**

1. Confirm you're viewing the region and compartment where you want to create the reserved public IP.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking**, go to **IP Management**, and click **Public IPs**.
3. Click **Create Reserved Public IP**.
4. Enter the following:
   - **Name**: An optional friendly name for the reserved public IP. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - **Compartment**: Leave as is.
   - **IP Pool**: (optional) The IP pool the reserved public IP is drawn from. If you don't select a pool you've created, the default Oracle pool is used.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Create Reserved Public IP**.

The new reserved public IP is created and displayed on the page. You can now assign it to an existing private IP if you like.

*To delete a reserved public IP from your pool*

The reserved public IP can be in the "Assigned" state. Deleting a reserved public IP automatically unassigns it from its private IP.

1. Confirm you're viewing the region and compartment that contains the reserved public IP.
2. Open the navigation menu. Under Core Infrastructure, go to Networking, go to IP Management, and click Public IPs.
3. For the reserved public IP you want to delete, click the Actions icon (three dots), and then click **Terminate**.
4. Confirm when prompted.

After a few seconds, the reserved public IP is unassigned (if it was assigned) and deleted from your pool.

*To assign a reserved public IP to a private IP*

Prerequisite: The private IP must not have an ephemeral or reserved public IP already assigned to it. If it does, first delete the ephemeral public IP, or unassign the reserved public IP.

1. Confirm you're viewing the compartment that contains the instance with the private IP you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICs.
   
   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. Click the VNIC that you're interested in.
6. Under Resources, click IP Addresses.

   The VNIC's primary private IP and any secondary private IPs are displayed.
7. For the private IP you're interested in, click the Actions icon (three dots), and then click **Edit**.
8. In the Public IP Type section, select the radio button for Reserved Public IP.
9. For **Reserved Public IP**, enter the reserved public IP you want to assign. You have three choices:
   - Create a new reserved public IP. You can optionally provide a friendly name for it. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - Assign a reserved public IP that isn't already assigned.
   - Move a reserved public IP from another private IP.
10. Click **Update**.

*To unassign a reserved public IP and return it to the pool*

1. Confirm you're viewing the compartment that contains the instance with the reserved public IP you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICS**.
   The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC you're interested in.
6. Under **Resources**, click **IP Addresses**.
   The VNIC's primary private IP and any secondary private IPs are displayed.
7. For the private IP you're interested in, click the Actions icon (three dots), and then click **Edit**.
8. In the **Public IP Address** section, for **Public IP Type**, select the radio button for **No Public IP**.
9. Click **Update**.

The reserved public IP is unassigned and returned to your pool.

*To move a reserved public IP from one private IP to another*

Let's say you want to move a reserved public IP from private IP 1 to private IP 2. In summary: Make sure private IP 2 doesn't have a public IP already assigned to it. Then assign the reserved public IP to private IP 2. It will be automatically unassigned from private IP 1 first. Detailed instructions:

1. Confirm you're viewing the compartment that contains the instance with private IP 2.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the instance to view its details.
4. Under **Resources**, click **Attached VNICS**.
   The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC you're interested in.
6. Under **Resources**, click **IP Addresses**.
   The VNIC's primary private IP and any secondary private IPs are displayed.
7. For private IP 2, click the Actions icon (three dots), and then click **Edit**.
8. If private IP 2 already has a public IP assigned to it:
   a. In the **Public IP Type** section, select the radio button for **No Public IP**.
   b. Click **Update**.
   c. Again for private IP 2, click the Actions icon (three dots), and then click **Edit**.
9. In the **Public IP Type** section, select the radio button for **Reserved Public IP**.
10. In the **Reserved Public IP** list, select the reserved public IP that you want to assign. It will be moved from the public IP it's currently assigned to.
11. Click **Update**.

*To change the display name for a reserved public IP*

1. Confirm you're viewing the region and compartment that contains the reserved public IP.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking**, go to **IP Management**, and click **Public IPs**.
3. For the reserved public IP you want to edit, click the Actions icon (three dots), and then click **Edit**.
4. Make your changes to the friendly name. The name doesn't have to be unique, and you can change it later. Avoid entering confidential information.
5. Click **Save**.

*To manage tags for a reserved public IP*

1. Confirm you're viewing the region and compartment that contains the reserved public IP.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking**, go to **IP Management**, and click **Public IPs**.
3. For the reserved public IP you're interested in, click the Actions icon (three dots), and then click **View Tags**. From there you can view the existing tags, edit them, and apply new ones.

For more information, see **Resource Tags** on page 211.
To move a reserved public IP to a different compartment

You can move a reserved public IP from one compartment to another. When you move a reserved public IP to a new
compartment, inherent policies apply immediately.

1. Open the navigation menu. Under Core Infrastructure, go to Networking, go to IP Management, and click Public IPs.
2. For the reserved public IP you're interested in, click the Actions icon (three dots), and then click Move Resource.
3. Choose the destination compartment from the list.
4. Click Move Resource.

For more information about using compartments and policies to control access to your cloud network, see Access Control on page 2831. For general information about compartments, see Managing Compartments on page 2431.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage public IPs, use these operations:

- **GetPublicIp**: Use this to get a publicIp object by specifying its OCID.
- **GetPublicIpByIpAddress**: Use this to get a publicIp object by specifying its public IP address.
- **GetPublicIpByPrivateIpId**: Use this to get a publicIp object by specifying the OCID of the private IP it's assigned to.
- **ListPublicIps**: Use this to list either your ephemeral or reserved publicIp objects.
- **CreatePublicIp**: Use this to create a new reserved public IP in your pool.
- **UpdatePublicIp**: Use this to assign, reassign, or unassign a reserved public IP, or to update the display name of an ephemeral or reserved public IP. You can also update a reserved public IP's tags.
- **DeletePublicIp**: Use this to delete an ephemeral public IP from its private IP, or delete a reserved public IP from your pool. The operation first unassigns the public IP.
- **ChangePublicIpCompartment**: Use this to move a reserved public IP from one compartment to another. This operation applies only to reserved public IPs. Ephemeral public IPs always belong to the same compartment as their VNIC and move accordingly.

Bring Your Own IP

Oracle Cloud Infrastructure allows you to Bring Your Own IP (BYOIP) address space to use with resources in Oracle Cloud Infrastructure, in addition to using Oracle owned addresses. BYOIP lets you manage your IPv4 CIDR blocks to align with your existing security, management, and deployment policies and achieve:

- **Solution continuity and hardcoded dependencies**: Your VCN is an extension of your public Internet presence, without needing to reinvent policies and management processes. If you have IP addresses hard-coded in devices or built architectural dependencies on specific IP addresses, using BYOIP you have a smooth migration to Oracle Cloud Infrastructure.
- **IP pool management**: Some network administrators require the ability to summarize groups of IP addresses into pools and to create resources for deployment such as load balancers, firewalls, or web servers. IP Pool management provides tools to manage reserved public IP addresses.
- **IP reputation**: Some Internet services rely on a contiguous IP address space (such as a full span of IP addresses from 1 through 255) and act as a trusted contact point between services such as major email service providers and mail delivery systems.

Oracle performs a validation process on imported CIDR blocks, and after validation you are notified that the CIDR block is available for advertisement. You can also create one or many public IP pools from this address space by specifying subranges from the BYOIP CIDR block and use IP pools to allocate specific resources. You can start or stop advertisement of the BYOIP routes when needed.
Networking

Requirements and Preparation

• You must have ownership of the public IPv4 CIDR block you want to import into Oracle Cloud Infrastructure, and the ownership must be registered with a supported Regional Internet Registry (RIR). Oracle validates ownership of your addresses. Only the following registries are supported, and the addresses must have a specified type or status:
  • American Registry for Internet Numbers (ARIN) - "Direct Allocation" and "Direct Assignment" network types
  • Réseaux IP Européens Network Coordination Centre (RIPE NCC) - "ALLOCATED PA," "LEGACY," "ASSIGNED PI," and "ALLOCATED-BY-RIR" allocation statuses
  • Asia-Pacific Network Information Centre (APNIC) – "ALLOCATED PORTABLE" and "ASSIGNED PORTABLE" allocation statuses
• The addresses in the IP address range must have a clean history. We might investigate the reputation of the IP address range and reserve the right to reject an IP address range that contains an IP address that is associated with malicious behavior.

Limits and Quotas

• Your addresses can only be imported to a specific Oracle region.
• You can use BYOIP with a CIDR block that is a minimum of /24 and a maximum of /8.
• You can't bring the same address range to more than one compartment at a time.
• A CIDR block that is /24 or smaller is required for addresses to be advertised to the Internet.
• You can bring up to 10 IPv4 address ranges to your OCI account.
• BYOIP is not available to Oracle Cloud Infrastructure Free Tier or Pay As You Go services.

BYOIP Process Overview

The steps needed for BYOIP in Oracle Cloud Infrastructure require significant time, so plan accordingly. The process is shown in the following diagram:
1. You request to import a public IPv4 CIDR block you own.

2. Oracle issues a verification token.

3. You modify and add the verification token to the information about that public IPv4 CIDR block kept by your RIR service. The details vary depending on the RIR. It can take up to one day for the update to take effect. If you move to the next step before that update takes effect, a day will be added to the total time to complete the process. See To import a BYOIP CIDR block on page 2885 for details.

4. Create a Route Origin Authorization (ROA) with your RIR. As part of the ROA, provide the Oracle BGP ASN (31898 for the commercial cloud). This allows Oracle to advertise the BYOIP CIDR block.

5. Request that Oracle finish the import request, creating a workflow that could take up to 10 days to complete, where Oracle communicates with the RIR and verifies that you own the IP addresses in the CIDR block.
6. Oracle provisions the BYOIP CIDR block to your VCN.
7. At this point, the BYOIP CIDR block is yours to manage in your VCN. You can add addresses to an IP pool, and then use them as reserved IP addresses. You can also advertise the IP addresses to the internet.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

**Limits on IAM Resources**

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

**Managing BYOIP using the console**

*To import a BYOIP CIDR block*

1. From the BYOIP list page, click Import BYOIP CIDR Block. The Import BYOIP CIDR Block screen appears.
2. In the Import BYOIP CIDR Block screen, enter a name for the BYOIP CIDR Block, choose the compartment, and enter the CIDR block you intend to bring to your tenancy. Avoid entering confidential information.
3. Click Save Changes. The details page for that BYOIP import request appears.
4. In the Next Steps section, make a copy of the validation token. Modify the token slightly, adding the following information as shown. You can use any text editor.

   OCITOKEN::<CIDRblock>::<validation_token>

   The completed token string might look something like: OCITOKEN::10.0.0.0/24:abcdefghij

5. Create a Route Origin Authorization (ROA) object that authorizes Oracle to advertise the BYOIP CIDR block. The Oracle BGP ASN is 31898 for the commercial cloud. For the US Government Cloud, see Oracle's BGP ASN on page 154. Set an expiry date at least 6 months in the future. Follow the instructions appropriate for your RIR.

   - **ARIN**: ROA Requests
   - **RIPE NCC**: Managing ROAs
   - **APNIC**: Route/ROA management

   **Note:**

   If you do not create an ROA, Oracle can't advertise the BYOIP CIDR block. Without being able to advertise the routes, there may be little point in importing them.

6. Now add the modified validation token to the RIR account information associated with your address range. Each RIR uses a slightly different method:

   - **ARIN**: Add the modified token string in the "Public Comments" section associated with your address range.
   - **RIPE NCC**: Add the modified token string as a new "descr" field associated with your address range.
   - **APNIC**: Add the modified token string to the "remarks" field for your address range by emailing it to helpdesk@apnic.net. The email must be sent from the APNIC authorized contact account for the IP address range.

   **Note:**

   The modified validation string must be associated with the address range information. Do not add it to the information for the organization that owns the address range.
7. Wait until both the ROA and the token registration is complete (up to a day) before you click the **Finish Import** button. Otherwise, the process can be delayed up to one day.

8. Return to the details page for the BYOIP request and click **Finish Import**. A confirmation screen appears.

9. Click **Finish Import**, confirming that you would like to validate the BYOIP request. Allow up to 10 days for Oracle to contact your RIR, validate the import, and provision the CIDR block. View the work requests to see the status.

**To view your BYOIP CIDR blocks**

1. Confirm you are viewing the region and compartment you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to **Networking**, go to **IP Management**, and click **BYOIP**.

**To rename a BYOIP CIDR block**

1. In the details page for that BYOIP CIDR block, click **Rename**. A window appears.
2. In the window, enter the new name. Avoid entering confidential information.
3. Click **Save Changes**.

**To remove a BYOIP CIDR block from a pool**

- **Note:**
  
  To successfully remove a BYOIP CIDR block from a pool, there must be no reserved public IP addresses in that address range. You may have to terminate one or more reserved public IP addresses.

1. In the details page for your BYOIP CIDR block, click on the Action Icon corresponding to the subrange you want to remove from a public IP pool, and then click on **Remove from Public IP Pool**. A confirmation window appears.
2. If you are sure you want to delete the BYOIP CIDR block, click **Remove CIDR Block**.

**To delete a BYOIP CIDR block**

To successfully delete a BYOIP CIDR block, it must be in the CREATING, PROVISIONED, ACTIVE, or FAILED state, and it must not have any subranges added to public IP pools.

- **Note:**
  
  If you delete a BYOIP CIDR block, you need to repeat the import process to undo your action.

1. In the details page for your BYOIP CIDR block, click **Delete**. A confirmation window appears.
2. If you are sure you want to delete the BYOIP CIDR block, click **Delete BYOIP CIDR block**.

**To advertise a BYOIP CIDR block**

A BYOIP CIDR block must be provisioned before it can be advertised.

- **Note:**
  
  The BYOIP CIDR block is advertised using a BGP ASN owned by Oracle. Oracle's BGP ASN for the commercial cloud is 31898.

1. In the details page for your BYOIP CIDR block, click **Advertise**. A confirmation window appears.
2. In the confirmation window, click **Advertise**.

**To withdraw a BYOIP CIDR block**

1. In the details page for a BYOIP CIDR block currently being advertised, click **Withdraw**. A confirmation window appears.
2. In the confirmation window, click on **Withdraw**.
To divide a BYOIP CIDR block and assign subranges to a public IP pool

1. From a BYOIP detail page, scroll down to the BYOIP CIDR Block Subranges section and click Manage BYOIP CIDR Block. The Manage BYOIP CIDR Blocks screen appears.
2. Either by entering a number for the CIDR suffix or using the up/down arrows next to the suffix, change the suffix number (often a /24). New rows in the table appear, representing possible subranges within the entire CIDR block.
3. For each of the newly created subranges of the BYOIP CIDR block, check the box in the first column of the table and click Add BYOIP CIDR Blocks to Public IP Pools.
   a. Choose whether to Select an Existing Public IP Pool or Create New Public IP Pool.
      - Select an Existing Public IP Pool: Choose an existing IP pool using the selection list.
      - Create New Public IP Pool: Assign the new pool a name and choose a compartment. You can move the public IP pool to another compartment later. Avoid entering confidential information.
   b. Click Add BYOIP CIDR Blocks to Public IP Pools
4. Repeat the previous step until all subranges of the BYOIP CIDR block are assigned to a public IP pool, then click Submit.

**Note:**
If a subrange of a BYOIP CIDR block is left unassigned to a pool, the table may look different after you click Submit.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage the ByoipRange object, use these operations:
- AdvertiseByoipRange
- ChangeByoipRangeCompartment
- CreateByoipRange
- DeleteByoipRange
- GetByoipRange
- ListByoipRanges
- UpdateByoipRange
- ValidateByoipRange
- WithdrawByoipRange

IP Pools

A public IP pool is simply a set of CIDR blocks allocated to a tenancy. These CIDR blocks can be all or part of a BYOIP CIDR block. Public IP CIDR blocks assigned to a pool are only available for your tenancy. Public IP pools are available as a source for IP allocation when launching a NAT gateway, load balancer, or compute instance. You can add more IP CIDR blocks to a public IP pool at any time. You can also:
- Create a Reserved IP: You can reserve individual IPs from your public IP pools. These reserved IP addresses can be attached to your resources.
- Direct launch from pool: You can launch resources with an IP directly allocated from a public IP pool without previously creating a reserved IP for that resource.
- Delete CIDR blocks and pools: You can delete the entire public IP pool or certain IP CIDR blocks within the pool, provided none of the IP addresses are currently attached or reserved.

Requirements and Preparation
- To use public IP pools with BYOIP addresses, you need to import your addresses.
- To reserve Oracle-supplied public IP addresses, select “Oracle” as the public IP pool when creating the reserved public IP address.
Limits and quotas

- You can create one or up to 10 public IP pools in a compartment.
- A public IP pool can have zero or more IP CIDR ranges assigned to it, with a minimum size of /28 to a maximum size of /24.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

Limits on IAM Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Managing IP pools using the console

To view your public IP pools

1. Confirm you're viewing the region and compartment you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Networking, go to IP Management, and click Public IP Pools.

To create a public IP pool

1. From the Public IP Pools list view, click Create Public IP Pool. The Create Public IP Pool screen appears.
2. Give the pool a name. Avoid entering confidential information.
3. Assign the Public IP pool to a compartment.
4. Click Create Public IP Pool.

To delete a public IP pool

1. From the Public IP Pools list view, select a public IP pool from the list and click Delete Public IP Pool. The Delete Public IP Pool verification screen appears.
2. If there are no warnings or errors, click Delete Public IP Pool. If this public IP pool contains reserved public IP addresses currently in use, you can't delete the public IP pool.

To rename a public IP pool

1. From the details view for a public IP pool, click Rename Public IP Pool.
2. Enter a new name for the public IP pool. Avoid entering confidential information.
3. Click Save Changes.

To add CIDR blocks to a public IP pool

1. From the details view for a public IP pool, click Add CIDR Blocks.
2. Choose a named BYOIP CIDR block.
3. Click Add CIDR Blocks.

To remove CIDR blocks from an IP pool

Note:

To successfully remove a BYOIP CIDR block from a public IP pool, there must be no reserved public IP addresses from that address range. You may have to terminate one or more reserved public IP addresses.
Networking

1. In the details page for your BYOIP CIDR block, click the Action Icon corresponding to the subrange you want to remove from a public IP pool, and then click Remove from Public IP Pool. A confirmation window appears.
2. If you are sure you want to delete the BYOIP CIDR block, click Remove CIDR Block.

To reserve a public IP

1. In the details page for a public IP pool, click the Create Reserved Public IP button.
2. Enter a name and specify the compartment for the new reserved public IP address. Avoid entering confidential information.
3. When finished, click Create Reserved Public IP.

To move a public IP pool to another compartment

1. From the details view for an IP pool, click the Move Public IP Pool button. An input screen appears.
2. Choose a new compartment for the public IP pool.
3. Click Move Public IP Pool.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage the Public IP Pool object, use these operations:

- AddPublicIpPoolCapacity
- ChangePublicIpPoolCompartment
- CreatePublicIpPool
- DeletePublicIpPool
- GetPublicIpPool
- ListPublicIpPools
- RemovePublicIpPoolCapacity
- UpdatePublicIpPool

IPv6 Addresses

This topic describes support for IPv6 addressing in your VCN.

Highlights

- IPv6 addressing is currently supported only in the US Government Cloud. See For All US Government Cloud Customers on page 148.
- During VCN creation, you choose whether the VCN is enabled for IPv6. You also choose whether each subnet in an IPv6-enabled VCN is enabled for IPv6. You cannot change whether a VCN or subnet is IPv6-enabled after creation.
- IPv6-enabled VCNs use a /56 IPv6 CIDR block. Oracle assigns a /56 public IPv6 CIDR block to the VCN for internet communication. You can either let the private IPv6 CIDR block be the same as the public CIDR, or provide your own value (in which case it's referred to as a custom IPv6 CIDR). All subnets are /64.
- You also choose whether a given VNIC in an IPv6-enabled subnet has IPv6 addresses (up to 32 maximum per VNIC), and whether each address can be used for internet communication.
- You can choose which particular IPv6 address in the subnet is assigned to a VNIC. This means you can plan how the VCN's private and public address space is allocated within your organization.
- Only these Networking gateways support IPv6 traffic: dynamic routing gateway (DRG) and internet gateway.
- Both inbound- and outbound-initiated IPv6 connections are supported between your VCN and the internet, and between your VCN and your on-premises network.
- Private IPv6 traffic between resources within a region (intra- and inter-VCN) is not yet supported. See other important details in Routing for IPv6 Traffic on page 2896.
- Both FastConnect and IPSec VPN support IPv6 traffic between your VCN and on-premises network. You must configure the FastConnect or IPSec VPN for IPv6.
Overview of IPv6 Addresses

Oracle supports dual-stack IPv4/IPv6 addressing for VCNs. Every VCN always supports IPv4, and you can optionally enable IPv6 during VCN creation. Enabling IPv6 for the VCN means that when you create a subnet, you can optionally enable it to also have IPv6 addresses. Therefore a VCN can have a mix of IPv4-only subnets and IPv6-enabled subnets.

After you create a Compute instance, you may optionally add an IPv6 to the VNIC. You can add up to 32 IPv6s to a given VNIC. You can remove an IPv6 from a VNIC at any time.

CIDRs Assigned to an IPv6-Enabled VCN

An IPv6-enabled VCN has 3 CIDR blocks assigned to it. The following table summarizes them.

<table>
<thead>
<tr>
<th>IPv4 or IPv6</th>
<th>Use and Size</th>
<th>Who Assigns the CIDR Block</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private IPv4 CIDR</td>
<td>Private communication</td>
<td>You</td>
<td>Typically RFC 1918 range</td>
</tr>
<tr>
<td></td>
<td>/16 to /30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private IPv6 CIDR*</td>
<td>On-premises communication&lt;br&gt;Only /56</td>
<td>Optionally, you can assign it. If you do, it's referred to in this documentation as a custom IPv6 CIDR. Or, you can let Oracle assign it.</td>
<td>If you assign it, see <a href="#">Overview of IPv6 Addresses</a> on page 2890.</td>
</tr>
<tr>
<td>Public IPv6 CIDR</td>
<td>Internet communication&lt;br&gt;Only /56</td>
<td>Oracle</td>
<td>If you assign the VCN's private IPv6 CIDR, it will be different from the public IPv6 CIDR that Oracle assigns. But if you let Oracle assign the VCN's private IPv6 CIDR, Oracle uses the same CIDR for both the private and public IPv6 CIDRs. That means the private address and public address for a given IPv6 are the same.</td>
</tr>
</tbody>
</table>

* Oracle assigns IPv6 CIDR blocks that are NOT in the IPv6 unique local address (ULA) range. This range is analogous to the IPv4 RFC 1918 private ranges. Therefore, all Oracle-assigned IPv6 CIDRs can be considered public ranges by this definition.
Allowed Custom IPv6 CIDR Ranges

Your custom IPv6 CIDR block can be in these general ranges:

- Global unicast: 2000::/3
- ULA: fc00::/7

But it cannot be in these IANA special registry ranges:

- IETF protocol assignments: 2001::/23
- Documentation: 2001:db8::/32
- 6to4: 2002::/16
- Direct Delegation AS112 Service: 2620:4f:8000::/56

Internet Communication

Regardless of whether you or Oracle assigns the VCN's private IPv6 CIDR, Oracle also assigns the VCN an IPv6 CIDR block for the public IP address space (the public IPv6 CIDR). These addresses are used for internet communication. If you do not assign a custom CIDR, Oracle uses the same Oracle-assigned public IPv6 CIDR for the private address space. This means that a given VNIC might use the same IPv6 IP address for both private and internet communication.

You control whether a given IPv6 address can be used for internet communication. If the IPv6 is in a private subnet, it can never be used for internet communication. If it's in a public subnet, you can enable or disable internet access for that IPv6 at any time. If internet access is enabled, the IPv6 uses its public IPv6 address for communication.

Assignment of IPv6 Addresses to a VNIC

To enable IPv6 for a given VNIC, you assign an IPv6 to the VNIC. You can assign up to 32 IPv6s to a VNIC.

As with IPv4, when assigning an IPv6, you can specify the particular address you want to use, or let Oracle choose one for you. By choosing the IPv6 addresses yourself, you can plan how the VCN's private and public address space is allocated within your organization.

You also choose whether the IPv6 has internet access enabled (it is enabled by default if the VNIC is in a public subnet). A VNIC with an internet-enabled IPv6 is not required to have a public IPv4 address.

You can move an IPv6 address from one VNIC to another in the same subnet.

After adding an IPv6 to a VNIC, you must configure the instance's OS to use the IPv6.

Format of IPv6 Addresses

IPv6 addresses have 128 bits.

An IPv6 CIDR block for a VCN must be /56 in size. The left 56 bits identify the VCN portion of the address. For example:

2001:0db8:0123::/56

An IPv6 CIDR block for a subnet must be /64 in size. The right 16 bits in a subnet's CIDR identify the subnet portion of the address. In the following example, the 1111 is the unique portion for the subnet:

2001:0db8:0123:1111::/64

The right-most 64 bits of an IPv6 address identify the unique portion specific to the particular IPv6 address. For example:


For a given IPv6, those right-most 64 bits are identical for both the private and public address for an IPv6. When you assign an IPv6 to a VNIC, you can specify which specific IPv6 address to use (those 64 bits). Therefore you can control how the private and public address space is allocated within your organization.
**Example 1: You assign a custom CIDR**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle recommends this option if you want instances within the same IPv6-enabled VCN to communicate with each other using public IPv6 addresses. For more information, see Routing for IPv6 Traffic on page 2896.</td>
</tr>
</tbody>
</table>

Let's say you provide this custom IPv6 CIDR: fd00:aaaa:0123::/56.

Oracle assigns a separate CIDR block for the VCN's public CIDR: 2001:0db8:9999::/56.

The following diagram illustrates the VCN and includes two subnets: public subnet 1111 and private subnet 1112.
The VNIC in the public subnet has a primary private IPv4 (10.0.1.4) with an optional public IP address assigned. The VNIC has a secondary private IPv4 (10.0.1.5), also with an optional public IP address assigned.

The VNIC also has two IPv6s. The first one has internet access enabled and therefore has both private and public IPv6 addresses, which are the following:
• Private IPv6 address: fd00:aaaa:0123:1111:abcd:ef01:2345:0006
• Public IPv6 address: 2001:0db8:9999:1111:abcd:ef01:2345:0006

Notice that the right-most 64 bits are the same for both the private and public IP address, as are the subnet's 16 bits. Only the left 48-most bits differ.

The second IPv6 in the public subnet does not have internet access enabled and therefore has only a private IP address, which is fd00:aaaa:0123:1111:abcd:ef01:2345:0007.

The second subnet is private, which means the VNICS can never have public IPv4 or IPv6 addresses. In this case, there's one VNIC that has a primary and secondary IPv4 with addresses 10.0.2.4 and 10.0.2.5, respectively.

The VNIC also has two IPv6s. The first has private address fd00:aaaa:0123:1112:abcd:ef01:2345:0006, and the second IPv6 has private address fd00:aaaa:0123:1112:abcd:ef01:2345:0007.

Example 2: You let Oracle assign the VCN's CIDR

You do not assign a custom CIDR, and Oracle assigns this CIDR: 2001:0db8:0123::/56. Oracle uses this same CIDR for both the private and public IP addresses.

The following diagram illustrates the VCN and includes two subnets: public subnet 1111 and private subnet 1112.
Networking

The VNIC in the public subnet has a primary private IPv4 (10.0.1.4) with an optional public IP address assigned. The VNIC has a secondary private IPv4 (10.0.1.5), also with an optional public IP address assigned.

The VNIC also has two IPv6s. The first one has internet access enabled and therefore has both private and public IPv6 addresses, which are the following:

- **Private IPv6**: 2001:0db8:0123:1111::abcd:ef01:2345:0006
  - **Internet access**: YES
- **Public IPv6**: 2001:0db8:0123:1111::abcd:ef01:2345:0006
- **Private IPv6**: 2001:0db8:0123:1111::abcd:ef01:2345:0007
  - **Internet access**: NO

The VNIC in the public subnet has a primary private IPv4 (10.0.1.4) with an optional public IP address assigned. The VNIC has a secondary private IPv4 (10.0.1.5), also with an optional public IP address assigned.

The VNIC also has two IPv6s. The first one has internet access enabled and therefore has both private and public IPv6 addresses, which are the following:
Networking


Notice that the two addresses are the same.

The second IPv6 does not have internet access enabled and therefore has only a private IP address, which is 2001:0db8:0123:1111:abcd:ef01:2345:0007.

The second subnet is private, which means the VNICs can never have public addresses, IPv4 or IPv6. In this case, there's one VNIC that has a primary and secondary IPv4 with addresses 10.0.2.4 and 10.0.2.5, respectively.

The VNIC also has two IPv6s. The first has private address 2001:0db8:0123:1112:abcd:ef01:2345:0006, and the second IPv6 has private address 2001:0db8:0123:1112:abcd:ef01:2345:0007.

Routing for IPv6 Traffic

Both inbound- and outbound-initiated IPv6 connections are supported between your VCN and the internet, and between your VCN and your on-premises network.

Here are other important details about routing of IPv6 traffic:

- Currently IPv6 traffic is supported only through these gateways:
  - **Dynamic routing gateway (DRG):** For access to your on-premises network or other networks outside the region. Both Oracle Cloud Infrastructure FastConnect and IPSec VPN support IPv6 traffic. For more details about IPv6 configuration, see the upcoming sections.
  - **Internet gateway:** For access to the internet.
- Traffic between instances on their public IPv6 addresses is supported and must traverse the VCN’s internet gateway. Exception: if the given IPv6 uses the same address for both private and public communication, traffic between instances on their public IPv6 address is not supported. Therefore, if you want instances in the same VCN to communicate with each other using public IPv6 addresses, specify your own private IPv6 CIDR when creating the VCN. This means the private address for an IPv6 in the VCN will be different than its public address. For more information, see Overview of IPv6 Addresses on page 2890.
- Private IPv6 traffic between resources within a region (intra- and inter-VCN) is not yet supported.

VCN Route Tables and IPv6

The VCN’s route tables support both IPv4 rules and IPv6 rules that use a DRG or internet gateway as the target. For example, the route table for a given subnet could have these rules:

- Rule to route traffic that matches a certain IPv4 CIDR to the VCN’s attached DRG
- Rule to route traffic that matches a certain IPv4 CIDR to the VCN’s service gateway
- Rule to route traffic that matches a certain IPv4 CIDR to the VCN’s NAT gateway
- Rule to route traffic that matches a certain IPv6 CIDR to the VCN’s attached DRG
- Rule to route traffic that matches a certain IPv6 CIDR to the VCN’s attached internet gateway

Security Rules for IPv6 Traffic

Like route tables, the VCN’s network security groups and security lists Security Rules on page 2833 support both IPv4 and IPv6 rules. For example, a network security group or security list could have these security rules:

- Rule to allow SSH traffic from the on-premises network's IPv4 CIDR
- Rule to allow ping traffic from the on-premises network's IPv4 CIDR
- Rule to allow SSH traffic from the on-premises network's **IPv6** CIDR
- Rule to allow ping traffic from the on-premises network's **IPv6** CIDR

The default security list in an IPv6-enabled VCN includes default IPv4 rules and the following default IPv6 rules:

- **Stateful ingress:** Allow IPv6 TCP traffic on destination port 22 (SSH) from source ::/0 and any source port. This rule makes it easy for you to create a new VCN with a public subnet and internet gateway, create a Linux instance,
add an internet-access-enabled IPv6, and then immediately connect with SSH to that instance without needing to write any security rules yourself.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
</table>
| The default security list does not include a rule to allow Remote Desktop Protocol (RDP) access. If you're using Windows images, add a stateful ingress rule for TCP traffic on destination port 3389 from source ::/0 and any source port.  
See To enable RDP access for more information. |

- **Stateful ingress**: Allow ICMPv6 traffic type 2 code 0 (Packet Too Big) from source ::/0 and any source port. This rule enables your instances to receive Path MTU Discovery fragmentation messages.
- **Stateful egress**: Allow all IPv6 traffic. This allows instances to initiate IPv6 traffic of any kind to any destination. Notice that this means the instances with an internet-access-enabled IPv6 can talk to any internet IPv6 address if the VCN has a configured internet gateway. And because stateful security rules use connection tracking, the response traffic is automatically allowed regardless of any ingress rules. For more information, see Stateful Versus Stateless Rules on page 2839.

**FastConnect and IPv6**

If you use *FastConnect*, you can configure it so that on-premises hosts with IPv6 addresses can communicate with an IPv6-enabled VCN. In general, you must ensure that the FastConnect virtual circuit has IPv6 BGP addresses, and update the VCN's routing and security rules for IPv6 traffic.

**About the IPv6 BGP Addresses**

A FastConnect virtual circuit always requires IPv4 BGP addresses, but IPv6 BGP addresses are optional and only required for IPv6 traffic. Depending on how you're using FastConnect, you might be asked to provide all of the virtual circuit's BGP addresses yourself (both IPv4 and IPv6).

The addresses consist of a pair: one for your end of the BGP session, and another for the Oracle end of the BGP session.

When you specify a BGP address pair, you must include a subnet mask that contains both of the addresses. Specifically for IPv6, the allowed subnet masks are:

- /64
- /96
- /126
- /127

For example, you could specify 2001:db8::6/127 for the address at your end of the BGP session, and 2001:db8::7/127 for the Oracle end.

**Process to Enable IPv6**

In general, here's how to enable IPv6 for a FastConnect virtual circuit:

- **Virtual circuit BGP**: Ensure the FastConnect virtual circuit has IPv6 BGP addresses. If you're responsible for providing the BGP IP addresses, when you set up a new virtual circuit or edit an existing one, there's a place for the two IPv4 BGP addresses. There's a separate check box for Enable IPv6 Address Assignment and a place to provide the two IPv6 addresses. Be aware that if you're editing an existing virtual circuit to add support for IPv6, it will go down while it's being reprovisioned to use the new BGP information.

- **VCN route tables**: For each IPv6-enabled subnet in the VCN, update its route table to include rules that route the IPv6 traffic from the VCN to the IPv6 subnets in your on-premises network. For example, the Destination CIDR Block for a route rule would be an IPv6 subnet in your on-premises network, and the Target would be the dynamic routing gateway (DRG) attached to the IPv6-enabled VCN.
• **VCN security rules:** For each IPv6-enabled subnet in the VCN, update its security lists or relevant network security groups to allow IPv6 traffic between the VCN and your on-premises network. See Security Rules for IPv6 Traffic on page 2896.

If you do not yet have a FastConnect connection, see these topics to get started:
- FastConnect Overview on page 3173
- FastConnect Requirements on page 3181

**VPN Connect and IPv6**

If you use VPN Connect, you can configure it so that on-premises hosts with IPv6 addresses can communicate with an IPv6-enabled VCN. Here’s how to enable IPv6 for the connection:

- **IPSec connection static routes:** Configure the IPSec connection with the IPv6 static routes of your on-premises network. Currently the Oracle IPSec VPN does not support BGP dynamic routing.
- **VCN route tables:** For each IPv6-enabled subnet in the VCN, update its route table to include rules that route the IPv6 traffic from the VCN to the IPv6 subnets in your on-premises network. For example, the Destination CIDR Block for a route rule would be an IPv6 static route for your on-premises network, and the Target would be the dynamic routing gateway (DRG) attached to the IPv6-enabled VCN.
- **VCN security rules:** For each IPv6-enabled subnet in the VCN, update its security lists or relevant network security groups to allow the wanted IPv6 traffic between the VCN and your on-premises network. See Security Rules for IPv6 Traffic on page 2896.

If you have an existing IPSec VPN that uses static routing, you can update the list of static routes to include ones for IPv6. Be aware that changing the list of static routes causes the IPSec VPN to go down while it's being reprovisioned. See Changing the Static Routes on page 3157.

If you do not yet have an IPSec VPN, see these topics to get started:
- VPN Connect Overview on page 2933
- Setting Up VPN Connect on page 2949
- Working with VPN Connect on page 3156

**DHCP**

Currently DHCPv6 auto-configuration of IP addresses is not supported.

**DNS**

The VCN’s Internet Resolver supports IPv6, which means resources in your VCN can resolve IPv6 addresses of hosts outside the VCN. IPv6 traffic between resources within the VCN is not yet supported, and assignment of a hostname to an IPv6 address is not supported.

**Load Balancers**

When you create a load balancer, you can optionally choose to have an IPv4/IPv6 dual-stack configuration. When you choose the IPv6 option, the Load Balancing service assigns both an IPv4 and an IPv6 address to the load balancer. The load balancer receives client traffic sent to the assigned IPv6 address. The load balancer uses only IPv4 addresses to communicate with backend servers. There is no IPv6 communication between the load balancer and the backend servers.

IPv6 address assignment occurs only at load balancer creation. You cannot assign an IPv6 address to an existing load balancer.

**Comparison of IPv4 and IPv6 for Your VCN**

The following table summarizes the differences between IPv4 and IPv6 addressing in a VCN.
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Addressing type supported</strong></td>
<td>IPv4 addressing is always required, regardless of whether IPv6 is enabled.</td>
<td>IPv6 addressing is optional per VCN, optional per subnet in an IPv6-enabled VCN, and optional per VNIC in an IPv6-enabled subnet.</td>
</tr>
<tr>
<td><strong>Supported traffic types</strong></td>
<td>IPv4 traffic is supported for all gateways. IPv4 traffic between instances within the VCN is supported (east/west traffic).</td>
<td>IPv6 traffic is supported only with these gateways: internet gateway and DRG. Both inbound- and outbound-initiated IPv6 connections are supported between your VCN and the internet, and between your VCN and your on-premises network. Private IPv6 traffic between resources within a region (intra- and inter-VCN) is not yet supported (east/west traffic). Also see the caveats in Routing for IPv6 Traffic on page 2896.</td>
</tr>
<tr>
<td><strong>VCN size</strong></td>
<td>/16 to /30</td>
<td>/56 only</td>
</tr>
<tr>
<td><strong>Subnet size</strong></td>
<td>/16 to /30, with 3 addresses reserved in each subnet by Oracle (first 2 and last 1).</td>
<td>/64 only, with 8 addresses in the subnet reserved by Oracle (first 4 and last 4).</td>
</tr>
<tr>
<td><strong>Private and public IP address space</strong></td>
<td>Private: A VCN's private IPv4 CIDR can be from an RFC 1918 range or a publicly routable range (in which case, it's treated as private). You must specify the range, unless you use the Console's VCN creation wizard, which always uses 10.0.0.0/16. Public: The VCN does not have a dedicated public IPv4 address space. Any public addresses in your VCN are always chosen by Oracle.</td>
<td>You can specify a /56 from the list of supported ranges for the private IPv6 CIDR (see Overview of IPv6 Addresses on page 2890). If you don't specify a range, Oracle assigns a /56 CIDR that is used for both the private and public IP address space. <strong>Important:</strong> You must assign this value if you want instances in the same VCN to communicate with each other using public IPv6 addresses. For more information, see Routing for IPv6 Traffic on page 2896. Unlike with IPv4, your VCN has a dedicated public IPv6 address space, which is always /56 in size. When you assign an IPv6 to a VNIC, you can choose the address, or you can let Oracle chose it.</td>
</tr>
</tbody>
</table>
### Networking

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP address assignment</strong></td>
<td>Private: Each VNIC gets a private IPv4 address. You can choose the address or let Oracle choose it. Public: You determine whether the private IPv4 address has a public IP address associated with it (assuming the VNIC is in a public subnet). Oracle chooses the public IP address. From an API standpoint: the PrivateIp object is separate from the PublicIp object. You can remove the public IP address from the private IPv4 address at any time.</td>
<td>You decide whether a VNIC in an IPv6-enabled subnet gets an IPv6. You can choose the private IPv6 address or let Oracle choose it. You also decide whether that IPv6 has internet access enabled (assuming the VNIC is in a public subnet). You can remove the internet access for that IPv6 at any time. When an IPv6 is internet enabled, it has a public IPv6 address. The public IPv6 address always has the same right-most 64 bits as the private IPv6 address. Recall that if Oracle assigns the VCN's private IPv6 CIDR, then the private and public CIDRs for the VCN are the same. In that case, each IPv6 uses the same address (all 128 bits) for both its private IP address and public IP address. From an API standpoint: both the private and public IP addresses are included in the IPv6 object and always exist together.</td>
</tr>
<tr>
<td><strong>Internet access</strong></td>
<td>You control whether a subnet is public or private. You add or remove a public IP address from a private IPv4 address on a VNIC (assuming the VNIC is in a public subnet).</td>
<td>You control whether a subnet is public or private. You do not add or remove a public IP address to or from the VNIC as you do with IPv4. Instead you enable or disable the internet access for a given IPv6 that you've added to a VNIC (assuming the VNIC is in a public subnet).</td>
</tr>
<tr>
<td><strong>Primary and secondary labels</strong></td>
<td>Each VNIC automatically has a primary private IP address, and you can assign up to 31 secondary private IPs per VNIC.</td>
<td>You choose to add an IPv6 to a VNIC. There is no primary or secondary label for it. You can assign up to 32 IPv6s per VNIC.</td>
</tr>
<tr>
<td><strong>Hostnames</strong></td>
<td>You can assign hostnames to IPv4 addresses.</td>
<td>You cannot assign hostnames to IPv6 addresses.</td>
</tr>
<tr>
<td><strong>Route rule limits</strong></td>
<td>See Service Limits on page 215.</td>
<td>IPv4 and IPv6 route rules can reside together in the same route table. IPv6 route rules can target only an internet gateway or DRG. Limit on number of IPv6 route rules in a route table: 8.</td>
</tr>
</tbody>
</table>
### Networking

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security rule limits</td>
<td>See Service Limits on page 215. IPv4 and IPv6 security rules can reside together in same network security group or security list. IPv6 security rules can use only IPv6 CIDR ranges for source or destination, and not a service CIDR label used for a service gateway. Limit on number of IPv6 security rules in a security list: 8 ingress and 8 egress. Limit on number of IPv6 security rules in a network security group: 16 total.</td>
<td>IPv4 and IPv6 security rules can reside together in same network security group or security list. IPv6 security rules can use only IPv6 CIDR ranges for source or destination, and not a service CIDR label used for a service gateway. Limit on number of IPv6 security rules in a security list: 8 ingress and 8 egress. Limit on number of IPv6 security rules in a network security group: 16 total.</td>
</tr>
<tr>
<td>Reserved public IP addresses</td>
<td>Supported.</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Regional or AD-specific</td>
<td>Primary private IPv4 addresses are AD-specific. Secondary private IPv4 addresses are AD-specific unless assigned to a VNIC in a regional subnet. Public IP addresses can be AD-specific or regional depending on the type (ephemeral or reserved). See Public IP Addresses on page 2875.</td>
<td>IPv6 addresses are regional.</td>
</tr>
</tbody>
</table>

### Setting Up an IPv6-Enabled VCN with Internet Access

Use the following process if you want to set up an IPv6-enabled VCN with internet access so you can easily launch an instance and connect to it by using its public IPv6 address.

**Task 1: Create the IPv6-enabled VCN**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.
3. Click Create Virtual Cloud Network.
4. Enter the following:
   - **Name**: A descriptive name for the VCN. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in Compartment**: Leave as is.
   - **CIDR Block**: A single, contiguous IPv4 CIDR block for the VCN. For example: 172.16.0.0/16. You cannot change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.
   - **Enable IPv6 Address Assignment**: Select the check box and optionally provide the private IPv6 CIDR in the field labeled Private IPv6 CIDR Block. You must provide the value if you want the instances in this IPv6-enabled VCN to communicate with each other using their public IP addresses. Leave the field blank if you want Oracle to assign the private IPv6 CIDR for you. You cannot later disable IPv6 for the VCN or change the CIDR. All IPv6-enabled VCNs are always /56 in size.
   - **Use DNS Hostnames in this VCN** (supported for IPv4 only): Required for assignment of DNS hostnames to hosts in the VCN, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the
Networking

VCN (<VCN DNS label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.

- **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.

5. Click **Create Virtual Cloud Network**.

The VCN is then created and displayed on the Virtual Cloud Networks page in the compartment you chose.

**Task 2: Create a regional IPv6-enabled public subnet**

1. While still viewing the VCN, click **Create Subnet**.
2. Enter the following:

   - **Name**: A descriptive name for the subnet (for example, Regional Public Subnet). It doesn't have to be unique, and you can change it later. Avoid entering confidential information.

   - **Regional or Availability Domain-specific subnet**: Oracle recommends creating only **regional subnets**, which means that the subnet can contain resources in any of the region's availability domains. If you instead choose **Availability Domain-Specific** (the only kind of subnet that Oracle originally offered), you must also specify an availability domain. This choice means that any instances or other resources later created in this subnet must also be in that availability domain.

   - **CIDR Block**: A single, contiguous IPv4 CIDR block for the subnet (for example, 172.16.0.0/24). The address block must be within the VCN's IPv4 CIDR block and not overlap any other subnets. You **cannot** change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, here's a CIDR calculator.

   - **Enable IPv6 Address Assignment**: Select the check box and provide your choice of 16 bits for the subnet (example: 1111). You **cannot** later disable IPv6 for the subnet or change the CIDR. All IPv6-enabled subnets are always /64 in size. For more information about IPv6 address format, see Overview of IPv6 Addresses on page 2890.

   - **Route Table**: Select the default route table.

   - **Private or public subnet**: Select **Public Subnet**, which means instances in the subnet can optionally have public IP addresses. For more information, see Access to the Internet on page 2752.

   - **Use DNS Hostnames in this Subnet** (supported for IPv4 only): This option is available only if you provided a DNS label for the VCN during creation. The option is required for assignment of DNS hostnames to hosts in the subnet, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the subnet, or the Console will generate one for you. The dialog box automatically displays the corresponding **DNS Domain Name** for the subnet (<subnet_DNS_label>.<VCN_DNS_label>.oraclevcn.com). For more information, see DNS in Your Virtual Cloud Network on page 2910.

   - **DHCP Options**: Select the default set of DHCP options.

   - **Security Lists**: Select the default security list.

   - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.

3. Click **Create Subnet**.

   The subnet is then created and displayed on the Subnets page.

**Task 3: Create the internet gateway**

1. Under **Resources**, click **Internet Gateways**.
2. Click **Create Internet Gateway**.
3. Enter the following:

   - **Name**: A descriptive name for the internet gateway. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

   - **Create in Compartment**: Leave as is.

   - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.

4. Click **Create Internet Gateway**.

   Your internet gateway is created and displayed on the Internet Gateways page. It's already enabled, but you must add route rules that allow IPv4 and IPv6 traffic to flow to the gateway.
Task 4: Update the default route table to use the internet gateway

The default route table starts out with no rules. Here you add rules that route all IPv4 and IPv6 traffic destined for addresses outside the VCN to the internet gateway. The existence of these rules also enables inbound connections to come from the internet to the subnet, through the internet gateway. You use security rules to control the types of traffic that are allowed in and out of the instances in the subnet (see the next task).

No route rule is required in order to route traffic within the VCN itself.

1. Under Resources, click Route Tables.
2. Click the default route table to view its details.
3. Click Add Route Rules.
4. Enter the following:
   - **Target Type**: Internet Gateway
   - **Destination CIDR block**: 0.0.0.0/0 (which means that all IPv4 non-intra-VCN traffic that is not already covered by other rules in the route table goes to the target specified in this rule).
   - **Compartment**: The compartment where the internet gateway is located.
   - **Target**: The internet gateway you created.
   - **Description**: An optional description of the rule.
5. Click + Additional Route Rule.
6. Enter the following:
   - **Target Type**: Internet Gateway
   - **Destination CIDR block**: ::/0 (for the IPv6 traffic).
   - **Compartment**: The compartment where the internet gateway is located.
   - **Target**: The internet gateway you created.
   - **Description**: An optional description of the rule.
7. Click Add Route Rules.

The default route table now has two rules for the internet gateway, one for IPv4 traffic and one for IPv6 traffic. Because the subnet was set up to use the default route table, the resources in the subnet can now use the internet gateway. The next step is to specify the types of traffic you want to allow in and out of the instances you later create in the subnet.

Task 5: Update the default security list (optional)

**Note:**

This task is about configuring security rules to allow traffic to and from your instances. Although this task uses a security list to implement those rules, you can also use network security groups to implement security rules.

Earlier you set up the subnet to use the VCN's default security list. This list already includes basic rules that allow essential IPv4 and IPv6 traffic. In this task, you add any additional security rules that allow the types of connections that the instances in the VCN will need.

For example: This is a public subnet with an internet gateway, so the instances you create might need to receive inbound HTTPS connections from the internet (if they're web servers). Here's how to add another rule to the default security list to enable that traffic:

2. Click the default security list to view its details. By default, you land on the Ingress Rules page.
3. Click Add Ingress Rule.
4. To enable inbound connections for HTTPS (TCP port 443), enter the following:
   - **Stateless**: Unselected (this is a stateful rule)
   - **Source Type**: CIDR
   - **Source CIDR**: 0.0.0.0/0 (or ::/0 if you want to enable IPv6 traffic with this rule)
   - **IP Protocol**: TCP
   - **Source Port Range**: All
   - **Destination Port Range**: 443
   - **Description**: An optional description of the rule.

5. Click **Add Ingress Rule**.

   **Important:**

   Security List Rule for Windows Instances

   If you're going to create Windows instances, you need to add a security rule to enable Remote Desktop Protocol (RDP) access. Specifically, you need a stateful ingress rule for TCP traffic on destination port 3389 from source 0.0.0.0/0 (and a separate rule with ::/0 for IPv6 traffic) and any source port.

   For more information, see [Security Rules](#page-2833) on page 2833.

For a production VCN, you typically set up one or more custom security lists for each subnet. If you like, you can edit the subnet to use different security lists. If you choose not to use the default security list, do so only after carefully assessing which of its default rules you want to duplicate in your custom security list. For example: the default ICMP rules in the default security list are important for receiving connectivity messages for IPv4.

**Task 6: Create an instance**

Your next step is to create an instance in the subnet. When you create the instance, you choose the availability domain, which VCN and subnet to use, and several other characteristics.

Each instance automatically gets a private IPv4 address. When you create an instance in a public subnet, you choose whether the instance gets a public IP address. A public IPv4 address is NOT required for public IPv6 traffic. But if you want to connect to the instance from an IPv4 host, you must give the instance a public IP address, or else you can't access them through the internet gateway. The default (for a public subnet) is for the instance to get a public IP address.

For more information and instructions, see [Launching an Instance](#page-2835).

**Task 7: Add an internet-enabled IPv6 to the instance**

1. While viewing the instance you just created, click **Attached VNICs**.
2. Click the VNIC.
3. Under Resources, click **IPv6 Addresses**.
4. Click **Assign Private IPv6 Address**.
5. Enter the following:
   - **Private IPv6 Address**: Optional. An available private IPv6 address of your choice from the subnet's private IPv6 CIDR (otherwise the private IP address is automatically assigned).
   - **Unassign if already assigned to another VNIC**: Leave this check box as is (cleared). Use this only to force reassignment of an IPv6 address if it's already assigned to another VNIC in the subnet. Relevant only if you specify a private IP address in the preceding field.
   - **Enable Internet Access**: Select this check box. This enables internet access and assigns the IPv6 a public address (if it's in a public subnet, which is the case here). See [Overview of IPv6 Addresses](#page-2890) on page 2890.
   - **Tags**: Leave as is. You can add tags later if you want. For more information, see [Resource Tags](#page-211) on page 211.
6. Click **Assign**.

   The IPv6 is created and then displayed on the **IPv6 Addresses** page for the VNIC. Notice that it has both a private and public IPv6 address.
Task 8: Configure the instance's OS to use the IPv6

You must configure the instance's OS to use the IPv6. For more information, see Configuring the OS to Use an IPv6 on page 2907.

After performing this task, you can connect to the instance over the internet with SSH or RDP from your on-premises network or a location on the internet. The host connecting to the instance must be using a public IPv6 address.

Managing IPv6s in the Console

This section includes basic tasks for working with IPv6-related resources.

To create an IPv6-enabled VCN

Important:
You can't enable IPv6 for an existing VCN. You can only enable IPv6 when creating a VCN. After enabling IPv6 for a VCN, you cannot disable it.

See the instructions in Task 1: Create the IPv6-enabled VCN on page 2901.

To create an IPv6-enabled subnet

Important:
After enabling IPv6 for a subnet, you cannot disable it.

Summary: Creating an IPv6-enabled subnet is similar to creating an IPv4 subnet. The only difference is that you must select the check box for Enable IPv6 Address Assignment and provide 16 bits for the subnet's portion of the IPv6 CIDR. See Overview of IPv6 Addresses on page 2890.

For general instructions, see Task 2: Create a regional IPv6-enabled public subnet on page 2902. If you want a private subnet, select the radio button for Private Subnet when creating the subnet.

To assign an IPv6 to a VNIC

The process for adding an IPv6 to a VNIC is similar to adding a secondary private IPv4 address. You can specify the particular IPv6 address to use or let Oracle choose it from the subnet. You can enable internet access if you like. The resulting public IPv6 address uses the same right-most 64 bits as the private IPv6 address. In certain situations, the entire IPv6 address is the same. For more information, see Overview of IPv6 Addresses on page 2890. After assigning the IPv6 to the VNIC, you must configure the OS to use the IPv6.

1. Assign the IPv6. For general instructions, see Task 7: Add an internet-enabled IPv6 to the instance on page 2904. If you want an IPv6 without internet access, do not select the check box for Enable Internet Access when assigning the IPv6.
2. Configure the OS to use the IPv6 address. For more information, see Configuring the OS to Use an IPv6 on page 2907.

To move an IPv6 to another VNIC in the subnet

The process is similar to moving a secondary private IPv4 address from one VNIC to another (let's call them the original VNIC and the new VNIC). You assign the IPv6 to the new VNIC, specify the private IPv6 address, and select the check box for Unassign if already assigned to another VNIC. Oracle automatically unassigns it from original VNIC and assigns it to the new VNIC. The public address for the IPv6 stays the same regardless of which VNIC the IPv6 is assigned to.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICs.
   The primary VNIC and any secondary VNICs attached to the instance are displayed.
5. Click the VNIC you're interested in.
7. Click Assign Private IP Address.
8. Enter the following:
   - **Private IPv6 Address**: The private IPv6 address that you want to move.
   - **Unassign if already assigned to another VNIC**: Select this check box to move the IPv6 address from the VNIC it's currently assigned to.
   - **Enable Internet Access**: Whether to assign a public IPv6 address. Available only if the VNIC is in a public subnet. See Overview of IPv6 Addresses on page 2890.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

9. Click **Assign**.

The private IP address is moved from the original VNIC to the new VNIC.

**To delete an IPv6 from a VNIC**

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICS.
   - The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC you're interested in.
7. For the IPv6 you want to delete, click the Actions icon (three dots), and then click Delete IPv6.
8. Confirm when prompted.

The IPv6 address is returned to the pool of available addresses in the subnet.

**To enable or disable internet access for an IPv6**

Internet access for an IPv6 is controlled by the IPv6's Enable Internet Access check box. When you enable internet access, the IPv6 is assigned a public IPv6 address. That address's right-most 64 bits are the same as the private IPv6 address. In certain situations, the entire IPv6 address is the same. For more information, see Overview of IPv6 Addresses on page 2890.

1. Confirm you're viewing the compartment that contains the instance you're interested in.
2. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
3. Click the instance to view its details.
4. Under Resources, click Attached VNICS.
   - The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC you're interested in.
7. For the IPv6 you're interested in, click the Actions icon (three dots), and then click Edit.
8. Either select or clear the check box for Enable Internet Access.
9. Click Update.

When you disable internet access, the public IPv6 address becomes null. If you re-enable internet access, the public IPv6 address is again assigned to the IPv6.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

For IPv6 addressing, there's an Ipv6 object with the following operations:

- ListIpv6s
- GetIpv6
Networking

- UpdateIpv6
- CreateIpv6
- DeleteIpv6

**Configuring the OS to Use an IPv6**

After assigning an IPv6 to a VNIC, you must configure the OS to use the IPv6.

**Getting the IPv6 Virtual Router IP (Default Gateway)**

You need the IPv6 virtual router IP (called the default gateway in Windows), which is included in the instance metadata available at the following URL:

```
```

Here's an example response:

```
[
   {
      "vnicId": "ocid1.vnic.oc1.phx.examplevq7kncmdtfr23dznohkd2cywjcem33eg3dxa",
      "privateIp": "10.0.3.7",
      "vlanTag": 3396,
      "macAddr": "00:00:17:01:14:0C",
      "virtualRouterIp": "10.0.3.1",
      "subnetCidrBlock": "10.0.3.0/24",
      "ipv6SubnetCidrBlock": "2001:0db8:95f4::/64",
      "ipv6VirtualRouterIp": "2001:0db8::200:17ff:fee3:c491"
   }
]
```

**Oracle Linux Configuration**

The following commands are for Oracle Linux 8 and Oracle Linux 7. They are NOT persistent through a reboot. You need the IPv6 virtual router IP from the instance metadata (see the previous section).

```
sysctl net.ipv6.conf.all.disable_ipv6=0
ip -6 addr add <private_IPv6_address>/64 dev <interface_name>
ip -6 route add default via <IPv6_virtual_router_IP> dev <interface_name>
```

For example:

```
sysctl net.ipv6.conf.all.disable_ipv6=0
ip -6 addr add 2001:0db8:95f4::abcd:1234/64 dev ens3
ip -6 route add default via 2001:0db8::200:17ff:fee3:c491 dev ens3
```

If you haven't yet, ensure that the VCN's route table and security rules are configured for the wanted IPv6 traffic. See Routing for IPv6 Traffic on page 2896 and Security Rules for IPv6 Traffic on page 2896.

**Windows Configuration**

You can use a command line or the Network Connections UI.

**Command Line**

If you use PowerShell, you must run it as an administrator. The following configuration persists through a reboot of the instance.
1. In your browser, go to the Console, and note the private IPv6 address that you want to configure on the instance.
2. Connect to the instance, and run the following command at a command prompt:
   
   ```
   ```
3. Note the value for the `ipv6VirtualRouterIp`, which is the `<default_gateway>` to use in the next step.
4. Run the following 2 commands:
   
   ```
   netsh interface ipv6 add address interface="Ethernet" 
   address=<private_IPv6_address>/64 
   netsh interface ipv6 add route prefix=::/0 interface="Ethernet" 
   nexthop=<default_gateway> publish=Yes
   ```
   
   For example:
   
   ```
   netsh interface ipv6 add address interface="Ethernet" 
   address=2001:0db8:95f4::abcd:1234/64 
   netsh interface ipv6 add route prefix=::/0 interface="Ethernet" 
   nexthop=2001:0db8::200:17ff:fee3:c491 publish=Yes
   ```
   
   If you haven’t yet, ensure that the VCN’s route table and security rules are configured for the wanted IPv6 traffic. See Routing for IPv6 Traffic on page 2896 and Security Rules for IPv6 Traffic on page 2896.

   You can run the following command to see that the IPv6 address has been configured for the interface:
   
   ```
   netsh interface ipv6 show addresses
   ```
   
   Later if you want to delete the address, you can use this command:
   
   ```
   netsh interface ipv6 delete address interface="Ethernet" 
   address=<private_IPv6_address>
   ```
   
   For example:
   
   ```
   netsh interface ipv6 delete address interface="Ethernet" 
   address=2001:0db8:95f4::abcd:1234
   ```
   
   Also delete the IPv6 from the VNIC. You can do that before or after executing the earlier command to delete the address from the OS configuration.

   **Network Connections UI**

   The following configuration persists through a reboot of the instance.

   1. In your browser, go to the Console, and note the private IPv6 address that you want to configure on the instance.
   2. Connect to the instance, and run the following command at a command prompt:
      
      ```
      ```
   3. Note the value for the `ipv6VirtualRouterIp`, which is the default gateway to use in a later step.
   4. In the instance’s Control Panel, go to Network and Internet, and view your network connections (see the image that follows for the set of dialog boxes you see in these steps).
   5. For the active networks, click the connection (Ethernet).
   6. Click Properties.
7. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

8. Select the radio button for **Use the following IP address**, and then enter the values you noted earlier for the private IPv6 address and default gateway. Use 64 for the subnet prefix length.

9. Click **OK** until the dialog boxes are closed.

If you haven't yet, ensure that the VCN's route table and security rules are configured for the wanted IPv6 traffic. See **Routing for IPv6 Traffic** on page 2896 and **Security Rules for IPv6 Traffic** on page 2896.
**DNS in Your Virtual Cloud Network**

The Domain Name System (DNS) lets computers use hostnames instead of IP addresses to communicate with each other.

**Choices for DNS in Your VCN**

Following are the choices for DNS name resolution for the instances in your VCN. You make this choice for *each subnet* in the VCN, using the subnet's set of DHCP options. This is similar to how you configure which route table and security lists are associated with each subnet. For more information, see [DHCP Options](#) on page 2917.

**Note:**

You use the Domain Name Server DHCP option to specify the DNS Type for the associated subnet. If you change the option's value, either restart the DHCP client on the instance or reboot the instance. Otherwise, the change does not get picked up until the DHCP client refreshes the lease (within 24 hours).

**DEFAULT CHOICE: INTERNET AND VCN RESOLVER**

This is an Oracle-provided option that includes two parts:

- **Internet Resolver:** Lets instances resolve hostnames that are publicly published on the internet. The instances do not need to have internet access by way of either an internet gateway or a connection to your on-premises network (such as an IPSec VPN connection through a DRG).
- **VCN Resolver:** Lets instances resolve hostnames (which you can assign) of other instances in the same VCN. For more information, see [About the DNS Domains and Hostnames](#) on page 2910.

By default, new VCNs you create use the Internet and VCN Resolver. If you're using the Networking API, this choice refers to the `VcnLocalPlusInternet` enum in the `DhcpDnsOption` object.

**Note:**

By default, the Internet and VCN Resolver does not let instances resolve the hostnames of hosts in your on-premises network connected to your VCN by IPSec VPN connection or FastConnect. That functionality can be achieved either by using a custom resolver or by configuring the VCN's private DNS resolver.

**CUSTOM RESOLVER**

Use DNS servers of your choice for resolution (maximum three). They could be DNS servers that are:

- Available through the internet. For example, 216.146.35.35 for Dyn's Internet Guide.
- In your VCN.
- In your on-premises network, which is connected to your VCN by way of an IPSec VPN connection or FastConnect (through a DRG).

**About the DNS Domains and Hostnames**

When you initially create a VCN and subnets, you may specify DNS labels for each. Subnet DNS labels can only be set if the VCN itself is created with a DNS label. The labels, along with the parent domain of `oraclevcn.com` form the VCN domain name and subnet domain name:

- **VCN domain name:** `<VCN DNS label>.oraclevcn.com`
- **Subnet domain name:** `<subnet DNS label>.<VCN DNS label>.oraclevcn.com`

When you then launch an instance, you may assign a hostname. It's assigned to the VNIC that's automatically created during instance launch (that is, the *primary VNIC*). Along with the subnet domain name, the hostname forms the instance's fully qualified domain name (FQDN):

- **Instance FQDN:** `<hostname>.<subnet DNS label>.<VCN DNS label>.oraclevcn.com`

For example: `database1.privatesubnet1.abccorpcvn1.oraclevcn.com`
The FQDN resolves to the instance's private IP address. The Internet and VCN Resolver also enables reverse DNS lookup, which lets you determine the hostname corresponding to the private IP address.

If you add a secondary VNIC to an instance, you can specify a hostname. The resulting FQDN resolves to the VNIC's private IP address (that is, the primary private IP).

If you add a secondary private IP to a VNIC, you can specify a hostname. The resulting FQDN resolves to that private IP address.

Important:

Oracle recommends that you always use the instance FQDN when sending messages to a host, or alternately specify only the hostname for messages sent within a VCN.

Requirements for DNS Labels and Hostnames

- VCN and subnet labels: Max 15 alphanumeric characters and must start with a letter. Notice that hyphens and underscores are NOT allowed. The value cannot be changed later.
- Hostnames: Max 63 characters and must be compliant with RFCs 952 and 1123. The value can be changed later.

Important:

The Networking service allows hostnames up to 63 characters. However, some older operating systems enforce shorter hostnames. In Linux, here's how to determine the maximum allowed hostname length:

```
getconf HOST_NAME_MAX
```

If an instance has a hostname longer than the OS-specific maximum, the instance's FQDN is not resolvable within the VCN. You can use the Networking service to update the VNIC and change the hostname to a shorter value.

Uniqueness:

- VCN DNS label should be unique across your VCNs (not required, but a best practice)
- Subnet DNS labels must be unique within the VCN
- Hostnames must be unique within the subnet

Tip:

Don't confuse the DNS label or hostname with the friendly name you can assign to the object (that is, the display name), which doesn't have to be unique.

Validation and Generation of the Hostname

If you've set DNS labels for the VCN and subnets, Oracle validates the hostname for DNS compliance and uniqueness during instance launch. If either of these requirements isn't met, the launch request fails.

If you don't specify a hostname during instance launch, Oracle tries to use the instance's display name as the hostname. If the display name does not pass the validation, Oracle automatically generates a DNS-compliant hostname that's unique across the subnet. You can see the generated hostname on the instance's page in the Console. In the API, the hostname is part of the VNIC object.

If you don't provide a hostname or display name during instance launch using the SDK or CLI, Oracle does not generate a display name or hostname. This means the instance won't be resolvable using the Internet and VCN Resolver.

If you don't provide a hostname or display name during instance launch using the Console, Oracle will auto-generate a display name and a corresponding DNS record, provided the Subnet has a valid DNS label associated with it.
**Note:**

The Linux OS hostname on the instance is automatically set to the hostname you set during instance launch (or the one generated by Oracle). If you change the hostname directly on the instance, the FQDN of the instance does not get updated.

If you add a secondary VNIC to an instance, or add a secondary private IP to a VNIC, Oracle never tries to generate a hostname. Provide a valid hostname if you want the private IP address to be resolvable using the Internet and VCN Resolver.

**DHCP Options for DNS**

Two DHCP options are related to DNS in your VCN:

- **Domain Name Server:** To specify your choice for DNS type (either Internet and VCN Resolver, or Custom Resolver).
- **Default value in the default set of DHCP options:** Internet and VCN Resolver
- **Search Domain:** To specify a single search domain. When resolving a DNS query, the OS appends this search domain to the value being queried. You can specify only one search domain for the set of DHCP options.
- **Default value in the default set of DHCP options:** The VCN domain name (\(<VCN\ DNS label>\).oraclevcn.com), if you specified a DNS label for the VCN during creation but did not specify a search domain value. If you specified a search domain value, then that value is used for the Search Domain option. If you did NOT specify a DNS label, the default set of DHCP options does not include a Search Domain option.

**Caution:**

Oracle recommends that you always use the instance FQDN when sending messages to a host in another subnet/VCN and do not rely on the DNS search domain.

**Important:**

In general, when *any* set of DHCP options is initially created (the default set or a custom set you create), the Networking service automatically adds the Search Domain option and sets it to the VCN domain name (\(<VCN\ DNS label>\).oraclevcn.com) if *all of these are true*:

- The VCN has a DNS label
- DNS Type = Internet and VCN Resolver
- You did NOT specify a search domain of your choice during creation of the set of DHCP options

After the set of DHCP options is created, you can always remove the Search Domain option or set it to a different value.

**How to Enable DNS Hostnames in Your VCN**

Only new VCNs created after the release of the Internet and VCN Resolver feature have automatic access to it. How to enable DNS hostnames for a new VCN depends on which interface you're using.

*If you create a VCN and subnets with the Console*

1. When creating the VCN:
   - Check the check box for **Use DNS Hostnames in this VCN**
   - Specify a DNS label of your choice for the VCN. If you check the check box but don't specify a DNS label, the Console assumes that you want to use the Internet and VCN Resolver in your VCN and automatically generates a DNS label for the VCN. The Console takes the VCN name you provided, removes non-
alphanumeric characters, ensures that the first character is a letter, and truncates the label to 15 characters. The Console displays the result, and if you don't like it, you can instead enter your own value in the DNS Label field. See About the DNS Domains and Hostnames on page 2910.

2. When creating the subnets:
   • Again, check the check box for Use DNS Hostnames in this Subnet
   • Specify a DNS label of your choice for each subnet. If you check the check box but don't specify the DNS label for a given subnet, the Console assumes you want to use the Internet and VCN Resolver for the subnet and automatically generates a DNS label for the subnet. The Console takes the subnet name you provided, removes non-alphanumeric characters, ensures that the first character is a letter, and truncates the label to 15 characters. The Console displays the result, and if you don't like it, you can instead enter your own value in the DNS Label field. See About the DNS Domains and Hostnames on page 2910.

   **Note:**
   Subnet DNS labels can only be set if the VCN itself is created with a DNS label.

   • Associate any set of DHCP options that has DNS type = Internet and VCN Resolver. The default set of DHCP options in the VCN uses the Internet and VCN Resolver by default.

3. When launching instances:
   • Specify a hostname (or at least a display name) for each instance. For more information, see About the DNS Domains and Hostnames on page 2910.

   If you don't check the check box for Use DNS Hostnames in this VCN when creating the VCN, you can't set the DNS label for the VCN or subnets, and you can't specify a hostname during instance launch.

   **Note:**
   The previous procedure assumes you create the VCN and subnets one at a time in the Console. The Console has a feature that automatically creates a VCN with subnets and an internet gateway all at the same time. If you use that feature to create the VCN and subnets, the Console automatically generates DNS labels for them.

If you create a VCN and subnets with the API

1. When creating the VCN:
   • Specify a DNS label for the VCN. See About the DNS Domains and Hostnames on page 2910. If you don't set a value (if it's null), Oracle assumes that you don't want to use the Internet and VCN Resolver, even if the DHCP options have Dhcpi\n   DnsOption serverType = VcnLocalPlusInternet.

2. When creating the subnets:
   • Specify a DNS label for each subnet. See About the DNS Domains and Hostnames on page 2910. If you specified a DNS label for the VCN, but you don't specify a DNS label for the subnet, Oracle assumes that you don't want the instances in the subnet to use the Internet and VCN Resolver and the ability to use hostnames to communicate with instances in the VCN is no longer available.

   **Note:**
   Subnet DNS labels can only be set if the VCN itself was created with a DNS label.

   • Associate any set of DHCP options that has Dhcpi\n   DnsOption serverType = VcnLocalPlusInternet, which is the default DHCP option in the VCN.

3. When launching instances:
   • Specify a hostname (or at least a display name) for each instance. For more information, see About the DNS Domains and Hostnames on page 2910.

   If you don't specify a DNS label when creating the VCN, you can't:
- Set the DNS label for the subnets (causing the CreateSubnet call to fail)
- Specify a hostname during instance launch (causing the LaunchInstance call to fail)
- Assign a hostname to a secondary VNIC or a secondary private IP

**Scenario 1: Use Internet and VCN Resolver with DNS Hostnames Across the VCN**

The typical scenario is to enable the Internet and VCN Resolver across your entire VCN, which allows all instances in the VCN to communicate with each other without knowing their IP addresses. To do that, follow the instructions in About the DNS Domains and Hostnames on page 2910, and assign a DNS label to the VCN and every subnet. Then assign every instance a hostname (or at least a display name) at launch. If you add a secondary VNIC or secondary private IP, also assign it a hostname. The instances can then communicate with each other using FQDNs instead of IP addresses.

**Scenario 2: Use a Private DNS Resolver to Resolve DNS Hostnames**

You can use a private DNS resolver to answer DNS queries for a VCN using a configuration you create. The resolver listens on 169.254.169.254 by default, but also allows you to define endpoints for listening for queries and forwarding them to other resolvers in other VCNs, a customer’s on-premises network, or other private network. For more information, see Private DNS resolvers.

**Scenario 3: Use Different DHCP Options Per Subnet**

**Scenario 1** assumes you want to use the Internet and VCN Resolver the same way across all subnets, and thus all instances in the VCN. You could, however, configure different DNS settings for each subnet, because the DHCP options are configured at the subnet level. The important thing to understand is: the subnet where you want to generate the DNS query is where you need to configure the corresponding Internet and VCN Resolver settings.

For example, if you want instance A in subnet A to resolve the hostname of instance B in subnet B, you must configure subnet A to use the Internet and VCN Resolver. Conversely, if you want instance B to resolve the hostname of instance A, you must configure subnet B to use the Internet and VCN Resolver.

You can configure a different set of DHCP options for each subnet. For example, you could set subnet A’s Search Domain to subneta.vcn1.oraclevcn.com, which means all instances in subnet A could use just hostnames to communicate with each other. You could similarly set subnet B’s Search domain to subnetb.vcn1.oraclevcn.com to enable Subnet B’s instances to communicate with each other with just hostnames.

**Private DNS resolvers**

A private DNS resolver answers DNS queries for a VCN per a configuration you create.

When you create a VCN and select the Use DNS hostnames in this VCN option, this choice creates a dedicated private DNS resolver and a default private view with system-managed zones. A private DNS resolver also handles internal DNS queries for your VCN based on private views and the private zones that you have created and the rules you create for the resolver. A private DNS zone has capabilities similar to an internet DNS zone, but only provides responses for clients that can reach it through a VCN. The default view is only used if the resolver does not get a match from the other attached private views, if there are any. A private resolver can be configured to use views and zones as well as conditional forwarding rules to define how to respond to DNS queries. To better understand views and zones, refer to Private DNS on page 1698.

You can create your own custom domains to use in addition to the system-generated names based on VCNs and subnets, and you can do VCN to VCN and VCN to on-premises resolution.

**To add a private view to a private resolver**

1. From the Virtual Cloud Network Details screen for your VCN, look in the VCN Information tab and click the name of the DNS resolver for the VCN. The Private Resolver Details screen appears.
2. From the Private Resolver Details screen, click Manage Private Views. The Manage Private Views screen appears.
3. Select a previously created private view from the drop down menu in the numbered Private view list.
4. To associate another view, click Additional Private View select another view.
5. When you are finished, click Save Changes.
Views created automatically by Oracle are available in addition to views you create.

**To remove a private view from a private resolver**

1. From the Private Resolver Details screen, click the check box next to the private view you want to remove from the resolver. Remove turns red, and can now be clicked. You can select other private views if necessary.
2. Click Remove.

**Note:**
You can also remove a private view from the Manage Private Views screen by clicking the red button labeled - and then clicking Save Changes.

**To rename a private resolver**

1. From the Private Resolver Details screen, click Edit.
2. Enter the new name for the resolver. Avoid entering confidential information. Then, click Save Changes.

**To manage DNS zones and views**

See Managing DNS Service Zones on page 1679.

**Resolver Endpoints**

A DNS forwarding resolver endpoint is required before you can create a resolver rule. Resolver endpoints are attached to a VCN or a subnet. No listening endpoint is required for compute instances sending queries to 169.254.169.254. Two types of endpoint are used:

- **Listening** - A listening endpoint receives queries from these sources: within the VCN, other VCN Resolvers, or your on-premises network's DNS. Once created, no further configuration is needed for a listening endpoint.
- **Forwarding** - A forwarding endpoint forwards DNS queries to the Listening endpoint for resolvers in other peered VCNs or your on-premises network's DNS. Decisions about where to forward queries are based on resolver rules that you define.

An endpoint can only be configured to either forward or listen.

**Note:**
Network security groups (NSGs) act as a virtual firewall for your DNS resolver endpoints. An NSG consists of a set of ingress and egress security rules that apply only to the associated DNS resolver endpoints.

**To create a resolver endpoint**

1. From the Virtual Cloud Network Details screen for your VCN, look in the VCN Information tab and click the name of the DNS resolver for the VCN. The Private Resolver Details screen appears.
2. From the Private Resolver Details screen, click Endpoints in the left-hand navigation.
3. Click Create Endpoint. The Create Endpoint screen appears.
4. Make choices for the following settings:
   - Select a name for the endpoint. The name can use any combination of letters and numbers, but the only supported special character is an underscore.
   - Select a subnet for the endpoint from the pull-down list.
   - Select the endpoint type, which can be either Listening or Forwarding. When you make this choice, you provide an IP address, or allow Oracle to assign one for the endpoint. This IP address is used by the resolver to forward DNS queries, or to listen for DNS queries from other systems. The IP address must be in the same CIDR block used by the VCN or subnet associated with the resolver.
   - Optional: Use a Network Security Group to control traffic. To use this feature, select an NSG to use with the endpoint. You can also add an NSG after the endpoint is created.
To delete a resolver endpoint

1. From the Private Resolver Details screen, click the Action button to the right of the endpoint you want to delete, and then click Delete.
2. Confirm the deletion by clicking Delete.

To add an NSG to a resolver endpoint

1. From the Private Resolver Details screen, click the name of the endpoint you want to associate with a Network Security group. The Endpoint Details screen appears.
2. Click Add Network Security Groups, and select up to five security groups to associate with the endpoint.

To remove an NSG from a resolver endpoint

1. From the Private Resolver Details screen, click the name of the endpoint you want to de-associate with a Network Security group. The Endpoint Details screen appears.
2. Click the X button to the right of the listed NSG. You could change to a different NSG if necessary.

Resolver Rules

Rules are used to answer queries that aren't answered by a resolver's views. They are checked in order, and each can optionally have conditions that limit which queries they apply to. Queries not matched by any view or rule are resolved from internet DNS. You can have up to 10 rules per resolver.

Note:
Endpoints are used in the rule, and they must exist before you create a resolver rule.

Use case

The most common application is to have one or more rules that follow this general form:

If <query domain> is <example.com>, forward using <forwarding-endpoint> to IP address X.X.X.X.

Followed by a final rule that follows this form:

If <anything else>, forward using <forwarding-endpoint> to IP address Y.Y.Y.Y.

So if the query is looking for example.com, the resolver internally forwards it to X.X.X.X through the specified forwarding endpoint and responds with the answer it receives. For any other query, it forwards to Y.Y.Y.Y through the same forwarding endpoint and responds with that answer it gets from Y.Y.Y.Y.

To create resolver rules

1. From the Private Resolver Details screen, click Rules in the Resources column. Click Manage Rules. The Manage Rules screen appears.
2. You can have up to 10 rules per resolver. For each rule, select:
   - **Rule condition**: Determines whether routing decisions are made based on the query's originating CIDR Block or Domain (up to 10 hostnames), or neither (Select None to match any CIDR Block or Domain).
   - **Client CIDR blocks or Domains**: Up to 10 CIDR blocks or domains.
   - **Rule action**: This field is read-only. Forward is the only option.
   - **Source endpoint**: The private endpoint used to forward queries when the rule condition is met.
   - **Destination IP address**: The address to forward the query to if the rule condition is met.
3. Click +Additional Rule to create another rule if necessary.
4. Click Save Changes when finished.
To edit resolver rules

1. From the Private Resolver Details screen, click Rules in the Resources column.
2. Click Manage Rules. The Manage Rules screen appears.
3. Make changes based on your intended design. These changes can include changing options in a rule, changing the order of rules, and removing rules altogether.
4. When finished, click Save Changes.

To remove resolver rules

1. From the Private Resolver Details screen, click Rules in the Resources column.
2. Click the check box in the row for the rule or rules you want to delete. Click Remove. The Confirm Removal screen appears.
3. Click Remove.

Reverse DNS (PTR)

A reverse DNS record, also known as a pointer record (PTR), resolves an IP address back to a fully qualified domain name (FQDN). It functions in the opposite way of an A (IPv4) or AAAA (IPv6) forward record. For example:
192.0.2.5 # myhost.mydomain.com

You can request that a PTR record be established for your cloud IP addresses:

1. Create an A (IPv4) or AAAA (IPv6) forward record that points the fully qualified domain name to the IP prior to opening the request. You can create the record using the Oracle Cloud Infrastructure DNS service, or a third-party DNS provider.
2. Open a service request and include the following information:
   a. The IP address and fully qualified domain name (FQDN) you want in the PTR.
   b. The FQDN of the forward record that you created in step 1.

After the service request is received, the forward (A or AAAA) record information is validated to be sure it can be successfully resolved, and Oracle creates the PTR record on your behalf.

Using the API

Use the following operations to manage resolvers and resolver endpoints:

- ListResolvers
- GetResolver
- UpdateResolver
- ChangeResolverCompartment
- ListResolverEndpoints
- CreateResolverEndpoint
- GetResolverEndpoint
- UpdateResolverEndpoint
- DeleteResolverEndpoint

DHCP Options

This topic describes how to manage the Dynamic Host Configuration Protocol (DHCP) options in a virtual cloud network (VCN).

Overview of DHCP Options

The Networking service uses DHCP to automatically provide configuration information to instances when they boot up. Although DHCP lets you change some settings dynamically, others are static and never change. For example, when you launch an instance, either you or Oracle specifies the instance's private IP address. Each time the instance
boots up or you restart the instance's DHCP client, DHCP passes that same private IP address to the instance. The address never changes during the instance's lifetime.

The Networking service provides **DHCP options** to let you control certain types of configuration on the instances in your VCN. You can change the values of these options at your discretion, unlike the static information that DHCP provides to the instance. The changes take effect the next time you restart a given instance's DHCP client or reboot the instance. For more details, see [Important Notes about Your Instances and DHCP Options](#) on page 2919.

Each subnet in a VCN can have a single set of DHCP options associated with it. That set of options applies to all instances in the subnet. Each VCN comes with a **default set of DHCP options** with initial values that you can change. If you don't specify otherwise, every subnet uses the VCN's default set of DHCP options.

The following table summarizes the available DHCP options you can configure.

<table>
<thead>
<tr>
<th>DHCP Option</th>
<th>Possible Values</th>
<th>Initial Value in the Default DHCP Options</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Name Server</strong></td>
<td>DNS Type: • Internet and VCN Resolver • Custom Resolver</td>
<td>DNS Type = Internet and VCN resolver. For more information, see <a href="#">Choices for DNS in Your VCN</a> on page 2910.</td>
<td>If you set DNS Type = Custom Resolver, you can specify up to three DNS servers of your choice. For more information, see <a href="#">Choices for DNS in Your VCN</a> on page 2910.</td>
</tr>
</tbody>
</table>
| **Search Domain** | A single search domain                                                      | If you've set up your VCN with a DNS label, the default value for the Search Domain option is the VCN domain name (`<VCN DNS label>.oraclevcn.com`). Otherwise, the Search Domain option is not present in the default set of DHCP options. | In general, when any set of DHCP options is initially created (the default set or a custom set you create), the Networking service automatically adds the Search Domain option and sets it to the VCN domain name (`<VCN DNS label>.oraclevcn.com`) if all of these are true:  
- The VCN has a DNS label  
- DNS Type = Internet and VCN Resolver  
- You did NOT specify a search domain of your choice during creation of the set of DHCP options.  
After the set of DHCP options is created, you can always remove the Search Domain option or set it to a different value.  
You can specify only a single search domain in a set of DHCP options. |
**Working with DHCP Options**

When you create a subnet, you specify which set of DHCP options to associate with the subnet. If you don't, the default set of DHCP options for the VCN is used. You can change which set of DHCP options the subnet uses at any time.

When creating a new set of DHCP options, you may optionally assign it a friendly name. It doesn't have to be unique, and you can change it later. Oracle automatically assigns the set of options a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

You can change the values of an individual DHCP option in a set, but notice that when you use the REST API to update a single option in a set, the new set of options replaces the entire existing set.

To delete a set of DHCP options, it must not be associated with a subnet yet. You can't delete a VCN's default set of DHCP options.

For information about the maximum number of DHCP options allowed, see Service Limits on page 215.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

**Important Notes about Your Instances and DHCP Options**

Whenever you change the value of one of the DHCP options, you must do one of the following for the change to take effect on existing instances in the subnets associated with that set of DHCP options: either restart the DHCP client on the instance, or reboot the instance.

Make sure to keep the DHCP client running so you can always access the instance. If you stop the DHCP client manually or disable NetworkManager (which stops the DHCP client on Linux instances), the instance can't renew its DHCP lease and will become inaccessible when the lease expires (typically within 24 hours). Do not disable NetworkManager unless you use another method to ensure renewal of the lease.

Stopping the DHCP client might remove the host route table when the lease expires. Also, loss of network connectivity to your iSCSI connections might result in loss of the boot drive.

Any changes you make to the `/etc/resolv.conf` file are overwritten whenever the DHCP lease is renewed or the instance is rebooted.

Changes you make to the `/etc/hosts` file are overwritten whenever the DHCP lease is renewed or the instance is rebooted. To persist your changes to the `/etc/hosts` file in Oracle Linux or CentOS instances, add the following line to `/etc/oci-hostname.conf`:

```
PRESERVE_HOSTINFO=2
```

If the `/etc/oci-hostname.conf` file does not exist, create it.

**Using the Console**

**To view a VCN's set of default DHCP options**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click DHCP Options.

   The default set and its details are displayed in the list.
To update options in an existing set of DHCP options

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click DHCP Options.
4. For the set you're interested in, click the Actions icon (three dots), and then click Edit:
   - For DNS Type: If want instances in the subnet to resolve internet hostnames and hostnames of instances in the VCN, select Internet and VCN Resolver. Or to use a DNS server of your choice, select Custom Resolver and then enter the server's IP address (three servers maximum). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - For Search Domain: If you want instances in the subnet to append a particular search domain when resolving DNS queries, enter it here. If the Search Domain option is already set to the VCN domain name and you're not sure why, see the details in Overview of DHCP Options on page 2917.
5. When you're done, click Save Changes.
6. If you have any existing instances in a subnet that uses this set of DHCP options, make sure to restart the DHCP client on each affected instance, or reboot the instance itself so that it picks up the new setting.

To create a new set of DHCP options

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click DHCP Options.
4. Click Create DHCP Options.
5. Enter the following:
   - Name: A friendly name for the set of options. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - Create in Compartment: The compartment where you want to create the set of DHCP options, if different from the compartment you're currently working in.
   - DNS Type: If want instances in the subnet to resolve internet hostnames and hostnames of instances in the VCN, select Internet and VCN Resolver. Or to use a DNS server of your choice, select Custom Resolver and then enter the server's IP address (three servers maximum). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - Search Domain: If you want instances in the subnet to append a particular search domain when resolving DNS queries, enter it here. Be aware that the Networking service automatically sets the Search Domain option in certain situations. See the details in Overview of DHCP Options on page 2917.
   - Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
6. When you're done, click Create DHCP Options.

The set of options is created and then displayed on the DHCP Options page of the compartment you chose. You can now specify this set of options when creating or updating a subnet.

To change which set of DHCP options a subnet uses

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click Subnets.
4. Click the subnet you're interested in.
5. Click Edit.
6. In the DHCP Options section, select the new set of DHCP options you want the subnet to use.
7. Click Save Changes.

    The changes take effect within a few seconds.
To delete a set of DHCP options

Prerequisite: To delete a set of DHCP options, it must not be associated with a subnet yet. You can't delete the default set of DHCP options in a VCN.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click DHCP Options.
4. For the set you want to delete, click the Actions icon (three dots), and then click Terminate.
5. Confirm when prompted.

To manage tags for a set of DHCP options

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click DHCP Options.
4. For the set you're interested in, click the Actions icon (three dots), and then click View Tags. From there you can view the existing tags, edit them, and apply new ones.

For more information, see Resource Tags on page 211.

To move a set of DHCP options to a different compartment

You can move a set of DHCP options from one compartment to another. When you move a set of DHCP options to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click DHCP Options.
4. For the set you're interested in, click the Actions icon (three dots), and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

For more information about using compartments and policies to control access to your cloud network, see Access Control on page 2831. For general information about compartments, see Managing Compartments on page 2431.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage a VCN's DHCP options, use these operations:

- ListDhcpOptions
- GetDhcpOptions
- UpdateDhcpOptions
- CreateDhcpOptions
- DeleteDhcpOptions
- ChangeDhcpOptionsCompartment

Route Tables

This topic describes how to manage the route tables in a virtual cloud network (VCN).

Overview of Routing for Your VCN

Your VCN uses virtual route tables to send traffic out of the VCN (for example, to the internet, to your on-premises network, or to a peered VCN). These virtual route tables have rules that look and act like traditional network route rules you might already be familiar with. Each rule specifies a destination CIDR block and the target (the next hop) for any traffic that matches that CIDR.
Here are basics about routing in your VCN:

- The primary routing scenario is for sending a subnet's traffic to destinations outside the VCN. A subnet has a single route table of your choice associated with it. All VNICs in that subnet are subject to the rules in the route table. The rules govern how the traffic leaving the subnet is routed.

- Traffic within the VCN is automatically handled by the VCN local routing. No route rules are required to enable that traffic. And in general: for any route table that belongs to a given VCN, you can't create a rule that lists that VCN's CIDR (or a sub-section) as the rule's destination. Oracle uses a subnet's route table only if the destination IP address is not within the VCN's CIDR block.

- If a route table has overlapping rules, Oracle uses the most specific rule in the table to route the traffic (that is, the rule with the longest prefix match).

- If there is no route rule that matches the network traffic you intend to route outside the VCN, the traffic is dropped (blackholed).

- IPv6 addressing and routing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

For important details about routing between your VCN and on-premises network, see Routing Details for Connections to Your On-Premises Network on page 2942.

### Working with Route Tables and Route Rules

Each VCN automatically comes with a default route table that has no rules. If you don't specify otherwise, every subnet uses the VCN's default route table. When you add route rules to your VCN, you can simply add them to the default table if that suits your needs. However, if you need both a public subnet and a private subnet (for example, see Scenario C: Public and Private Subnets with a VPN on page 2769), you instead create a separate (custom) route table for each subnet.

Each subnet in a VCN uses a single route table. When you create the subnet, you specify which one to use. You can change which route table the subnet uses at any time. You can also edit a route table's rules, or remove all the rules from the table.

You may optionally assign a descriptive name to a custom route table during creation. It doesn't have to be unique, and you can change it later. Oracle automatically assigns the route table a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

A route rule specifies a destination CIDR block and the target (the next hop) for any traffic that matches that CIDR. Here are the allowed types of targets for a route rule:

- **dynamic routing gateway (DRG):** For subnets that need private access to networks connected to your VCN (for example, your on-premises network connected with an IPSec VPN or FastConnect, or a peered VCN in another region).
- **internet gateway:** For public subnets that need direct access to the internet.
- **NAT gateway:** For subnets with instances that do not have public IP addresses but need outbound access to the internet.
- **service gateway:** For subnets that need private access to Oracle services such as Object Storage.
- **local peering gateway (LPG):** For subnets that need private access to a peered VCN in the same region.
- **private IP:** For subnets that need to route traffic to an instance in the VCN. For more information, see Using a Private IP as a Route Target on page 2924. Also see Overview of Routing for Your VCN on page 2921.

### Note:

You can't delete a particular resource if it's the target in a route rule. For example, you can't delete an internet gateway that has traffic routed to it. You must first delete all rules (in all route tables) with that internet gateway as the target.

When adding a route rule to a route table, you provide the destination CIDR block and target (plus the compartment where the target resides). Exception: if the target is a service gateway, instead of a destination CIDR block, you
specify an Oracle-provided string that represents the public endpoints for the service of interest. That way you don't need to know all the service's CIDR blocks, which might change over time.

If you misconfigure a rule (for example, enter the wrong destination CIDR block), the network traffic you intended to route might be dropped (blackholed) or sent to an unintended target.

You can move route tables from one compartment to another. Moving a route table doesn't affect its attachment to VCNs or subnets. When you move a route table to a new compartment, inherent policies apply immediately and affect access to the route table. For more information, see Access Control on page 2831.

You can't delete a VCN's default route table. To delete a custom route table, it must not be associated with a subnet yet. Or, in the advanced scenario of transit routing, it must not be associated with a DRG attachment or LPG in the VCN.

For information about the maximum number of route tables and route rules, see Service Limits on page 215.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

**Advanced Scenarios: Transit Routing**

This documentation includes a few basic networking scenarios to help you understand the Networking service and generally how the components work together. See scenarios A, B, and C in Networking Scenarios on page 2756.

Scenarios A–C show your on-premises network connected to a VCN by way of FastConnect or VPN Connect, and accessing only the resources in that VCN.

The following advanced routing scenarios give your on-premises network additional access beyond the resources in the connected VCN. Traffic travels from your on-premises network to the VCN, and then transits through the VCN to its destination. See these topics:

- **Transit Routing: Access to Multiple VCNs in the Same Region** on page 2780: Your on-premises network has access to multiple VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect. The VCNs are in a hub-and-spoke topology, with the on-premises network connected to the VCN that acts as the hub. The spoke VCNs are peered with the hub VCN.
- **Transit Routing: Private Access to Oracle Services** on page 2803: Your on-premises network has private access to Oracle services in the Oracle Services Network by way of the connected VCN and the VCN's service gateway. The traffic does not go over the internet.

Both of the transit routing scenarios involve creating route tables that you associate with a gateway instead of a subnet.

For example:

- For **Transit Routing: Access to Multiple VCNs in the Same Region** on page 2780, you create a route table for a DRG attachment, and then multiple route tables, each for different LPGs.
- For **Transit Routing: Private Access to Oracle Services** on page 2803, you create a route table for a DRG attachment and a route table for a service gateway.

The Networking service imposes restrictions on how the route tables can be used:

- DRG attachment: If you associate a route table with the DRG attachment on a VCN, the route table can contain only rules that use an LPG on the VCN, a service gateway on the VCN, or a private IP in the VCN as the target.
- LPG or service gateway: If you associate a route table with an LPG or a service gateway, the route table can contain only rules that use the VCN's attached DRG or a private IP in the VCN as the target.
A DRG attachment or LPG can exist without a route table associated with it. However, after you associate a route table with a DRG attachment or LPG, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table’s rules, or delete some or all of the rules.

### Using a Private IP as a Route Target

If you’re not familiar with the definition of a private IP, see [Private IP Addresses](#) on page 2864. In short: a private IP is an object that contains a private IP address and related properties and has its own **OCID**.

### General Use Cases

As mentioned earlier, Oracle uses a given subnet's route table only for traffic with a destination IP address outside the VCN. Typically you set up one or more rules to route that traffic to a gateway on the VCN (for example, a DRG connected to your on-premises network, or an internet gateway connected to the internet). However, you might want to route that traffic (going to destinations outside the VCN) through an instance in the VCN first. In that case, you can use a private IP in the VCN as the target instead of a gateway on the VCN. Here are a few reasons you might do this:

- To implement a virtual network appliance (NVA) such as a firewall or intrusion detection that filters outgoing traffic from instances.
- To manage an overlay network on the VCN, which lets you run container orchestration workloads.
- To implement Network Address Translation (NAT) in the VCN. Note that Oracle instead recommends using a **NAT gateway** with your VCN. In general, NAT enables outbound internet access for instances that don't have direct internet connectivity.

To implement these use cases, there's more to do than simply route traffic to the instance. There's also configuration required on the instance itself.

**Tip:**

You can enable high availability of the private IP route target by using a **secondary private IP address**. In the event of a failure, you can move the secondary private IP from an existing VNIC to another VNIC in the same subnet. See [Using the Console](#) on page 2866 (Console instructions) and [UpdatePrivateIp](#) (API instructions).

### Requirements for Using a Private IP as a Target

- The private IP must be in the same VCN as the route table.
- The private IP's VNIC must be configured to skip the source/destination check so that the VNIC can forward traffic. By default, VNICs are configured to perform the check. For more information, see [Overview of VNICs and Physical NICs](#) on page 2856.
- You must configure the instance itself to forward packets.
- The route rule must specify the OCID of the private IP as the target, and not the IP address itself. Exception: If you use the Console, you can instead specify the private IP address itself as the target, and the Console determines and uses the corresponding OCID in the rule.

**Important:**

A route rule with a private IP target can result in blackholing in these cases:

- The instance the private IP is assigned to is stopped or terminated
- The VNIC the private IP is assigned to is updated to enable the source/destination check or is deleted
- The private IP is unassigned from the VNIC

When a target private IP is terminated, in the Console, the route rule displays a note that the target OCID no longer exists.
Networking

For failover: If your target instance is terminated before you can move the secondary private IP to a standby, you must update the route rule to use the OCID of the new target private IP on the standby. The rule uses the target's OCID and not the private IP address itself.

General Setup Process

1. Determine which instance will receive and forward the traffic (the NAT instance, for example).
2. Choose a private IP on the instance (can be on the instance's primary VNIC or a secondary VNIC). If you want to implement failover, set up a secondary private IP on one of the VNICs on the instance.
3. Disable the source/destination check on the private IP's VNIC. See Overview of VNICs and Physical NICs on page 2856.
4. Get the OCID for the private IP. If you're using the Console, you can get either the OCID or the private IP address itself, along with the name of the private IP's compartment.
5. For the subnet that needs to route traffic to the private IP, view the subnet's route table. If the table already has a rule with the same destination CIDR but a different target, delete that rule.
6. Add a route rule with the following:
   
   • Target type: Private IP.
   • Destination CIDR block: If all traffic leaving the subnet needs to go to the private IP, use 0.0.0.0/0.
   • Compartment: The compartment of the private IP.
   • Target: The OCID of the private IP. If you're using the Console and instead enter the private IP address itself, the Console determines the corresponding OCID and uses it as the target for the route rule.
   
   • Description: An optional description of the rule.

As mentioned earlier, you must configure the instance itself to forward packets.

Using the Console

To view a VCN's default route table

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Route Tables.

   The default route table is displayed in the list of tables.

4. Click the default route table to view its details.

To update rules in an existing route table

You can add, edit, or delete rules.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Route Tables.
4. Click the route table you're interested in.
5. If you want to create a new route rule, click Add Route Rule and enter the following:

   • Target Type: See the list of target types in Overview of Routing for Your VCN on page 2921. If the target type is a DRG, the VCN's attached DRG is automatically selected as the target, and you don't have to specify
the target yourself. If the target is a private IP, make sure you've first disabled the source/destination check on
the private IP's VNIC. For more information, see Using a Private IP as a Route Target on page 2924.

- **Destination CIDR Block**: Only if the target is not a service gateway. The value is the destination CIDR block
  for the traffic. A value of 0.0.0.0/0 means that all non-intra-VCN traffic that is not already covered by other
  rules in the route table will go to the target specified in this rule.
- **Destination Service**: Only if the target is a service gateway. The value is the service CIDR label that you're
  interested in.
- **Compartment**: The compartment where the target is located.
- **Target**: The target. If the target is a private IP, enter its OCID. Or you can enter the private IP address itself, in
  which case the Console determines the corresponding OCID and uses it as the target for the route rule.
- **Description**: An optional description of the rule.

6. If you want to delete an existing rule, click the Actions icon (three dots), and then click **Remove**.
7. If you wanted to edit an existing rule, click the Actions icon (three dots), and then click **Edit**.

**To create a route table**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click **Route Tables**.
4. Click **Create Route Table**.
5. Enter the following:
   - **Name**: A friendly name for the route table. The name doesn't have to be unique, and it cannot be changed later
     in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in Compartment**: The compartment where you want to create the route table, if different from the
     compartment you're currently working in.

6. Optionally, click **Additional Route Rule** to add one or more route rules, each with the following information
   (remember, a route table can exist with no rules until you're ready to add them):
   - **Target Type**: See the list of target types in Overview of Routing for Your VCN on page 2921. If the target
     type is a DRG, the VCN's attached DRG is automatically selected as the target, and you don't have to specify
     the target yourself. If the target is a private IP, make sure you've first disabled the source/destination check on
     the private IP's VNIC. For more information, see Using a Private IP as a Route Target on page 2924.
   - **Destination CIDR Block**: Only if the target is not a service gateway. The value is the destination CIDR block
     for the traffic. A value of 0.0.0.0/0 means that all non-intra-VCN traffic that is not already covered by other
     rules in the route table will go to the target specified in this rule.
   - **Destination Service**: Only if the target is a service gateway. The value is the service CIDR label that you're
     interested in.
   - **Compartment**: The compartment where the target is located.
   - **Target**: The target. If the target is a private IP, enter its OCID. Or you can enter the private IP address itself, in
     which case the Console determines the corresponding OCID and uses it as the target for the route rule.
   - **Description**: An optional description of the rule.

7. **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to
   that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information
   about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option
   (you can apply tags later) or ask your administrator.

8. Click **Create Route Table**.

   The route table is created and then displayed on the **Route Tables** page in the compartment you chose. You can
   now specify this route table when creating or updating a subnet.

**To change which route table a subnet uses**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click **Subnets**.
4. Click the subnet you're interested in
Networking

5. Click Edit.
6. In the Route Table section, select the new route table you want the subnet to use.
7. Click Save Changes.

The changes take effect within a few seconds.

To move a route table to a different compartment

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click Route Tables.
4. Find the route table in the list, click the the Actions icon (three dots), and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To delete a route table

Prerequisite: To delete a route table, it must not be associated with a subnet yet. You can't delete the default route table in a VCN.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Route Tables.
4. Click the route table you're interested in.
5. Click Terminate.
6. Confirm when prompted.

To manage tags for a route table

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Route Tables.
4. Click the route table you're interested in.
5. Click the Tags tab to view or edit the existing tags. Or click Apply tag(s) to add new ones.

For more information, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage a VCN's route tables, use these operations:

- ListRouteTables
- GetRouteTable
- UpdateRouteTable
- CreateRouteTable
- DeleteRouteTable
- ChangeRouteTableCompartment

Dynamic Routing Gateways (DRGs)

This topic describes how to manage a dynamic routing gateway (DRG). This topic uses the terms dynamic routing gateway and DRG interchangeably. The Console uses the term Dynamic Routing Gateway, whereas for brevity the API uses DRG.

You use a DRG when connecting your existing on-premises network to your virtual cloud network (VCN) with one (or both) of these:

- IPSec VPN
Networking

- Oracle Cloud Infrastructure FastConnect

You also use a DRG when peering a VCN with a VCN in a different region:
- Remote VCN Peering (Across Regions) on page 3280

**Overview of Dynamic Routing Gateways**

You can think of a DRG as a virtual router that provides a path for private traffic (that is, traffic that uses private IPv4 addresses) between your VCN and networks outside the VCN's region.

For example, if you use an IPSec VPN or Oracle Cloud Infrastructure FastConnect (or both) to connect your on-premises network to your VCN, that private IPv4 address traffic goes through a DRG that you create and attach to your VCN. For scenarios for using a DRG to connect a VCN to your on-premises network, see Networking Scenarios on page 2756. For important details about routing to your on-premises network, see Routing Details for Connections to Your On-Premises Network on page 2942.

Also, if you decide to peer your VCN with a VCN in another region, your VCN's DRG routes traffic to the other VCN over a private backbone that connects the regions (without traffic traversing the internet). For information about connecting VCNs in different regions, see Remote VCN Peering (Across Regions) on page 3280.

**Working with DRGs and DRG Attachments**

For the purposes of access control, when creating a DRG, you must specify the compartment where you want the DRG to reside. If you're not sure which compartment to use, put the DRG in the same compartment as the VCN. For more information, see Access Control on page 2831.

You may optionally assign a friendly name to the DRG. It doesn't have to be unique, and you can change it later. Oracle automatically assigns the DRG a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

A DRG is a standalone object. To use it, you must attach it to a VCN. A VCN can be attached to only one DRG at a time, and a DRG can be attached to only one VCN at a time. You can detach a DRG and reattach it at any time. In the API, the process of attaching creates a DrgAttachment object with its own OCID. To detach the DRG, you delete that attachment object.

After attaching a DRG, you must update the routing in the VCN to use the DRG. Otherwise, traffic from the VCN will not flow to the DRG. See To route a subnet's traffic to a DRG on page 2930.

To delete a DRG, it must not be attached to a VCN or connected to another network by way of IPSec VPN, Oracle Cloud Infrastructure FastConnect, or remote VCN peering. Also, there must not be a route rule that lists that DRG as a target.

For information about the number of DRGs you can have, see Service Limits on page 215.

**Routing a Subnet's Traffic to a DRG**

The basic routing scenario sends traffic from a subnet in the VCN to the DRG. For example, if you're sending traffic from the subnet to your on-premises network, you set up a rule in the subnet's route table. The rule's destination CIDR is the CIDR for the on-premises network (or a subnet within), and the rule's target is the DRG. For more information, see Route Tables on page 2921.

**Advanced Scenarios: Transit Routing**

This documentation includes a few basic networking scenarios to help you understand the Networking service and generally how the components work together. See scenarios A, B, and C in Networking Scenarios on page 2756.

Scenarios A–C show your on-premises network connected to a VCN by way of FastConnect or VPN Connect, and accessing only the resources in that VCN.

The following advanced routing scenarios give your on-premises network additional access beyond the resources in the connected VCN. Traffic travels from your on-premises network to the VCN, and then transits through the VCN to its destination. See these topics:
• **Transit Routing: Access to Multiple VCNs in the Same Region** on page 2780: Your on-premises network has access to *multiple* VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect. The VCNs are in a hub-and-spoke topology, with the on-premises network connected to the VCN that acts as the hub. The spoke VCNs are peered with the hub VCN.

• **Transit Routing: Private Access to Oracle Services** on page 2803: Your on-premises network has *private access* to Oracle services in the Oracle Services Network by way of the connected VCN and the VCN's *service gateway*. The traffic does not go over the internet.

In the transit routing scenarios, the VCN has a route table associated with its **DRG attachment** (typically route tables are associated with a VCN's subnets). That route table lets you manage routing of traffic through the VCN that is connected to the on-premises network.

When you attach a DRG to a VCN, you can optionally associate a route table with the attachment. Or if you already have a DRG attachment, you can associate a route table with it. The route table must belong to the attached VCN. A route table associated with a DRG attachment can contain only rules that use one of the following as a target:

- A **local peering gateway** (LPG) on the attached VCN
- A **service gateway** on the attached VCN
- A **private IP** in the attached VCN

A DRG attachment can exist without a route table associated with it. However, after you associate a route table with a DRG attachment, there must always be a route table associated with it. But, you can associate a **different** route table. You can also edit the table's rules, or delete some or all of the rules.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators: see **IAM Policies for Networking** on page 2832.

**Using the Console**

In general, to use a DRG, you must complete these steps:

1. Create the DRG.
2. Attach the DRG to your VCN.
3. Route subnet traffic to the DRG. This involves updating the route table associated with each subnet that must send traffic to the DRG. If all the subnets use the VCN's default route table, you must only update that one table.

**To create a DRG**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see **Access Control** on page 2831.
3. Click **Create Dynamic Routing Gateway**.
4. Enter the following items:

   - **Create in Compartment**: The compartment where you want to create the DRG, if different from the compartment you're currently working in.
   - **Name**: A descriptive name for the DRG. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click **Create Dynamic Routing Gateway**.

The resource is created and then displayed on the **Dynamic Routing Gateways** page of the compartment you chose. It will be in the "Provisioning" state for a short period. You can connect it to other parts of your network only after provisioning is complete.

**To update a DRG's name**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG you're interested in.
3. Click **Edit**.
4. Edit the name. Avoid entering confidential information. Then click **Save Changes**.

**To attach a DRG to a VCN**

**Note:** A VCN can be attached to only one DRG at a time, and a DRG can be attached to only one VCN at a time. The attachment is automatically created in the compartment that holds the VCN.

The following instructions have you navigate to the DRG and then choose which VCN to attach. You could instead navigate to the VCN and then choose which DRG to attach.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG you want to attach.
3. Under **Resources**, click **Virtual Cloud Networks**. If you want to attach the DRG to a VCN in a different compartment than the one you're working in, choose that compartment from the list on the left side of the page.
4. Click **Attach to Virtual Cloud Network**.
5. Select the VCN.
6. (Optional) Only if you're setting up an advanced scenario for transit routing, you can associate a route table with the DRG attachment (you can do this later if you want to):
   a. Click **Show Advanced Options**.
   b. Select the route table that you want to associate with the DRG attachment.
7. Click **Attach to Virtual Cloud Network**.

The attachment will be in the "Attaching" state for a short period before it's ready.

After it's ready, make sure to create a route rule that directs subnet traffic to this DRG. See **To route a subnet's traffic to a DRG** on page 2930.

**To route a subnet's traffic to a DRG**

For each subnet that must send traffic to the DRG, you must add a route rule to the route table associated with that subnet. If all the subnets in the VCN use the default route table, you must add a rule to only that one table.

If all non-intra-VCN traffic that's not covered by another rule in the table must be routed to the DRG, then this is the new rule to add:

- **Target Type:** Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
- **Destination CIDR Block** = 0.0.0.0/0. If you want to limit the rule to a specific network (for example, your on-premises network), then use that network's CIDR instead of 0.0.0.0/0.

For step-by-step instructions, see **To update rules in an existing route table** on page 2925.

**To associate a route table with an existing DRG attachment**

**Important:**

Perform this task only if you're setting up an advanced scenario for transit routing. See **Transit Routing: Access to Multiple VCNs in the Same Region**
A DRG attachment can exist without a route table associated with it. However, after you associate a route table with a DRG attachment, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

**Prerequisites:** The route table must exist and belong to the VCN that the DRG is already attached to.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG that is attached to the VCN that has the route table.
3. Click the Actions icon (three dots), and then click either:
   - **Associate Route Table:** If the DRG attachment has no route table associated with it yet.
   - **Associate Different Route Table:** If you're changing which route table is associated with the DRG attachment.
4. Select the route table.
5. Click **Associate Route Table**.

The route table is associated with the DRG attachment.

**To detach a DRG from a VCN**

**Note:** You do not need to remove the route rule that routes traffic to the DRG before you detach the DRG from the VCN.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG you want to detach.
3. Under **Resources**, click **Virtual Cloud Networks** to see the VCN the DRG is attached to. If the VCN is in a different compartment than the one you're working in, choose that compartment from the list on the left side of the page.
4. Click the Actions icon (three dots), and then click **Detach**.
5. Confirm when prompted.

The attachment will be in the "Detaching" state for a short period.

**To delete a DRG**

**Prerequisites:**

- The DRG must not be attached to a VCN.
- The DRG must not be connected to another network by way of an IPSec VPN, FastConnect, or remote VCN peering.
- There must not be a route rule that lists the DRG as a target.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG you're interested in.
3. Click **Terminate**.
4. Confirm when prompted.

The DRG will be in the "Terminating" state for a short period while it's being deleted.

**To manage tags for a DRG**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG you're interested in.
3. Click the **Tags** tab to view or edit the existing tags. Or click **Add Tags** to add new ones.

For more information, see **Resource Tags** on page 211.
To move a dynamic routing gateway to a different compartment

You can move a dynamic routing gateway from one compartment to another. When you move a dynamic routing gateway to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Dynamic Routing Gateways.
2. Click the DRG you're interested in.
3. Find the DRG in the list, click the the Actions icon (three dots), and then click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.

For more information about using compartments and policies to control access to your cloud network, see Access Control on page 2831. For general information about compartments, see Managing Compartments on page 2431.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage your DRGs, use these operations:

- ListDrgs
- CreateDrg
- GetDrg
- UpdateDrg
- DeleteDrg
- ChangeDrgCompartment
- ListDrgAttachments
- CreateDrgAttachment: This attaches a DRG to a VCN and results in a DrgAttachment object with its own OCID. You may optionally specify a route table if you're setting up the advanced routing scenario called transit routing.
- GetDrgAttachment
- UpdateDrgAttachment: Among other things, this associates a route table with an existing DRG attachment for transit routing.
- DeleteDrgAttachment: This detaches a DRG from a VCN by deleting the DrgAttachment.

For information about route table operations, see Route Tables on page 2921.

VPN Connect

VPN Connect provides a site-to-site IPSec VPN between your on-premises network and your virtual cloud network (VCN).

Create a service request Ask the community
Networking

**VPN Connect Overview**
The VPN connection uses industry-standard IPSec protocols. The Oracle service that provides site-to-site connectivity is named VPN Connect (also referred to as an IPSec VPN). VPN Connect provides a site-to-site IPSec VPN between your on-premises network and your virtual cloud network (VCN). The IPSec protocol suite encrypts IP traffic before the packets are transferred from the source to the destination and decrypts the traffic when it arrives.

Other secure VPN solutions include OpenVPN, a Client VPN solution that can be accessed in the Oracle Marketplace. OpenVPN connects individual devices to your VCN, but not whole sites or networks.

This topic gives an overview of a site-to-site IPSec VPN for your VCN. For scenarios that include an IPSec VPN, see Scenario B: Private Subnet with a VPN on page 2761 and Scenario C: Public and Private Subnets with a VPN on page 2769.

**Required Personnel and Knowledge**
Typically the following types of personnel are involved in setting up an IPSec VPN with Oracle Cloud Infrastructure:

- **Dev Ops team member** (or similar function) who uses the Oracle Cloud Infrastructure Console to set up the cloud components required for the virtual network and IPSec VPN.
- **Network engineer** (or similar function) who configures the customer-premises equipment (CPE) device with information provided by the Dev Ops team member.

**Tip:**
The Dev Ops team member must have the required permission to create and manage the cloud components. If the person is the default administrator for your Oracle Cloud Infrastructure tenancy or a member of the Administrators group, then they have the required permission. For information about

---

**Use cases**

**Securely connect to Oracle Cloud**
Securely connect your existing infrastructure to the cloud by using industry-standard encryption algorithms.

**Connect multiple locations to the cloud**
Connect your headquarters, branch locations, and private data centers to Oracle Cloud so all of your offices can access applications.

**Connect to other public clouds**
Securely connect to workloads in other providers’ cloud services.

**Build redundant connectivity for Oracle FastConnect**
Already have Oracle FastConnect? VPN Connect can provide a redundant connection to Oracle Cloud Infrastructure.
restricting access to your networking components, see Access Control on page 2831.

The personnel should be familiar with the following concepts and definitions:

- The fundamentals of Oracle Cloud Infrastructure
- The basic Networking service components
- General IPSec VPN tunnel functionality

**CLOUD RESOURCES**

Anything you provision on a cloud platform. For example, with Oracle Cloud Infrastructure, a cloud resource can refer to a VCN, compute instance, user, compartment, load balancer, or any other service component on the platform.

**ON-PREMISES**

A widely used term in cloud technologies that refers to your traditional data center environments. On-premises can refer to a colocation scenario, a dedicated floor space, a dedicated data center building, or a desktop running under your desk.

**ORACLE CLOUD IDENTIFIER (OCID)**

A unique identifier assigned to each resource that you provision on Oracle Cloud Infrastructure. The OCID is a long string that Oracle automatically generates. You can't choose the value for an OCID or change a resource's OCID. For more information, see Resource Identifiers on page 197.

**About the Oracle IPSec VPN**

In general, IPSec can be configured in the following modes:

- **Transport mode:** IPSec encrypts and authenticates only the actual payload of the packet, and the header information stays intact.
- **Tunnel mode (supported by Oracle):** IPSec encrypts and authenticates the entire packet. After encryption, the packet is then encapsulated to form a new IP packet that has different header information.

Oracle Cloud Infrastructure supports only the tunnel mode for IPSec VPNs.

Each Oracle IPSec VPN consists of multiple redundant IPSec tunnels. For a given tunnel, you can use either Border Gateway Protocol (BGP) dynamic routing or static routing to route that tunnel's traffic. More details about routing follow.

IPSec VPN site-to-site tunnels offer the following advantages:

- Public internet lines are used to transmit data, so dedicated, expensive lease lines from one site to another aren't necessary.
- The internal IP addresses of the participating networks and nodes are hidden from external users.
- The entire communication between the source and destination sites is encrypted, significantly lowering the chances of information theft.

**Note:**
IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

**Routing for the Oracle IPSec VPN**

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE device to use both tunnels (if your device supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing:** The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
• **Static routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

**Important Routing Details for an Oracle IPSec VPN**

Here are important details to understand about routing for your IPSec VPN:

**Routing choices:**

- Originally, the Oracle IPSec VPN supported only static routing, and you were required to provide at least one static route for the overall IPSec connection.
- Now two different types of routing are available (BGP and static routing), and you configure the routing type per tunnel. *Only one type of routing at a time is supported for a given tunnel.*
- In general, Oracle encourages you to use the same routing type for all tunnels in your IPSec connection. Exception: if you're in the process of transitioning between static routing and BGP, then one tunnel might temporarily still use static routing while the other has already been switched to BGP.
- When you create an IPSec connection, static routing is the default type of routing for all tunnels *unless you explicitly configure each tunnel to use BGP.*

**Routing information required:**

- If you choose BGP, for each tunnel you must provide two IP addresses (one for each of the two BGP speakers in the tunnel's BGP session). The addresses must be in the encryption domain for the IPSec connection. You must also provide the BGP autonomous system number (BGP ASN) for your network.
- If you choose static routing, you must provide at least one static route (maximum 10). The static routes are configured with the *overall IPSec connection,* so the same set of static routes are used for *all* tunnels in the IPSec connection that are configured to use static routing. You can change the static routes at any time after creating the IPSec connection. If you're doing PAT between your CPE device and VCN, the static route for the IPSec connection is the PAT IP address. See Example Layout with PAT on page 2966.
- If you choose static routing, you may optionally provide an IP address for each end of the tunnel for the purposes of tunnel troubleshooting or monitoring.
- If the tunnel is configured to use BGP, the IPSec connection's static routes are ignored. Any static routes associated with the IPSec connection are used for routing a given tunnel's traffic *only if that tunnel is configured to use static routing.* This is especially relevant if you have an IPSec VPN that uses static routing, but want to switch to using BGP.

**Changing the routing:**

- If you want to change a tunnel from BGP to static routing, you must first ensure that the IPSec connection itself has at least one static route associated with it.
- You can change an existing tunnel's routing type at any time (unless the tunnel is currently being provisioned by Oracle). While you change the routing, the tunnel remains up (its IPSec status does not change). However, traffic flowing through the tunnel is disrupted temporarily during re provisioning and while you reconfigure your CPE device. For information about making changes to an existing IPSec VPN, see Working with VPN Connect on page 3156.
- Because you configure the routing type separately for each tunnel, if you want to switch your IPSec VPN from static routing to BGP, you can do it one tunnel at a time. This avoids the entire IPSec VPN being down. For instructions, see Changing from Static Routing to BGP Dynamic Routing on page 3160.

**Route Advertisements and Path Preferences When You Have Multiple Connections**

When you use BGP, the DRG attached to your VCN advertises routes to your CPE.

If you set up multiple connections between your on-premises network and VCN, you must understand what routes the DRG advertises and how to set path preferences to use your desired connection.

For important information, see Routing Details for Connections to Your On-Premises Network on page 2942.
Preferring a Specific Tunnel in the IPSec VPN

Within an IPSec VPN, you can influence which tunnel is preferred. Here are items you can configure:

- **Your CPE's BGP local preference**: If you use BGP, you can configure the BGP local preference attribute on your CPE device to control which tunnel is preferred for connections initiated from your on-premises network to your VCN. Because Oracle generally uses asymmetric routing, you must configure other attributes if you want Oracle to respond on that same tunnel. See the next two items.

- **More specific routes on the preferred tunnel**: You can configure your CPE to advertise more specific routes for the tunnel that you want to prefer. Oracle uses the route with the longest prefix match when responding to or initiating connections.

- **AS path prepending**: BGP prefers the shortest AS path, so if you use BGP, you can use AS path prepending to control which tunnel has the shortest path for a given route. Oracle uses the shortest AS path when responding to or initiating connections.

Overview of the IPSec VPN Components

If you're not already familiar with the basic Networking service components, see Networking on page 2746 before proceeding.

When you set up an IPSec VPN for your VCN, you must create several Networking components. You can create the components with either the Console or the API. See the following diagram and description of the components.

**cpe object**

At your end of the IPSec VPN is the actual device in your on-premises network (whether hardware or software). The term *customer-premises equipment (CPE)* is commonly used in some industries to refer to this type of on-premises equipment. When setting up the VPN, you must create a virtual representation of the device. Oracle calls the virtual representation a CPE, but this documentation typically uses the term *CPE object* to help distinguish the virtual representation from the actual CPE device. The CPE object contains basic information about your device that Oracle needs.
**DYNAMIC ROUTING GATEWAY (DRG)**

At Oracle’s end of the IPSec VPN is a virtual router called a dynamic routing gateway, which is the gateway into your VCN from your on-premises network. Whether you’re using an IPSec VPN or Oracle Cloud Infrastructure FastConnect private virtual circuits to connect your on-premises network and VCN, the traffic goes through the DRG. For more information, see Dynamic Routing Gateways (DRGs) on page 2927.

A network engineer might think of the DRG as the **VPN headend**. After creating a DRG, you must **attach** it to your VCN, using either the Console or API. You must also add one or more route rules that route traffic from the VCN to the DRG. Without that DRG attachment and the route rules, traffic does not flow between your VCN and on-premises network. At any time, you can detach the DRG from your VCN but maintain all the remaining VPN components. You can then reattach the DRG, or attach it to another VCN.

**ipsec connection**

After creating the CPE object and DRG, you connect them by creating an IPSec connection, which you can think of as a parent object that represents the overall IPSec VPN. The IPSec connection has its own **OCID**. When you create this component, you configure the type of routing to use for each tunnel, and you provide any related routing information.

**TUNNEL**

An IPSec tunnel is used to encrypt traffic between secure IPSec endpoints. Oracle creates two tunnels in each IPSec connection for redundancy. Each tunnel has its own **OCID**. Oracle recommends that you configure your CPE device to support both tunnels in case one fails or Oracle takes one offline for maintenance. Each tunnel has configuration information that your network engineer needs when configuring your CPE device. This information includes an IP address and shared secret, as well as ISAKMP and IPSec parameters. You can use the CPE Configuration Helper to gather the information that the network engineer needs. For more information, see Supported IPSec Parameters on page 2945 and Verified CPE Devices on page 2969.

**Access Control for the Components**

For the purposes of access control, when you set up the IPSec VPN, you must specify the compartment where you want each of the components to reside. If you’re not sure which compartment to use, put all the components in the same compartment as the VCN. Note that the IPSec tunnels always reside in the same compartment as the parent IPSec connection. For information about compartments and restricting access to your networking components, see Access Control on page 2831.

**Component Names and Identifiers**

You can optionally assign a descriptive name to each of the components when you create them. These names don't have to be unique, although it's a best practice to use unique names across your tenancy. Avoid entering confidential information. Oracle automatically assigns each component an OCID. For more information, see Resource Identifiers.

**If Your CPE Is Behind a NAT Device**

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's **public** IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's **private** IP address, as show in the following diagram.
Note:

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

About the Tunnel Shared Secret

Each tunnel has a shared secret. By default, Oracle assigns the shared secret to the tunnel unless you provide a shared secret yourself. You can provide a shared secret for each tunnel when you create the IPSec connection, or later after the tunnels are created. For the shared secret, only letters, numbers, and spaces are allowed. If you change an existing tunnel's shared secret, the tunnel goes down while it is being reprovisioned.

For instructions, see Changing the Shared Secret That an IPSec Tunnel Uses on page 3159.

Resources for Configuring the CPE

Your network engineer must configure the CPE at your end of the IPSec connection. To make it easier, Oracle provides these resources:

- **CPE Configuration Helper**: A tool in the Oracle Console that generates a set of content that the network engineer can use when configuring the CPE.
- **A list of verified CPE devices**: For each device, Oracle provides configuration instructions.
- **A list of supported IPSec parameters**: If your CPE is not on the list of verified devices, you can use this list of parameters to configure your CPE.

For more information, also see CPE Configuration on page 2967.

Monitoring Your Connection

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring your connection, VPN Connect Metrics on page 3164.

What’s Next?

See these related topics:

- **VPN Connect Quickstart** on page 2939
- **Setting Up VPN Connect** on page 2949
- **Supported IPSec Parameters** on page 2945
The VPN Connect workflow is the quickest way to set up a site-to-site VPN between your on-premises network and your virtual cloud network (VCN). The workflow is a guided, step-by-step process in the Console that sets up the VPN plus related Networking service components.

Other secure VPN solutions include OpenVPN, a Client VPN solution that can be accessed in the Oracle Marketplace. OpenVPN connects individual devices to your VCN, but not whole sites or networks.

**Purpose of the Workflow**

VPN Connect involves setting up and configuring several Networking service components. The workflow sets up those components for you. In general, the workflow does the following:

- Uses a template with assumptions that will help you get started.
- Asks you for some basic network information.
- Sets up the Networking service components for you.
- Lets you generate configuration content for a network engineer to use when configuring your customer-premises equipment (CPE) device.

The workflow is a task within the overall process of setting up VPN Connect, which is illustrated in the following diagram. The workflow is the shaded box.

Notice that the overall process includes work by a network engineer in your organization. That engineer provides information that you, in turn, must supply during the workflow. The workflow returns information that the network engineer needs when configuring your CPE device. You can use the CPE Configuration Helper to consolidate the necessary information into an organized template for the network engineer.

The following short sections summarize each task.

**Task 1: Information to get from your network engineer**

- CPE device's public IP address.
- If the CPE is behind a NAT device, get the CPE IKE identifier. For more information, see Overview of the IPSec VPN Components on page 2936.
- On-premises network routes.
- If you use BGP dynamic routing with the VPN:
  - Your network's BGP ASN
  - For each of the two IPSec tunnels that will be created, the pair of BGP IP addresses (with subnet mask) that you want to use for the inside tunnel interfaces at the ends of each tunnel. For example:
    - Tunnel 1: Inside tunnel interface - CPE: 10.0.0.8/31
    - Tunnel 1: Inside tunnel interface - Oracle: 10.0.0.9/31
    - Tunnel 2: Inside tunnel interface - CPE: 10.0.0.16/31
    - Tunnel 2: Inside tunnel interface - Oracle: 10.0.0.17/31
• If you don't already have a VCN: The CIDR to use for the new VCN that will be created. For the workflow, the allowed VCN size is /16 to /24. The CIDR must not overlap with your on-premises network.

Task 2: Workflow
You walk through the workflow in the Console. For more information, see these sections:
• Where to Access the Workflow in the Console on page 2942
• What the Workflow Creates for You on page 2940

Task 3: Information to give to your network engineer
You use the CPE Configuration Helper to generate configuration content that your network engineer can use to configure the CPE.

The content includes these items:
• For each IPSec tunnel, the Oracle VPN IP address and shared secret.
• The supported IPSec parameter values.
• Information about the VCN.
• CPE-specific configuration information.

Task 4: CPE configuration
Your network engineer takes the information you provide and configures your CPE device.

Task 5: Testing
You and the network engineer test the connection and confirm that traffic is flowing.

Alternative to the Workflow
If you prefer, you can manually set up VPN Connect yourself. For step-by-step instructions, see Setting Up VPN Connect on page 2949.

What the Workflow Creates for You
Most Oracle customers who set up a VPN Connect already have a VCN to connect to their on-premises network. In that case, the workflow creates the numbered components in the following diagram. The table describes each component.

<table>
<thead>
<tr>
<th>Number</th>
<th>Component</th>
<th>Description</th>
<th>Can Use Existing One or Create New One?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CPE</td>
<td>A CPE is a virtual representation of your actual CPE device. This virtual representation contains basic information such as the CPE device's public IP address.</td>
<td>Yes, you can either use an existing CPE or the workflow creates a new one.</td>
</tr>
<tr>
<td>Number</td>
<td>Component</td>
<td>Description</td>
<td>Can Use Existing One or Create New One?</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Dynamic routing gateway (DRG)</td>
<td>A DRG is a <em>virtual representation</em> of the actual router at the Oracle end of your VPN Connect.</td>
<td>Yes. If you use an existing one, it must not already be attached to a VCN.</td>
</tr>
<tr>
<td>3</td>
<td>VCN Connect IPSec tunnels</td>
<td>The workflow creates two <em>IPSec tunnels</em>, each with specific configuration information that you must provide to your network engineer. Note: The workflow uses IKEv1 for the tunnels. If you want to use IKEv2 instead, after creating the IPSec connection, edit each tunnel in the Oracle Console to use IKEv2. Then configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For more information, see Using IKEv2 on page 3158.</td>
<td>No. The workflow automatically creates the tunnels.</td>
</tr>
</tbody>
</table>
• Default security list. The workflow configures the subnet to use this security list, which automatically comes with default rules to enable basic traffic flow. The workflow also adds these rules:
  • One or more rules to allow all types of traffic from your on-premises network. There's one rule per on-premises network route that you provide in the workflow. Notice that the security list does not include rules to allow ping.

After the workflow completes, you can modify the VCN's configuration in any way you want. For example, you could edit the route rules and security list rules, add more subnets, remove the internet gateway, and so on.

After the workflow completes, you can also use the CPE Configuration Helper to generate configuration content that your network engineer can use to configure the CPE.

**Where to Access the Workflow in the Console**

**Option 1:**
1. In the Console, click the Oracle Cloud icon at the top of the page to go to the Console home page.

   The page has a Quick Actions section to take you directly to common tasks.
2. Click the quick action for Networking: Set up a network with a wizard.
3. Select VCN with VPN Connect and Internet Connectivity, and then click Start Workflow.

**Option 2:**
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click Networking Quickstart.
3. Select VCN with VPN Connect and Internet Connectivity, and then click Start Workflow.

**Related Topics**
- VPN Connect Overview on page 2933
- Setting Up VPN Connect on page 2949
- Supported IPSec Parameters on page 2945
- CPE Configuration on page 2967
- Verified CPE Devices on page 2969
- Using the CPE Configuration Helper on page 2970
- Working with VPN Connect on page 3156
- VPN Connect FAQ
- Using the API for VPN Connect on page 3163

**Routing Details for Connections to Your On-Premises Network**

You might use multiple site-to-site connections between your on-premises network and virtual cloud network (VCN) for redundancy or other reasons.

For example, you might use both FastConnect private peering and VPN Connect to the dynamic routing gateway (DRG) attached to your VCN. Or perhaps you use redundant VPN Connect connections to the DRG (for an example scenario, see Example Layout with Multiple Geographic Areas on page 2965). Or perhaps you use FastConnect public peering, FastConnect private peering, and VPN Connect.

This topic covers important details about route advertisement and path preferences when you have multiple connections.

**DRG Route Advertisements to Your On-Premises Network**

FastConnect private peering and VPN Connect provide your on-premises network with private access to a VCN. Both types of connections terminate on a single DRG that is attached to the VCN. Remember that VPN Connect can use either Border Gateway Protocol (BGP) or static routing, or a combination. FastConnect always uses BGP for route advertisements.

The DRG advertises the routes for the individual subnets in the DRG's attached VCN. A DRG can be attached to only a single VCN, and a VCN can be attached to only a single DRG.
If you set up transit routing to multiple VCNs for your on-premises network, the DRG advertises other routes. Transit routing is an advanced routing scenario that involves a single FastConnect or VPN Connect and multiple peered VCNs in a hub-and-spoke layout. With transit routing, the DRG also advertises routes for the VCNs that are peered with the DRG's attached VCN (the hub).

If you set up your on-premises network with private access to Oracle services through the VCN's service gateway, the DRG advertises more routes. They are routes for the Oracle Services Network, which is available with the service gateway. For a list of those ranges, see Public IP Addresses for VCNs and the Oracle Services Network on page 193.

Important:
If you're using VPN Connect with static routing, and you've configured the VCN to give your on-premises network private access to Oracle services, you must configure your edge device with the routes for the Oracle Services Network public IP ranges that are advertised by the DRG over the private path (through the service gateway). For a list of those ranges, see Public IP Addresses for VCNs and the Oracle Services Network on page 193.

Routing Preferences for Traffic from Oracle to Your On-Premises Network
This section describes how Oracle chooses which path to use when sending traffic to your on-premises network. The traffic can be for responding to a request or initiating new connections.

Routers generally prefer to use the most specific route (the one with the longest prefix match).

However, if the routes for the different paths are the same, Oracle uses the shortest AS path when sending traffic to your on-premises network, regardless of which path was used to initiate the connection to Oracle. Therefore asymmetric routing is allowed. Asymmetric routing here means that Oracle's response to a request can follow a different path than the request. For example, depending on how your edge device (also called your customer-premises equipment, or CPE) is configured, you could send a request over VPN Connect, but the Oracle response could come back over FastConnect. If you want to force routing to be symmetric, Oracle recommends using BGP and AS path prepending with your routes to influence which path Oracle uses when responding to and initiating connections.

Oracle implements AS path prepending to establish preference on which path to use if your edge device advertises the same route and routing attributes over multiple different connection types between your on-premises network and VCN. The details are summarized in the following table. Unless you're influencing routing in some way, when the same route is advertised over multiple paths to the DRG at the Oracle end of the connections, Oracle prefers the paths in the following order:

<table>
<thead>
<tr>
<th>Oracle preference</th>
<th>Path</th>
<th>Details of how Oracle prefers the path</th>
<th>Resulting AS path for the route</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FastConnect</td>
<td>Oracle prepends no ASNs to the routes that your edge device advertises, for a total AS path length of 1.</td>
<td>Your ASN</td>
</tr>
<tr>
<td>2</td>
<td>VPN Connect with BGP routing</td>
<td>Oracle prepends a single private ASN on all the routes that your edge device advertises over VPN Connect with BGP, for a total AS path length of 2.</td>
<td>Private ASN, Your ASN</td>
</tr>
</tbody>
</table>
If you have two connections of the same type (for example, two IPSec VPNs that both use BGP), and you advertise the same routes across both connections, **Oracle prefers the oldest continuously advertised route** when responding to requests or initiating connections.

The above table above assumes you are sending a single autonomous system number in your AS path. Oracle honors the complete AS path you send. If you use static routing, and also send an AS path that has "Your ASN" plus 2 or more other ASNs, it can cause unexpected behavior because Oracle's routing preference may change accordingly.

While static policy-based VPN routing behavior is documented above, Oracle also recommends that if you use FastConnect connections with VPN backup, you employ BGP on your IPSEC route-based VPN. This strategy allows you to have full control of failover behavior.

**Routing Preferences for Traffic from Your On-Premises Network to Oracle**

You can configure your edge device to prefer a specific path when sending traffic from your on-premises network to Oracle. The following section describes a particular situation where you must do that to ensure a consistent traffic path if your on-premises hosts use Oracle services.

Your on-premises network can access public Oracle Services Network services such as Object Storage over multiple paths. You can use public paths, such as the internet or FastConnect public peering. With these public paths, the on-premises hosts communicate with Oracle services by using public IP addresses.

You can also set up your on-premises network with private access to Oracle services through the VCN's service gateway. A service gateway lets hosts in your on-premises network use any of the services listed in Service Gateway: Supported Cloud Services in Oracle Services Network and communicate with those Oracle services from your private IP addresses.

If you've configured your on-premises network with multiple connection paths to Oracle services, your edge device may receive route advertisement of the Oracle services' public IP address routes over multiple paths. Here are the possible paths you can use with your on-premises network:

- Public access paths:
  - Internet service provider (ISP)
  - FastConnect public peering
- Private access paths by way of the VCN's DRG and service gateway:
  - FastConnect private peering
  - VPN Connect

Your edge device receives route advertisements from the DRG and possibly from routers over public paths. Most of the routes for Oracle services that the DRG advertises have a longer prefix (they are more specific) than the routes for Oracle services that are advertised over the public access paths. Therefore, if you set up your network with both public access and private access to Oracle services, **you must configure your edge device to prefer the private access path to the DRG** for traffic from the on-premises network to Oracle services. Setting up both public and private access ensures a consistent path for access to Oracle services.

For a list of the public IP ranges advertised over FastConnect public peering, see [FastConnect Public Peering Advertised Routes](#) on page 3219.
For a list of the regional public IP ranges advertised over the private paths (for a VCN with a service gateway), see Public IP Addresses for VCNs and the Oracle Services Network on page 193.

**Related Resources**

For additional information, see these related resources:

- Connectivity Redundancy Guide (PDF)
- VPN Connect Best Practices (PDF)
- FastConnect Redundancy Best Practices on page 3185

**Supported IPSec Parameters**

This topic lists the supported phase 1 (ISAKMP) and phase 2 (IPSec) configuration parameters for VPN Connect. Oracle chose these values to maximize security and to cover a wide range of CPE devices. If your CPE device is not on the list of verified devices, use the information here to configure your device.

You can also use the CPE Configuration Helper to gather information that a network engineer uses when configuring the CPE device.

**Important:**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec VPN connection. Even if you configure one tunnel as primary and another as backup, traffic from your VCN to your on-premises network can use any tunnel that is "up" on your device. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

**Supported Encryption Domain or Proxy ID**

The values for the encryption domain (also known as a proxy ID, security parameter index (SPI), or traffic selector) depend on whether your CPE supports route-based tunnels or policy-based tunnels. For more information about the correct encryption domain values to use, see Supported Encryption Domain or Proxy ID on page 2948.

**Supported Parameters for the Commercial Cloud**

This section lists the supported parameters if your VPN Connect is for the commercial cloud. For a list of the commercial cloud regions, see Regions and Availability Domains on page 180.

For some parameters, Oracle supports multiple values, and the recommended one is noted.

Oracle supports the following parameters for IKEv1 or IKEv2. Check the documentation for your particular CPE to confirm which parameters the CPE supports for IKEv1 or IKEv2.

**Phase 1 (ISAKMP)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAKMP Protocol</td>
<td>Version 1</td>
</tr>
<tr>
<td>Exchange type</td>
<td>Main mode</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Pre-shared keys *</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>AES-256-cbc (recommended)</td>
</tr>
<tr>
<td></td>
<td>AES-192-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-128-cbc</td>
</tr>
</tbody>
</table>
### Networking

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication algorithm</strong></td>
<td>SHA-2 384 (recommended)</td>
</tr>
<tr>
<td></td>
<td>SHA-2 256</td>
</tr>
<tr>
<td></td>
<td>SHA-1 (also called SHA or SHA1-96)</td>
</tr>
<tr>
<td><strong>Diffie-Hellman group</strong></td>
<td>group 2 (MODP 1024)</td>
</tr>
<tr>
<td></td>
<td>group 5 (MODP 1536)</td>
</tr>
<tr>
<td></td>
<td>group 14 (MODP 2048)</td>
</tr>
<tr>
<td></td>
<td>group 19 (ECP 256)</td>
</tr>
<tr>
<td></td>
<td><strong>group 20 (ECP 384)</strong> (recommended)</td>
</tr>
<tr>
<td><strong>IKE session key lifetime</strong></td>
<td>28800 seconds (8 hours)</td>
</tr>
<tr>
<td>* Only numbers, letters, and spaces are allowed characters in pre-shared keys.</td>
<td></td>
</tr>
</tbody>
</table>

### Phase 2 (IPSec)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPSec Protocol</strong></td>
<td>ESP, tunnel mode</td>
</tr>
<tr>
<td><strong>Encryption algorithm</strong></td>
<td><strong>AES-256-gcm</strong> (recommended)</td>
</tr>
<tr>
<td></td>
<td>AES-192-gcm</td>
</tr>
<tr>
<td></td>
<td>AES-128-gcm</td>
</tr>
<tr>
<td></td>
<td>AES-256-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-192-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-128-cbc</td>
</tr>
<tr>
<td><strong>Authentication algorithm</strong></td>
<td>If using GCM (Galois/Counter Mode), no authentication algorithm is required because authentication is included with GCM encryption.</td>
</tr>
<tr>
<td></td>
<td>If not using GCM, the following options are supported:</td>
</tr>
<tr>
<td></td>
<td><strong>HMAC-SHA-256-128</strong> (recommended)</td>
</tr>
<tr>
<td></td>
<td>HMAC-SHA1-96</td>
</tr>
<tr>
<td><strong>IPSec session key lifetime</strong></td>
<td>3600 seconds (1 hour)</td>
</tr>
<tr>
<td><strong>Perfect Forward Secrecy (PFS)</strong></td>
<td>enabled, group 5</td>
</tr>
</tbody>
</table>

**Supported Parameters for the Government Cloud**

This section lists the supported parameters if your VPN Connect is for the Government Cloud. For more information, see For All US Government Cloud Customers on page 148.

For some parameters, Oracle supports multiple values, and the recommended one is highlighted in **bold text**.

Oracle supports the following parameters for IKEv1 or IKEv2. Check the documentation for your particular CPE to confirm which parameters the CPE supports for IKEv1 or IKEv2.
### Phase 1 (ISAKMP)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAKMP protocol</td>
<td>Version 1</td>
</tr>
<tr>
<td>Exchange type</td>
<td>Main mode</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Pre-shared keys *</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>AES-256-cbc (recommended)</td>
</tr>
<tr>
<td></td>
<td>AES-192-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-128-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>SHA-2 384 (recommended)</td>
</tr>
<tr>
<td></td>
<td>SHA-2 256</td>
</tr>
<tr>
<td></td>
<td>SHA-1 (also called SHA or SHA1-96)</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>group 14 (MODP 2048)</td>
</tr>
<tr>
<td></td>
<td>group 19 (ECP 256)</td>
</tr>
<tr>
<td></td>
<td>group 20 (ECP 384) (recommended)</td>
</tr>
<tr>
<td>IKE session key lifetime</td>
<td>28800 seconds (8 hours)</td>
</tr>
</tbody>
</table>

* Only numbers, letters, and spaces are allowed characters in pre-shared keys.

### Phase 2 (IPSec)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec protocol</td>
<td>ESP, tunnel mode</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>AES-256-gcm (recommended)</td>
</tr>
<tr>
<td></td>
<td>AES-192-gcm</td>
</tr>
<tr>
<td></td>
<td>AES-128-gcm</td>
</tr>
<tr>
<td></td>
<td>AES-256-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-192-cbc</td>
</tr>
<tr>
<td></td>
<td>AES-128-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>If using GCM (Galoiis/Counter Mode), no authentication algorithm is required because authentication is included with GCM encryption.</td>
</tr>
<tr>
<td></td>
<td>If not using GCM, use HMAC-SHA-256-128.</td>
</tr>
<tr>
<td>IPSec session key lifetime</td>
<td>3600 seconds (1 hour)</td>
</tr>
<tr>
<td>Perfect Forward Secrecy (PFS)</td>
<td>enabled, group 14</td>
</tr>
</tbody>
</table>
Networking

**Supported Encryption Domain or Proxy ID**

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

![Note:

Other vendors or industry documentation might use the term *proxy ID*, *security parameter index (SPI)*, or *traffic selector* when referring to SAs or encryption domains.](image)

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels**: Also called *next-hop-based tunnels*. A route table lookup is performed on a packet's destination IP address. If that route's egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

- **Policy-based tunnels**: The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

**Encryption domain for route-based tunnels**

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address**: Any (0.0.0.0/0)
- **Destination IP address**: Any (0.0.0.0/0)
- **Protocol**: IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

**Encryption domains for policy-based tunnels**

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an *encryption domain*.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.
Networking

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

Setting Up VPN Connect

This topic gives instructions for constructing a site-to-site VPN Connect link to your VCN. For general information about IPSec VPNs, see VPN Connect Overview on page 2933.

Before You Get Started

To prepare, do these things first:

- Read this section: Routing for the Oracle IPSec VPN on page 2934
- Answer these questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is your VCN’s CIDR?</td>
<td></td>
</tr>
<tr>
<td>What is the public IP address of your CPE device? If you have multiple devices for redundancy, get the IP address for each.</td>
<td></td>
</tr>
<tr>
<td>Note: If your CPE device is behind a NAT device, see Overview of the IPSec VPN Components on page 2936 and also Requirements and Prerequisites on page 2968.</td>
<td></td>
</tr>
</tbody>
</table>
Networking

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will you use port address translation (PAT) between each CPE device and your VCN?</td>
<td></td>
</tr>
<tr>
<td>What type of routing do you plan to use? If you want BGP dynamic routing, list the BGP session IP addresses to use and the ASN of your network. The IP addresses must be part of the IPSec VPN's encryption domain. If you want static routing, what are the static routes for your on-premises network? See Routing for the Oracle IPSec VPN on page 2934. Do you plan to use policy based routing or multiple encryption domains? See Encryption domains for policy-based tunnels on page 2948. Do you want to provide each tunnel's shared secret or let Oracle assign them? See Overview of the IPSec VPN Components on page 2936.</td>
<td></td>
</tr>
<tr>
<td>• Draw a diagram of your network layout (for examples, see the first task in Example: Setting Up a Proof of Concept IPSec VPN on page 2951). Think about which parts of your on-premises network need to communicate with your VCN, and the reverse. Map out the routing and security rules that you need for your VCN.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip:</strong> If you have an existing Oracle IPSec VPN that uses static routing, you can change the tunnels to instead use BGP dynamic routing.</td>
<td></td>
</tr>
</tbody>
</table>

**Overall Process**

Here's the overall process for setting up an IPSec VPN:

1. **Complete the tasks listed in Before You Get Started on page 2949.**
2. **Set up the IPSec VPN components** (instructions in Example: Setting Up a Proof of Concept IPSec VPN on page 2951):
   a. Create your VCN.
   b. Create a DRG.
   c. Attach the DRG to your VCN.
   d. Create a route table and route rule for the DRG.
   e. Create a security list and required rules.
   f. Create a subnet in the VCN.
   g. Create a CPE object and provide your CPE device's public IP address.
   h. Create an IPSec connection to the CPE object and provide required routing information.
3. **Use the CPE Configuration Helper:** Your network engineer must configure your CPE device with information that Oracle provides during the previous steps. The CPE Configuration Helper generates the information for your network engineer. For more information, see Using the CPE Configuration Helper on page 2970 and also CPE Configuration on page 2967.
4. **Have your network engineer configure your CPE device.**
5. **Validate connectivity.**
   If you plan to set up redundant connections, see the Connectivity Redundancy Guide.
**Example: Setting Up a Proof of Concept IPSec VPN**

**Tip:**
Oracle offers a quickstart workflow to make it easier to set up VPN Connect. For more information, see [VPN Connect Quickstart](#) on page 2939.

This example scenario shows how to set up a single IPSec VPN with a simple layout that you might use for a proof of concept (POC). It follows tasks 1 and 2 in [Overall Process](#) on page 2950 and shows each component in the layout being created. For each task, there's a corresponding screenshot from the Console to help you understand what information is needed. For more complex layouts, see [Example Layout with Multiple Geographic Areas](#) on page 2965 or [Example Layout with PAT](#) on page 2966.

**Task 1: Gather information**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is your VCN's CIDR?</td>
<td>172.16.0.0/16</td>
</tr>
<tr>
<td>What is the public IP address of your CPE device? If you have multiple devices for redundancy, get the IP address for each. Note: If your CPE device is behind a NAT device, see <a href="#">Overview of the IPSec VPN Components</a> on page 2936 and also <a href="#">Requirements and Prerequisites</a> on page 2968.</td>
<td>142.34.145.37</td>
</tr>
<tr>
<td>Will you be doing port address translation (PAT) between each CPE device and your VCN?</td>
<td>No</td>
</tr>
<tr>
<td>What type of routing do you plan to use? There are three mutually exclusive choices:</td>
<td><strong>BGP dynamic routing example:</strong></td>
</tr>
<tr>
<td>If you plan to use BGP dynamic routing, list the BGP session IP addresses to use and the ASN of your network.</td>
<td>Tunnel 1:</td>
</tr>
<tr>
<td>If you plan to use static routing, list the static routes for your on-premises network. See <a href="#">Routing for the Oracle IPSec VPN</a> on page 2934.</td>
<td>• BGP Inside tunnel interface - CPE: 10.0.0.16/31</td>
</tr>
<tr>
<td>If you plan to use policy-based routing or require multiple encryption domains, list the IPv4 or IPv6 CIDR blocks used on each end of the connection. See <a href="#">Encryption domains for policy-based tunnels</a> on page 2948.</td>
<td>• BGP Inside tunnel interface - Oracle: 10.0.0.17/31</td>
</tr>
<tr>
<td>Do you want to provide each tunnel's shared secret or let Oracle assign them? See <a href="#">Overview of the IPSec VPN Components</a> on page 2936.</td>
<td><strong>Static routing example:</strong> Use 10.0.0.0/16 for the static route for a simple POC.</td>
</tr>
<tr>
<td></td>
<td><strong>Policy-based routing example:</strong></td>
</tr>
<tr>
<td></td>
<td>Use ??? for a simple POC.</td>
</tr>
<tr>
<td></td>
<td>Let Oracle assign.</td>
</tr>
</tbody>
</table>
Here’s an example diagram for task 1 that uses BGP dynamic routing:

Here’s an example diagram for task 1 that uses static routing:

Here’s an example diagram for task 1 that uses policy-based routing:

Task 2a: Create the VCN
If you already have a VCN, skip to the next task.

Tip:
When you use the Console to create a VCN, you can create only the VCN, or you can create the VCN with several related resources. This task creates only the VCN, and the subsequent tasks create the other required resources.
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.

3. Click Create Virtual Cloud Network.

4. Enter the following values:
   - **Name**: A descriptive name for the cloud network. It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **CIDR Block**: A single, contiguous CIDR block for the cloud network (for example, 172.16.0.0/16). You can’t change this value later. See Allowed VCN Size and Address Ranges on page 2750. For reference, use a CIDR calculator.
   - **Enable IPv6 Address Assignment**: This option is available only if the VCN is in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

5. You can provide values for the rest of the options, or you can ignore them:
   - **DNS Resolution**: Required for assignment of DNS hostnames to hosts in the VCN, and required if you plan to use the VCN's default DNS feature (called the Internet and VCN Resolver). If the check box is selected, you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding DNS Domain Name for the VCN (VCN DNS label). For more information, see DNS in Your Virtual Cloud Network on page 2910.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. Click Create Virtual Cloud Network.

The VCN is created and displayed on the page. Ensure that it's done being provisioned before continuing.
Task 2b: Create the DRG

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Dynamic Routing Gateways.
2. Click Create Dynamic Routing Gateway.
3. Enter the following values:
   - **Create in Compartment**: Leave as is (the VCN's compartment).
   - **Name**: A descriptive name for the DRG. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Tags**: Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.
4. Click Create Dynamic Routing Gateway.

The DRG is created and displayed on the page. Ensure that it's done being provisioned before continuing.

Tip:

You could also use this DRG as the gateway for Oracle Cloud Infrastructure FastConnect, which is an alternative way to connect your on-premises network to your VCN.

Task 2c: Attach the DRG to the VCN

1. Click the name of the DRG you created.
2. Under Resources, click Virtual Cloud Networks.
3. Click Attach to Virtual Cloud Network.
4. Select the VCN. Ignore the section for advanced options, which is only for an advanced routing scenario called transit routing, which is not relevant here.

5. Click Attach.

The attachment is in the Attaching state for a short period before it's ready.

Task 2d: Create a route table and route rule for the DRG

Although the VCN comes with a default route table (without any rules), in this task you create a custom route table with a route rule for the DRG. In this example, your on-premises network is 10.0.0.0/16. You create a route rule that takes any traffic destined for 10.0.0.0/16 and routes it to the DRG. When you create a subnet in task 2f, you associate this custom route table with the subnet.

If you already have an existing VCN with a subnet, you don’t need to create a route table or subnet. Instead you can update the existing subnet’s route table to include the route rule for the DRG.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click your VCN.
3. Click Route Tables to see your VCN's route tables.
4. Click Create Route Table.
5. Enter the following values:
   - Name: A descriptive name for the route table (for example, MyExampleRouteTable). The name doesn’t have to be unique, and it can’t be changed later in the Console (but you can change it in the API). Avoid entering confidential information.
   - Create in compartment: Leave as is.
   - Click + Additional Route Rule, and enter the following:
     - Target Type: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
     - Destination CIDR Block: The CIDR for your on-premises network (10.0.0.0/16 in this example).
     - Description: An optional description of the rule.
     - Tags: Leave the tag information as is.
6. Click Create Route Table.

The route table is created and displayed on the page. However, the route table doesn't do anything unless you associate it with a subnet during subnet creation (see task 2f).
Task 2e: Create a security list

By default, incoming traffic to the instances in your VCN is set to DENY on all ports and all protocols. In this task, you set up two ingress rules and one egress rule to allow basic required network traffic. Your VCN comes with a default security list with a set of default rules. However, in this task you create a separate security list with a more restrictive set of rules focused on traffic with your on-premises network. When you create a subnet in task 2f, you associate this security list with the subnet.

Tip:

Security lists are one way to control traffic in and out of the VCN's resources. You can also use network security groups, which let you apply a set of security rules to a set of resources that all have the same security posture.

Important:

In the following procedure, ensure that the on-premises CIDR that you specify in the security list rules is the same (or smaller) than the CIDR that you specified in the route rule in the preceding task. Otherwise, traffic will be blocked by the security lists.

1. While still viewing your VCN, click Security Lists on the left side of the page.
2. Click Create Security List.
3. Enter the following values:
   - Name: A descriptive name for the security list. The name doesn't have to be unique, and it cannot be changed later in the Console (but you can change it in the API). Avoid entering confidential information.
   - Create in compartment: Leave as is.
4. In the Allow Rules for Ingress section, click Add Ingress Rule and enter the following values for the ingress rule, which allows incoming SSH on TCP port 22 from your on-premises network:
   - Source Type: CIDR
   - Source CIDR: The CIDR for your on-premises network (10.0.0.0/16 in this example)
   - IP Protocol: TCP.
   - Source Port Range: Leave as is (the default All).
   - Destination Port Range: 22 (for SSH traffic).
   - Description: An optional description of the rule.

5. In the Allow Rules for Egress section, click Add Egress Rule enter the following values for the egress rule, which allows outgoing TCP traffic on all ports to your on-premises network:
   - Destination Type: CIDR
   - Destination CIDR: The CIDR for your on-premises network (10.0.0.0/16 in this example).
   - IP Protocol: TCP.
   - Source Port Range: Leave as is (the default All).
   - Destination Port Range: Leave as is (the default All).
   - Description: An optional description of the rule.

6. Leave the tag information as is.

7. Click Create Security List.

The security list is created and displayed on the page. However, the security list doesn't do anything unless you associate it with a subnet during subnet creation (see task 2f).

**Task 2f: Create a subnet**

In this task, you create a subnet in the VCN. Typically a subnet has a CIDR block smaller than the VCN's CIDR. Any instances that you create in this subnet have access to your on-premises network. Oracle recommends using regional subnets. Here you create a regional private subnet.

1. While still viewing your VCN, click Subnets on the left side of the page.
2. Click Create Subnet.
3. Enter the following values:

- **Name**: A descriptive name for the subnet. It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
- **Regional or AD-specific subnet**: Select the radio button for **Regional**. Oracle recommends using regional subnets.
- **CIDR Block**: A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). It must be within the cloud network's CIDR block and can't overlap with any other subnets. You can't change this value later. See [Allowed VCN Size and Address Ranges](#) on page 2750. For reference, use a CIDR calculator.
- **Enable IPv6 Address Assignment**: This option is available only if the VCN is in the US Government Cloud. For more information, see [IPv6 Addresses](#) on page 2889.
- **Route Table**: The route table that you created earlier.
- **Private Subnet**: Select this option. For more information, see [Access to the Internet](#) on page 2752.
- **Use DNS Hostnames in this Subnet**: Leave as is (selected).
- **DHCP Options**: The set of DHCP options to associate with the subnet. Select the default set of DHCP options for the VCN.
- **Security Lists**: The security list that you created earlier.
- **Tags**: Leave as is. You can add tags later if you want. For more information, see [Resource Tags](#) on page 211.

4. Click **Create Subnet**.

The subnet is created and displayed on the page. The basic VCN in this example is now set up, and you're ready to create the remaining components for the IPSec VPN.

**Task 2g: Create a CPE object and provide your CPE device's public IP address**

In this task, you create the CPE object, which is a virtual representation of your CPE device.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Customer-Premises Equipment**.
2. Click **Create Customer-Premises Equipment**.
3. Enter the following values:
   - **Create in Compartment**: Leave as is (the VCN's compartment).
   - **Name**: A descriptive name for the CPE object. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **IP Address**: The public IP address of the CPE device at your end of the VPN (see the list of information to gather in [Before You Get Started](#) on page 2949).
   - **Tags**: Leave as is. You can add tags later if you want. For more information, see [Resource Tags](#) on page 211.
4. Click **Create**.

The CPE object is created and displayed on the page.
Task 2h: Create an IPSec connection to the CPE object

In this task, you create the IPSec tunnels and configure the type of routing for them (BGP dynamic routing or static routing).

**Tip:**

If you have an existing Oracle IPSec VPN that uses static routing, you can change the tunnels to instead use BGP dynamic routing.

For BGP dynamic routing

In this example, you configure both tunnels to use BGP dynamic routing.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.
2. Click Create IPSec Connection.
3. Enter the following values:
   - **Create in Compartment:** Leave as is (the VCN's compartment).
   - **Name:** Enter a descriptive name for the IPSec connection. It doesn’t have to be unique, and you can change it later. Avoid entering confidential information.
   - **Customer-Premises Equipment Compartment:** Leave as is (the VCN's compartment).
   - **Customer-Premises Equipment:** Select the CPE object that you created earlier.
   - **Dynamic Routing Gateway Compartment:** Leave as is (the VCN's compartment).
   - **Dynamic Routing Gateway:** Select the DRG that you created earlier.
   - **Static Route CIDR:** Leave empty because this IPSec connection uses BGP dynamic routing. You configure the two tunnels to use BGP in subsequent steps.
4. Click Show Advanced Options.
5. On the **CPE IKE Identifier** tab (optional): Oracle defaults to using the public IP address of the CPE. But if your CPE is behind a NAT device, you might need to enter a different value. You can either enter the new value here, or change the value later.

6. On the **Tunnel 1** tab (required):
   - **Name**: Enter a descriptive name for the tunnel. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - **Provide custom shared secret** (optional): By default, Oracle provides the shared secret for the tunnel. If you want to provide it instead, select this check box and enter the shared secret. You can change the shared secret later.
   - **IKE Version**: The Internet Key Exchange (IKE) version to use for this tunnel. Only select IKEv2 if your CPE supports it. You must also then configure the CPE to use only IKEv2 for this tunnel.
   - **Routing Type**: Select the radio button for **BGP Dynamic Routing**.
   - **BGP ASN**: Enter your network's ASN.
   - **Inside Tunnel Interface - CPE**: Enter the BGP IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel. For example: 10.0.0.16/31. The IP address must be part of the IPSec VPN's encryption domain.
   - **Inside Tunnel Interface - Oracle**: Enter the BGP IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel. For example: 10.0.0.17/31. The IP address must be part of the IPSec VPN's encryption domain.

7. On the **Tunnel 2** tab (required):
   - **Name**: Enter a descriptive name for the tunnel. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - **Provide custom shared secret** (optional): By default, Oracle provides the shared secret for the tunnel. If you want to provide it instead, select this check box and enter the shared secret. You can change the shared secret later.
   - **IKE Version**: The Internet Key Exchange (IKE) version to use for this tunnel. Only select IKEv2 if your CPE supports it. You must also then configure the CPE to use only IKEv2 for this tunnel.
   - **Routing Type**: Select the radio button for **BGP Dynamic Routing**.
   - **BGP ASN**: Enter your network's ASN.
   - **Inside Tunnel Interface - CPE**: Enter the BGP IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel. Use a different IP address than for tunnel 1. For example: 10.0.0.18/31. The IP address must be part of the IPSec VPN's encryption domain.
   - **Inside Tunnel Interface - Oracle**: Enter the BGP IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel. Use a different IP address than for tunnel 1. For example: 10.0.0.19/31. The IP address must be part of the IPSec VPN's encryption domain.

8. On the **Tags** tab (optional): Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.

9. Click **Create IPSec Connection**.
   
   The IPSec connection is created and displayed on the page. It will be in the Provisioning state for a short period.

   The displayed tunnel information includes:
   - The Oracle VPN IP address (for the Oracle VPN headend).
   - The tunnel's IPSec status (possible values are Up, Down, and Down for Maintenance). At this point, the status is Down. Your network engineer still must configure your CPE device.
   - The tunnel's BGP status. At this point, the status is Down. Your network engineer still must configure your CPE device.

   To view the tunnel's shared secret, click the tunnel to view its details, and then click **Show** next to **Shared Secret**.

10. Copy the Oracle VPN IP address and shared secret for each of the tunnels to an email or other location so you can deliver it to the network engineer who will configure your CPE device.

    You can view this tunnel information here in the Console at any time.
You have now created all the components required for the IPSec VPN. But your network engineer must configure your CPE device before network traffic can flow between your on-premises network and VCN.

For static routing

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.
2. Click Create IPSec Connection.
3. Enter the following values:
   - Create in Compartment: Leave as is (the VCN's compartment).
   - Name: Enter a descriptive name for the IPSec connection. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - Customer-Premises Equipment Compartment: Leave as is (the VCN's compartment).
   - Customer-Premises Equipment: Select the CPE object that you created earlier.
   - Dynamic Routing Gateway Compartment: Leave as is (the VCN's compartment).
   - Dynamic Routing Gateway: Select the DRG that you created earlier.
   - Static Route CIDR: Enter at least one static route CIDR (see the list of information to gather in Before You Get Started on page 2949). For this example, enter 10.0.0.0/16. You can enter up to 10 static routes, and you can change the static routes later.
4. Click Show Advanced Options.
5. On the CPE IKE Identifier tab (optional): Oracle defaults to using the public IP address of the CPE. But if your CPE is behind a NAT device, you might need to enter a different value. You can either enter the new value here, or change the value later.
6. On the **Tunnel 1** tab (optional):

   - **Tunnel Name**: Enter a descriptive name for the tunnel. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - **Provide custom shared secret** (optional): By default, Oracle provides the shared secret for the tunnel. If you want to provide it instead, select this check box and enter the shared secret. You can change the shared secret later.
   - **IKE Version**: The Internet Key Exchange (IKE) version to use for this tunnel. Only select IKEv2 if your CPE supports it. You must also then configure the CPE to use only IKEv2 for this tunnel.
   - **Routing Type**: Leave the radio button for *Static Routing* selected.
   - **Inside Tunnel Interface - CPE** (optional): You can provide an IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel for the purposes of tunnel troubleshooting or monitoring. For example: 10.0.0.16/31. The IP address must be part of the IPSec VPN's encryption domain.
   - **Inside Tunnel Interface - Oracle** (optional): You can provide an IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel for the purposes of tunnel troubleshooting or monitoring. For example: 10.0.0.17/31. The IP address must be part of the IPSec VPN's encryption domain.

7. On the **Tunnel 2** tab (optional):

   - **Tunnel Name**: Enter a descriptive name for the tunnel. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - **Provide custom shared secret** (optional): By default, Oracle provides the shared secret for the tunnel. If you want to provide it instead, select this check box and enter the shared secret. You can change the shared secret later.
   - **IKE Version**: The Internet Key Exchange (IKE) version to use for this tunnel. Only select IKEv2 if your CPE supports it. You must also then configure the CPE to use only IKEv2 for this tunnel.
   - **Routing Type**: Leave the radio button for *Static Routing* selected.
   - **Inside Tunnel Interface - CPE** (optional): You can provide an IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel for the purposes of tunnel troubleshooting or monitoring. Use a different IP address than for tunnel 1. For example: 10.0.0.18/31. The IP address must be part of the IPSec VPN's encryption domain.
   - **Inside Tunnel Interface - Oracle** (optional): You can provide an IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel for the purposes of tunnel troubleshooting or monitoring. Use a different IP address than for tunnel 1. For example: 10.0.0.19/31. The IP address must be part of the IPSec VPN's encryption domain.

8. **Tags**: Leave as is. You can add tags later if you want. For more information, see *Resource Tags* on page 211.

9. Click **Create IPSec Connection**.

   The IPSec connection is created and displayed on the page. It will be in the Provisioning state for a short period.

   The displayed tunnel information includes:

   - The Oracle VPN IP address (for the Oracle VPN headend).
   - The tunnel's IPSec status (possible values are Up, Down, and Down for Maintenance). At this point, the status is Down. Your network engineer still must configure your CPE device.

   To view the tunnel's shared secret, click the tunnel to view its details, and then click **Show** next to **Shared Secret**.

10. Copy the Oracle VPN IP address and shared secret for each of the tunnels to an email or other location so you can deliver it to the network engineer who will configure the CPE device.

   You can view this tunnel information here in the Console at any time.

   You have now created all the components required for the IPSec VPN. But your network engineer must configure the CPE device before network traffic can flow between your on-premises network and VCN.

   For more information, see *CPE Configuration* on page 2967.

For policy-based routing

   Set up **VPN Connect with policy-based routing**.
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

2. Click Create IPSec Connection.

3. Enter the following values:
   - Create in Compartment: Leave as is (the VCN's compartment).
   - Name: Enter a descriptive name for the IPSec connection. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - Customer-Premises Equipment Compartment: Leave as is (the VCN's compartment).
   - Dynamic Routing Gateway Compartment: Leave as is (the VCN's compartment).
   - Static Route CIDR: Enter at least one static route CIDR (see the list of information to gather in Before You Get Started on page 2949). For this example, enter 10.0.0.0/16. You can enter up to 10 static routes, and you can change the static routes later.

4. Click Show Advanced Options.

5. On the CPE IKE Identifier tab (optional): Oracle defaults to using the public IP address of the CPE. But if your CPE is behind a NAT device, you might need to enter a different value. You can either enter the new value here, or change the value later.

6. On the Tunnel 1 tab (optional):
   - Tunnel Name: Enter a descriptive name for the tunnel. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
   - Provide custom shared secret (optional): By default, Oracle provides the shared secret for the tunnel. If you want to provide it instead, select this check box and enter the shared secret. You can change the shared secret later.
   - IKE Version: The Internet Key Exchange (IKE) version to use for this tunnel. Only select IKEv2 if your CPE supports it. You must also then configure the CPE to use only IKEv2 for this tunnel.
   - Routing Type: Select the radio button for Policy-based routing.
   - On-premises: You can provide multiple IPv4 or IPv6 CIDR blocks used by resources in your on-premises network, with routing determined by the CPE device policies.

   Note:

   See Encryption domains for policy-based tunnels on page 2948 for limitations on how many IPv4 or IPv6 CIDR blocks can be used.

   - Oracle Cloud: You can provide multiple IPv4 or IPv6 CIDR blocks used by resources in your VCN.

   Note:

   See Encryption domains for policy-based tunnels on page 2948 for limitations on how many IPv4 or IPv6 CIDR blocks can be used.

   - Inside Tunnel Interface - CPE (optional): You can provide an IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel for the purposes of tunnel troubleshooting or monitoring. For example: 10.0.0.16/31. The IP address must be part of one of the IPSec VPN's encryption domains.

   - Inside Tunnel Interface - Oracle (optional): You can provide an IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel for the purposes of tunnel troubleshooting or monitoring. For example: 10.0.0.17/31. The IP address must be part of one of the IPSec VPN's encryption domains.
7. On the **Tunnel 2** tab (optional):

- **Tunnel Name:** Enter a descriptive name for the tunnel. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.
- **Provide custom shared secret** (optional): By default, Oracle provides the shared secret for the tunnel. If you want to provide it instead, select this check box and enter the shared secret. You can change the shared secret later.
- **IKE Version:** The Internet Key Exchange (IKE) version to use for this tunnel. Only select IKEv2 if your CPE supports it. You must also then configure the CPE to use only IKEv2 for this tunnel.
- **Routing Type:** Select the radio button for **Policy-based** routing.
- **On-premises:** You can provide multiple IPv4 or IPv6 CIDR blocks used by resources in your on-premises network, with routing determined by the CPE device policies.
  
  **Note:** See Encryption domains for policy-based tunnels on page 2948 for limitations.

- **Oracle Cloud:** You can provide multiple IPv4 or IPv6 CIDR blocks used by resources in your VCN.
  
  **Note:** See Encryption domains for policy-based tunnels on page 2948 for limitations.

- **Inside Tunnel Interface - CPE** (optional): You can provide an IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel for the purposes of tunnel troubleshooting or monitoring. For example: 10.0.0.16/31. The IP address must be part of one of the IPSec VPN's encryption domains.
- **Inside Tunnel Interface - Oracle** (optional): You can provide an IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel for the purposes of tunnel troubleshooting or monitoring. For example: 10.0.0.17/31. The IP address must be part of one of the IPSec VPN's encryption domains.

8. **Tags:** Leave as is. You can add tags later if you want. For more information, see Resource Tags on page 211.

9. **Click Create IPSec Connection.**

   The IPSec connection is created and displayed on the page. It will be in the Provisioning state for a short period.

   The displayed tunnel information includes:

   - The Oracle VPN IP address (for the Oracle VPN headend).
   - The tunnel's IPSec status (possible values are Up, Down, and Down for Maintenance). At this point, the status is Down. Your network engineer still must configure your CPE device.

   To view the tunnel's shared secret, click the tunnel to view its details, and then click **Show** next to **Shared Secret**.

10. **Copy the Oracle VPN IP address and shared secret for each of the tunnels to an email or other location, then deliver it to the network engineer who configures the CPE device.**

   You can view this tunnel information here in the Console at any time.

   You have now created all the components required for the IPSec VPN. But your network engineer must configure the CPE device before network traffic can flow between your on-premises network and VCN.

   For more information, see CPE Configuration on page 2967.

**Task 3: Use the CPE Configuration Helper**

Use the CPE Configuration Helper to generate configuration content that your network engineer can use to configure the CPE.

The content includes these items:

- For each IPSec tunnel, the Oracle VPN IP address and shared secret.
- The supported IPSec parameter values.
- Information about the VCN.
- CPE-specific configuration information.
For more information, see Using the CPE Configuration Helper on page 2970.

**Task 4: Have your network engineer configure your CPE**

Provide your network engineer with the following items:

- The content generated by the CPE Configuration Helper.
- The general IPSec parameters that Oracle supports.

**Important:**
Be sure to have your network engineer configure your CPE device to support both of the tunnels in case one fails or Oracle takes one down for maintenance. If you're using BGP, see Routing for the Oracle IPSec VPN on page 2934.

**Task 5: Validate connectivity**

After the network engineer configures your CPE device, you can confirm that the tunnel's IPSec status is Up and green. Next, you can create a Linux instance in the subnet in your VCN. You should then be able to use SSH to connect to the instance's private IP address from a host in your on-premises network. For more information, see Creating an Instance on page 695.

**Example Layout with Multiple Geographic Areas**

The following diagram shows an example with this configuration:

- Two networks in separate geographical areas that each connect to your VCN
- A single CPE device in each area
- Two IPSec VPNs (one for each CPE device)

Notice that each IPSec VPN has two routes associated with it: one for the particular geographical area's subnet, and a default 0.0.0.0/0 route. Oracle learns about the available routes for each tunnel either through BGP (if the tunnels use BGP), or because you've set them as static routes for the IPSec connection (if the tunnels use static routing).
Following are some examples of situations in which the 0.0.0.0/0 route can provide flexibility:

- Assume that the CPE 1 device goes down (see the next diagram). If Subnet 1 and Subnet 2 can communicate with each other, your VCN could still reach the systems in Subnet 1 because of the 0.0.0.0/0 route that goes to CPE 2.

- Assume that your organization adds a new geographical area with Subnet 3 and initially just connects it to Subnet 2 (see the next diagram). If you added a route rule to your VCN’s route table for Subnet 3, the VCN could reach systems in Subnet 3 because of the 0.0.0.0/0 route that goes to CPE 2.

**Example Layout with PAT**

The following diagram shows an example with this configuration:

- Two networks in separate geographical areas that each connect to your VCN
- Redundant CPE devices (two in each geographical area)
- Four IPSec VPNs (one for each CPE device)
- Port address translation (PAT) for each CPE device

For each of the four connections, the route that Oracle needs to know about is the PAT IP address for the specific CPE device. Oracle learns about the PAT IP address route for each tunnel either through BGP (if the tunnels use
BGP), or because you've set the relevant address as a static route for the IPSec connection (if the tunnels use static routing).

When you set up the route rules for the VCN, you specify a rule for each PAT IP address (or an aggregate CIDR that covers them all) with your DRG as the rule's target.

**What's Next?**

See these related topics and procedures:

- [VPN Connect Quickstart](#) on page 2939
- [CPE Configuration](#) on page 2967
- [Verified CPE Devices](#) on page 2969
- [Using the CPE Configuration Helper](#) on page 2970
- [Changing from Static Routing to BGP Dynamic Routing](#) on page 3160
- [Working with VPN Connect](#) on page 3156
- [VPN Connect FAQ](#)
- [Using the API for VPN Connect](#) on page 3163
- [VPN Connect Metrics](#) on page 3164
- [VPN Connect Troubleshooting](#) on page 3166

**CPE Configuration**

This topic is for network engineers. It explains how to configure the on-premises device (the customer-premises equipment, or CPE) at your end of the IPSec VPN so traffic can flow between your on-premises network and virtual cloud network (VCN). See these related topics:

- [Networking](#) on page 2746: For general information about the parts of a VCN
- [VPN Connect](#) on page 2932: For various topics about IPSec VPNs
- [Verified CPE Devices](#) on page 2969: For a list of CPE devices Oracle has verified
The following figure shows the basic layout of the IPSec VPN connection.

Requirements and Prerequisites
There are several requirements and prerequisites to be aware of before moving forward.

Routing Considerations
For important details about routing for your IPSec VPN see Routing for the Oracle IPSec VPN on page 2934.

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec VPN connection. Even if you configure one tunnel as primary and another as backup, traffic from your VCN to your on-premises network can use any tunnel that is "up" on your device. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

If you use BGP dynamic routing with your IPSec VPN, you can configure routing so that Oracle prefers one tunnel over the other.

Note that the Cisco ASA policy-based configuration uses a single tunnel.

Creation of Cloud Network Components
You or someone in your organization must have already used the Oracle Console to create a VCN and an IPSec connection, which consists of multiple IPSec tunnels for redundancy. You must gather the following information about those components:

- VCN OCID: The VCN OCID is a unique Oracle Cloud Infrastructure identifier that has a UUID at the end. You can use this UUID or any other string that helps you identify this VCN in the device configuration and doesn't conflict with other object-group or access-list names.
- VCN CIDR
- VCN CIDR subnet mask
- For each IPSec tunnel:
  - The IP address of the Oracle IPSec tunnel endpoint (the VPN headend)
  - The shared secret

Information About Your CPE Device
You also need some basic information about the inside and outside interfaces of your on-premises device (your CPE). For a list of the required information for your particular CPE, see the links in this list: Verified CPE Devices on page 2969.

Oracle recommends that you disable NAT-T at your CPE when establishing IPSec tunnels with Oracle Cloud Infrastructure. Unless you have multiple CPEs sharing the same NAT IP, NAT-T is not required.

If your CPE is behind a NAT device, you can provide Oracle with your CPE's IKE identifier. For more information, see Overview of the IPSec VPN Components on page 2936.
Route-Based Versus Policy-Based IPSec

The Oracle VPN headends use route-based tunnels, but can work with policy-based tunnels with some caveats. See Encryption domains for policy-based tunnels on page 2948 for full details.

IPSec VPN Best Practices

- **Configure all tunnels for every IPSec connection:** Oracle deploys multiple IPSec headends for all your connections to provide high availability for your mission-critical workloads. Configuring all the available tunnels is a key part of the "Design for Failure" philosophy. (Exception: Cisco ASA policy-based configuration, which uses a single tunnel.)

- **Have redundant CPEs in your on-premises locations:** Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant CPE devices. You add each CPE to the Oracle Cloud Infrastructure Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. Oracle may use any tunnel that is "up" to send traffic back to your on-premises network. For more information, see Routing for the Oracle IPSec VPN on page 2934.

- **Consider backup aggregate routes:** If you have multiple sites connected via IPSec VPNs to Oracle Cloud Infrastructure, and those sites are connected to your on-premises backbone routers, consider configuring your IPSec connection routes with both the local site aggregate route as well as a default route.

  Note that the DRG routes learned from the IPSec connections are only used by traffic you route from your VCN to your DRG. The default route will only be used by traffic sent to your DRG whose destination IP address does not match the more specific routes of any of your tunnels.

Confirming the Status of the Connection

After you configure the IPSec connection, you can test the connection by launching an instance into the VCN and then pinging it from your on-premises network. For information about launching an instance, see Launching an Instance. To ping the instance, the VCN's security rules must allow ping traffic.

You can get the status of the IPSec tunnels in the API or Console. For instructions, see To view the status and configuration information for the IPSec tunnels on page 3157.

Device Configurations

For links to the specific configuration information for each verified CPE device, see Verified CPE Devices on page 2969.

Verified CPE Devices

The following devices or software have been verified for use with VPN Connect.

**Note:**

Oracle provides configuration instructions for the vendors and devices in the following table. Make sure to use the configuration instructions for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the following table, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Device</th>
<th>Minimum Software Version</th>
<th>Configuration</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Software Technologies</td>
<td>2200 or Open Server</td>
<td>R80.20</td>
<td>Check Point Configuration Options on page 2972</td>
<td>Video</td>
</tr>
<tr>
<td>Cisco Systems</td>
<td>ASA</td>
<td>9.7.1 (recommended)</td>
<td>Cisco ASA Configuration Options on page 3020</td>
<td>Video: Route-based</td>
</tr>
<tr>
<td>Cisco Systems</td>
<td>2921</td>
<td>IOS version 15.4(3)M3</td>
<td>Cisco IOS on page 3046</td>
<td>Video</td>
</tr>
<tr>
<td>Fortinet</td>
<td>FortiGate-VM</td>
<td>6.0.4</td>
<td>FortiGate on page 3058</td>
<td>Video</td>
</tr>
<tr>
<td>Furukawa Electric</td>
<td>FITELnet-F220/F221</td>
<td>01.00(00)[0][00.00.0]</td>
<td>Furukawa Electric on page 3072</td>
<td></td>
</tr>
<tr>
<td>Juniper Networks</td>
<td>MX 240</td>
<td>JunOS 15.1</td>
<td>Juniper MX on page 3076</td>
<td></td>
</tr>
<tr>
<td>Juniper Networks</td>
<td>SRX 240</td>
<td>JunOS 11.0</td>
<td>Juniper SRX on page 3089</td>
<td>Video</td>
</tr>
<tr>
<td>Libreswan</td>
<td></td>
<td>3.18</td>
<td>Libreswan on page 3102</td>
<td>Video</td>
</tr>
<tr>
<td>NEC</td>
<td>IX3315</td>
<td>10.2.16</td>
<td>NEC IX Series on page 3110</td>
<td></td>
</tr>
<tr>
<td>NEC</td>
<td>IX2106</td>
<td>10.2.16</td>
<td>NEC IX Series on page 3110</td>
<td></td>
</tr>
<tr>
<td>Palo Alto Networks</td>
<td>PA-500</td>
<td>PanOS version 8.0.0</td>
<td>Palo Alto on page 3120</td>
<td>Video</td>
</tr>
<tr>
<td>WatchGuard Technologies</td>
<td>Firebox</td>
<td>Fireware v12</td>
<td>WatchGuard on page 3153</td>
<td></td>
</tr>
<tr>
<td>Yamaha</td>
<td>RTX1210</td>
<td>Firmware Rev.14.01.28</td>
<td>Yamaha RTX Series on page 3153</td>
<td></td>
</tr>
<tr>
<td>Yamaha</td>
<td>RTX830</td>
<td>Firmware Rev.15.02.03</td>
<td>Yamaha RTX Series on page 3153</td>
<td></td>
</tr>
</tbody>
</table>

**Using the CPE Configuration Helper**

After you set up VPN Connect, your network engineer must configure the customer-premises equipment (CPE) at your end of the connection (for example, a router). The configuration includes details about your virtual cloud network (VCN) and the IPSec tunnels in the VPN Connect. This topic describes how to use the CPE Configuration Helper in the Oracle Console to generate information that a network engineer uses to configure the CPE. Notice that the CPE Configuration Helper is also referred to as the Helper.

**Overview of the Helper**

For the IPSec tunnels in a VPN Connect to work, your network engineer must configure your CPE with specific information. The information comes from different sources. Oracle provides some of it in several places within the Oracle Console. The Helper collects the necessary information in one place and then organizes it to make CPE configuration easier for the network engineer. You can copy or download the resulting content to a file.
The configuration information that the network engineer needs depends on which vendor makes the CPE. To ensure that the Helper can produce vendor-specific content, you specify which vendor makes your CPE. See the one-time prerequisite in Using the Helper on page 2971.

In some cases, the Helper might ask for information about your network and include it in the content. If you don't know the answers, you can leave them blank. The resulting content then uses placeholder variables to show where the network engineer needs to provide the answers.

The content that the Helper produces includes these items:

- The Oracle VPN headend for the tunnel (the IP address at the Oracle end)
- The shared secret (pre-shared key) for the tunnel
- Your VCN's CIDR
- BGP information (if you're using BGP dynamic routing for the tunnel)
- The IPSec parameters that Oracle supports
- Other relevant information

**Using the Helper**

One-time prerequisite: Specify the CPE vendor

Edit the CPE and select the vendor. If you're not sure which vendor makes your CPE, or it's not in the list, select Other.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Customer-Premises Equipment.
2. Select the CPE you're interested in, and then click Edit.
3. For Vendor, select your CPE vendor from the list. If you're not sure which vendor makes your CPE, or it's not in the list, select Other.
4. If prompted, select a value for Platform/Version. Here are guidelines:
   - Oracle recommends using a route-based configuration if possible.
   - If you do not see your specific CPE platform or version in the list, choose the closest platform/version that predates your CPE version.
5. Click Save Changes.

Open the Helper from one of three locations

You can access the Helper from three different locations in the Oracle Console. Where you access the Helper controls the scope of the content it produces:

- **The CPE page:** The Helper produces content for all IPSec connections that terminate on the CPE. Notice that there could be IPSec connections in compartments that you do not have access to. If you don't have permission to view a particular IPSec connection, it is not included in the content.
- **An IPSec connection page:** The Helper produces content for one individual IPSec connection (all tunnels within the connection).
- **A tunnel's page:** The Helper produces content for one tunnel in an IPSec connection.

1. Under Core Infrastructure, go to Networking and navigate to the resource page you're interested in:
   - The CPE page
   - The IPSec connection page
   - The tunnel page
2. Click Open CPE Configuration Helper.

   The Helper opens on the right side of the page.

   It shows basic information such as the CPE's public IP address and vendor.

Generate the content

The Helper has a Create Content button at the bottom. After you click it and the content is produced, there are buttons to copy or download the content to a file. Give the content to your network engineer, along with the link to
the configuration topic for your CPE type (see Verified CPE Devices on page 2969). You can return to the Helper at any time and again generate the configuration content.

**Tip:**

For certain CPE vendors, the Helper displays fields for vendor-specific information that is used for CPE configuration. The fields might be blank or already have values. You can fill in the blank fields or leave them as is. For blank fields, the resulting content displays placeholder variables to show where the network engineer needs to fill in the values.

**Instructions:**

1. Review the template of information in the Helper. Optionally fill in any blank fields.
2. Click **Create Content** at the bottom of the Helper.
   
   The Helper generates the content.

   **Note:**
   
   See this known issue if you instead see an error that says *The CPE is missing the vendor information (the device type). Update the CPE and add the vendor information.*

3. Click either **Copy Configuration to Clipboard** or **Download Configuration** (to download it to a file).
4. Click **Close**.
5. Give the following items to your network engineer:
   - A link to the configuration topic for your CPE type. See Verified CPE Devices on page 2969.
   - The Helper content that you generated.

**If You Update Your VPN Connect**

You could change aspects of your VPN Connect, and after you do, you might want to generate the Helper content again. For example, imagine that you have an IPSec connection that uses static routing, and you decide to change it to use BGP dynamic routing. After updating the Oracle Console with the new routing information, you can generate the Helper content again for the IPSec connection. You can then give that new content to your network engineer to configure the CPE accordingly.

**Related Topics**

- VPN Connect Overview on page 2933
- VPN Connect Quickstart on page 2939
- Setting Up VPN Connect on page 2949
- Supported IPSec Parameters on page 2945
- CPE Configuration on page 2967
- Verified CPE Devices on page 2969
- Working with VPN Connect on page 3156
- VPN Connect FAQ
- Using the API for VPN Connect on page 3163

**Check Point Configuration Options**

Choose the configuration that suits your situation:

- Check Point: Route-Based on page 2972
- Check Point: Policy-Based on page 2997

**Check Point: Route-Based**

This topic provides a route-based configuration for Check Point CloudGuard. The instructions were validated with Check Point CloudGuard version R80.20.
Networking

This topic is for route-based (VTI-based) configuration. If you instead want policy-based configuration, see Check Point: Policy-Based on page 2997.

Check Point experience is required. This topic does not include how to add Check Point CloudGuard Security Gateway to Check Point CloudGuard Security Manager. For more information about using Check Point products, see the Check Point documentation.

**Important:**

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are for example purposes only.

![Diagram of a basic IPSec connection to Oracle Cloud Infrastructure](image)

**Best Practices**

This section covers general best practices and considerations for using VPN Connect.

**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).
Networking

Routing Protocol Considerations

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing:** The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
- **Static routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

Other Important CPE Configurations

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

**Note:**

Other vendors or industry documentation might use the term *proxy ID, security parameter index (SPI), or traffic selector* when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels:** Also called *next-hop-based tunnels*. A route table lookup is performed on a packet's destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.
• **Policy-based tunnels**: The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address**: Any (0.0.0.0/0)
- **Destination IP address**: Any (0.0.0.0/0)
- **Protocol**: IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

**Important:**

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
Networking

- An encryption domain must always be between two CIDR blocks of the same IP version.

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's private IP address, as shown in the following diagram.

![Diagram showing CPE configuration behind a NAT device](image)

**Note:**

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see [Changing the CPE IKE Identifier That Oracle Uses](#) on page 3158.

**Supported IPSec Parameters**

For a vendor-neutral list of supported IPSec parameters for all regions, see [Supported IPSec Parameters](#) on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see [Required VPN Connect Parameters for Government Cloud](#) on page 152 and also [Oracle's BGP ASN](#) on page 154. For the United Kingdom Government Cloud, see [Oracle's BGP ASN](#) on page 171.

**CPE Configuration (Route-Based)**

**Important:**

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.
The following figure shows the basic layout of the IPSec connection.

![Diagram of IPSec connection]

**About Using IKEv2**

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

If you want to use IKEv2, there’s a variation on one of the tasks presented in the next section. Specifically, in task 4, when configuring encryption, select IKEv2 only for the encryption method.

**Configuration Process**

**Redundancy with BGP Over IPSec**

For redundancy, Oracle recommends using BGP over IPSec. By default, if you have two connections of the same type (for example, two IPSec VPNs that both use BGP), and you advertise the same routes across both connections, Oracle prefers the oldest established route when responding to requests or initiating connections. If you want to force routing to be symmetric, Oracle recommends using BGP and AS path prepending with your routes to influence which path Oracle uses when responding to and initiating connections. For more information, see Routing Details for Connections to Your On-Premises Network on page 2942.

The Oracle DRG uses /30 or /31 as subnets for configuring IP addresses on the interface tunnels. Remember that the IP address must be part of the IPSec VPN’s encryption domain and must be allowed in the firewall policy to reach the peer VPN through the interface tunnel. You might need to implement a static route through the tunnel interface for the peer IP address.

Oracle’s BGP ASN in commercial regions is 31898. If you’re configuring VPN Connect for the Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle’s BGP ASN on page 154.

For your side, you can use a private ASN. Private ASNs are in the range 64512–65534.

**Task 1: Install IPSec VPN on Check Point CloudGuard Security Gateway**

**Prerequisite:** Before starting, add Check Point CloudGuard Security Gateway to Check Point CloudGuard Security Manager. Also establish the Secure Internal Communication (SIC) so you can configure the IPSec tunnel by using the Check Point Smart Console. For instructions to add the Security Gateway to CloudGuard or to establish the SIC, see the Check Point documentation.
1. Install the IPSec VPN module. Oracle recommends that you also install the Monitoring module for traffic analysis.

2. Click OK to save your changes.

Task 2: Create the VTI interface from GAIA

In this task, you configure a VTI interface that passes traffic by using routing rules from the VTI interface to the newly created IPSec tunnel.

1. Log in to the GAIA portal using the Check Point CloudGuard Security Gateway public or private IP address.
2. On the GAIA portal, select the Advanced view.
3. Under Network Management, go to Network Interfaces.
4. Click **Add**, and then click **VPN Tunnel**.
5. Specify the following items:

- **VPN Tunnel ID:** A number that will be added to the VTI interface called vpnt*, where the asterisk is the VPN tunnel ID number specified. For VPN tunnel ID = 1, the interface is labeled vpnt1.
- **Peer:** The name of the interoperable device that you created earlier for the IPSec tunnel. In this case, the name is OCI-VPN_BGP1.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the name you specify here does not match the name of the interoperable device, traffic does not flow through the IPSec tunnel.</td>
</tr>
</tbody>
</table>

- **Numbered:** Select **Numbered** to create a numbered interface.
- **Local Address:** The local IP address that was specified in the Oracle Console as the **Inside Tunnel Interface - CPE.**
- **Remote Address:** The remote IP address that was specified in the Oracle Console as the **Inside Tunnel Interface - Oracle.**

6. Click **OK.**

7. Under **Network Management,** go to **IPv4 Static Routes.**

8. Specify the following items:

- **Static route for the Oracle IP address:** Add an IP address with /32 mask for the remote IP address that was specified in the Oracle Console as the **Inside Tunnel Interface - Oracle.**
- **Static routes to the VCN subnets:** If you're using static routing for this IPSec connection to Oracle, add at least one subnet for the Oracle VCN to be reached through the IPSec tunnel. The following screenshot shows
Networking

a static route to 172.31.2.0/26. If you're using BGP for this IPSec connection to Oracle, skip this item because those routes are learned through BGP (see the next section).

Now all traffic with a specific destination learned from a static route will pass through the newly created IPSec tunnel.

9. Get the interfaces and verify that the VPN tunnel is in the list:
   a. In the Smart Console, go to **Gateways & Servers**.
   b. Select the **Check Point Security Gateways**, and double-click.
   c. Under **General Properties**, on the **Network Management** page, select **Get Interfaces**.

   The VPN tunnel interface should appear in the list.

10. To force a route-based VPN to take priority, create an empty group and assign it to the VPN domain:
   a. On the **VPN Domain** page, select **Manually defined**, and then select **Create empty group**.
   b. Click **New**, select **Group**, and then select **Simple Group**.
   c. Enter an **Object Name**, and then click **OK**. Do not assign any objects to this empty group.

---

Task 3: Create an interoperable device

Later, you will create a VPN Community. Before you can, you must create an **Interoperable Device** that will be used in Check Point CloudGuard Security Gateway to define the Oracle DRG.
1. Create the new interoperable device.
2. On the **General Properties** page of the new interoperable device, add a name to identify the IPSec tunnel. Enter the IP address that Oracle assigned for the Oracle end of the tunnel when creating the IPSec connection.

![Image of Interoperable Device - OCI-VPN_BGP1](image)

3. To force the route-based VPN to take priority, you must create an empty group and assign it to the VPN domain. To do that, on the **Topology** page, in the **VPN Domain** section, select **Manually defined**, and select the empty group.
4. On the **IPSec VPN** page, you can optionally add the new interoperable device to an existing VPN Community. You can skip this step if you don't yet have any VPN Communities created.

Notice that you skip the **Traditional mode configuration**, because you will define all the Phase 1 and Phase 2 parameters in the VPN Community in a later step. The VPN Community applies those parameters to all interoperable devices that belong to the VPN Community.
5. On the **Link Selection** page, under **Always use this IP address**, select **Main address**, which was the address you specified when creating the interoperable device. If necessary, you can use a specific IP address that will be used as the IKE ID.
6. On the VPN Advanced page, select **Use the community settings**, which applies all the options and values in the VPN Community, including the Phase 1 and Phase 2 parameters.

7. Click **OK** to save your changes.

Task 4: Create a VPN community

1. Go to **Security Policies**, and then from **Access Tools**, select **VPN Communities**.
2. Create a **Star Community**.

3. For the star community, add a name.
4. On the Gateways page, select the values for Center Gateways and Satellite Gateways. This star community acts as a settings template for the interoperable devices you specify in Center Gateways and Satellite Gateways.

- Center Gateways: For the Check Point CloudGuard Security Gateway.
- Satellite Gateways: For the CPE that connects to the Oracle DRG for each IPSec tunnel.
5. To allow traffic, go to **Global Properties**, and then **VPN**, and then **Advanced**.
6. Select the check box for **Enable VPN Directional Match in VPN Column**. Later you will create a security policy that uses a directional match condition to allow traffic to pass based on routing rules.

7. Click **OK**.
8. On the **Encryption** page, configure the Phase 1 and Phase 2 parameters that Oracle supports. For a list of those values, see [Supported IPSec Parameters](#) on page 2945.

If you're configuring VPN Connect for the Government Cloud, see [Required VPN Connect Parameters for Government Cloud](#) on page 152.

Notice that if you want to use IKEv2, for the **Encryption Method**, instead select **IKEv2 only**.
9. On the Tunnel Management page, select **Set Permanent Tunnels**. Oracle recommends that you:

- Select **On all tunnels in the community** to keep all the Oracle IPSec tunnels up all the time.
- In the **VPN Tunnel Sharing** section, select **One VPN tunnel per Gateway pair**.

The latter option generates only one pair of IPSec security associations (SAs), and each SA with only one security parameter index (SPI) (unidirectional).

When you use policy-based tunnels, every policy entry generates a pair of IPSec SAs, (also referred to as an encryption domain).

**Important:**

The Oracle VPN headend can support multiple encryption domains, but there are limitations. See Encryption domains for policy-based tunnels on page 2948 for full details.

Oracle creates a route-based IPSec connection, which means that everything is routed through an encryption domain that has 0.0.0.0/0 (any) for local traffic and 0.0.0.0/0 (any) for remote traffic. For more information, see Supported Encryption Domain or Proxy ID on page 2948.
10. On the Shared Secret page, select **Use only Shared Secret for all external members**, and add the shared secret that Oracle generated for the tunnel when creating the IPSec connection.

Currently Oracle supports only shared secret keys. Note that you can change the shared secret in the Oracle Console.

![Shared Secret page](image)

11. Click **OK** to save your changes.

Task 5: Create a security policy

1. Go to **Access Control**, and then the **Policy** tab. Create specific security policies by using **Directional Match Condition**, which allows traffic to pass based on routing tables. Set up the condition with these settings:
   - **Internal_Clear > VPN Community created**
   - **VPN Community created > VPN Community created**
   - **VPN Community created > Internal_Clear**

   In this case, the **VPN Community** is **OCI-DRG-BGP** and the **Internal_Clear** is predefined by Check Point.

![Policy tab](image)

2. Click **OK** to save your changes.
3. Click **Install Policy** to apply the configuration.

Task 1: Enable BGP

Perform the following steps for each tunnel.

1. Go to **Advanced Routing**, and then **BGP**.
2. Under BGP Global Settings, click Change Global Settings, and then add a router ID and local ASN.

3. Click Save.

Task 2: Redistribute routes into BGP

1. Go to Advanced Routing, and then Route Distribution.
2. Click **Add Redistribution From**, and then select **Interface**, which is for adding all connected subnets.

![Add Redistribution From Interface](image)

3. In the **Add Redistribution from Interface** dialog, configure the following items:
   - **To Protocol**: Select **BGP AS 31898**, which is the Oracle ASN for commercial regions. If you're configuring VPN Connect for the Government Cloud, see Oracle's **BGP ASN** on page 154.
   - **Interface**: Select **all** to advertise all connected subnets.

![Add Redistribution from Interface Configuration](image)

4. Click **Save**.
Networking

Now the BGP session should be up and advertising and receiving subnets.

**Verification**

The following CLI command verifies BGP peers and routing.

```
show bgp peers
```

The following command verifies that you're receiving BGP routes.

```
show route bgp
```

The following command verifies the routes that are being advertised. In this example, replace `<remote_IP_address>` with the remote IP address that was specified in the Oracle Console as the **Inside Tunnel Interface - Oracle**

```
show bgp peer <remote_IP_address> advertise
```

The following command verifies the routes that are being received.

```
show bgp peer <remote_IP_address> received
```

Use options 2 and 4 in the following command to verify security associations (SAs).

```
vpn tunnelutil

***********     Select Option     ***********

(1)   List all IKE SAs
(2)   * List all IPsec SAs
(3)   List all IKE SAs for a given peer (GW) or user (Client)
(4)   * List all IPsec SAs for a given peer (GW) or user (Client)
(5)   Delete all IPsec SAs for a given peer (GW)
(6)   Delete all IPsec SAs for a given User (Client)
(7)   Delete all IPsec+IKE SAs for a given peer (GW)
(8)   Delete all IPsec+IKE SAs for a given User (Client)
(9)   Delete all IPsec SAs for ALL peers and users
(0)   Delete all IPsec+IKE SAs for ALL peers and users

* To list data for a specific CoreXL instance, append "-i <instance number>" to your selection.

(Q)   Quit

******************************************************************************
```

A **Monitoring service** is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see **VPN Connect Metrics** on page 3164.

If you have issues, see **VPN Connect Troubleshooting** on page 3166.

**Check Point: Policy-Based**

This topic provides a policy-based configuration for Check Point CloudGuard. The instructions were validated with Check Point CloudGuard version R80.20.

This topic is for policy-based configuration. If you instead want route-based (VTI-based) configuration, see **Check Point: Route-Based** on page 2972.
Check Point experience is required. This topic does not include how to add Check Point CloudGuard Security Gateway to Check Point CloudGuard Security Manager. For more information about using Check Point products, see the Check Point documentation.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor. If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments. If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.</td>
</tr>
</tbody>
</table>

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are for example purposes only.

---

**Best Practices**

This section covers general best practices and considerations for using VPN Connect.

**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).
Routing Protocol Considerations

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.

- **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

Other Important CPE Configurations

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

**Note:**

Other vendors or industry documentation might use the term proxy ID, security parameter index (SPI), or traffic selector when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels**: Also called next-hop-based tunnels. A route table lookup is performed on a packet's destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.
• **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

**Encryption domain for route-based tunnels**

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

**Encryption domain for policy-based tunnels**

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an *encryption domain*.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

**Important:**

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
Networking

- An encryption domain must always be between two CIDR blocks of the same IP version.

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's private IP address, as shown in the following diagram.

Note:

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as cpe.example.com. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Supported IPSec Parameters

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

CPE Configuration (Policy-Based)

Important:

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.
Networking

The following figure shows the basic layout of the IPSec connection.

![IPSec Connection Diagram]

**About Using IKEv2**

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

If you want to use IKEv2, there’s a variation on one of the tasks presented in the next section. Specifically, in task 4, when configuring encryption, select **IKEv2 only** for the encryption method.

**Configuration Process**

Task 1: Install IPSec VPN on Check Point CloudGuard Security Gateway

**Prerequisite:** Before starting, add Check Point CloudGuard Security Gateway to Check Point CloudGuard Security Manager. Also establish the Secure Internal Communication (SIC) so you can configure the IPSec tunnel by using the Check Point Smart Console. For instructions to add the Security Gateway to CloudGuard or to establish the SIC, see the Check Point documentation.

![GPX Status Table]

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>IP</th>
<th>Version</th>
<th>Active Blades</th>
<th>Hardware</th>
<th>CPU Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>gw-manager</td>
<td>R30.20</td>
<td>🌐</td>
<td>🌐</td>
<td>Open server</td>
<td>🟢 🟢 🟢 🟢 4%</td>
</tr>
<tr>
<td>🟢</td>
<td>gw-security</td>
<td>130.51.111.77</td>
<td>R30.20</td>
<td>🌐</td>
<td>Open server</td>
<td>🟢 🟢 🟢 🟢 0%</td>
</tr>
</tbody>
</table>
1. Install the IPSec VPN module. Oracle recommends that you also install the Monitoring module for traffic analysis.

2. Click OK to save your changes.

Task 2: Configure IPSec settings for Check Point CloudGuard Security Gateway

This task covers the most important options used for an IPSec tunnel with Oracle Cloud Infrastructure.

1. On the Network Management page, import all the interfaces. You can do this by clicking Get Interfaces, which contains options for Get Interfaces With Topology and Get Interfaces Without Topology. This example uses
Get Interfaces Without Topology so that you can define the purpose of each interface as an external or internal network.

All of these interfaces will be used in the VPN Domain as subnets advertised by Check Point CloudGuard Security Gateway in the IPSec encryption domain.
2. On the **VPN Domain** page, Oracle recommends that you select the option **for All IP Addresses behind Gateway are based on Topology information**. This option adds all the subnets discovered in **Network Management** to the IPSec Encryption Domain.

You can instead select the option for **Manually defined**. However, that requires a **Network Object** with all subnets to include in the IPSec encryption domain.
3. If your Check Point CloudGuard Security Gateway uses 1:1 NAT to map private IP addresses to public IP addresses: On the Link Selection page, under Always use this IP address, select Statically NATed IP and specify the IP address that you want to use as your IKE ID.

If you don’t want to use a public IP address as the local IKE ID, you can use another value (such as a private IP address), but the value will not match the one expected on the Oracle DRG. To resolve this, you can change the value that Oracle uses in the Oracle Console (see the instructions that follow).

**To change the CPE IKE identifier that Oracle uses (Oracle Console)**

a. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

A list of the IPSec connections in the compartment that you’re viewing is displayed. If you don’t see the one you’re looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

b. For the IPSec connection you’re interested in, click the Actions icon (three dots), and then click Edit.

The current CPE IKE identifier that Oracle is using is displayed at the bottom of the dialog.

c. Enter your new values for CPE IKE Identifier Type and CPE IKE Identifier, and then click Save Changes.

4. Click OK to save your changes.

**Task 3: Create an interoperable device**

Later, you will create a VPN Community. Before you can, you must create an Interoperable Device that will be used in Check Point CloudGuard Security Gateway to define the Oracle DRG.
1. Create the new interoperable device.
2. On the **General Properties** page of the new interoperable device, add a name to identify the IPSec tunnel. Enter the IP address that Oracle assigned for the Oracle end of the tunnel when creating the IPSec connection.
3. On the **Topology** page, Oracle recommends that you create a new topology by clicking **New** and then adding the Oracle VCN subnets to be used for the tunnel.

You can instead select the option for **Manually defined**. However, that requires a **Network Object** with all subnets to include in the IPSec Encryption Domain.
4. On the **IPSec VPN** page, you can optionally add the new interoperable device to an existing VPN Community. You can skip this step if you don't yet have any VPN Communities created.

Notice that you skip the **Traditional mode configuration**, because you will define all the Phase 1 and Phase 2 parameters in the VPN Community in a later step. The VPN Community applies those parameters to all interoperable devices that belong to the VPN Community.
5. On the Link Selection page, under Always use this IP address, select Main address, which is the address that you specified when creating the interoperable device. If necessary, you can use a specific IP address that will be used as the IKE ID.
6. On the **VPN Advanced** page, select **Use the community settings**, which applies all the options and values in the VPN Community, including the Phase 1 and Phase 2 parameters.

7. Click **OK** to save your changes.

Task 4: Create a VPN community

1. Go to **Security Policies**, and then from **Access Tools**, select **VPN Communities**.
2. Create a **Star Community**.

3. For the star community, add a name.
4. On the **Gateways** page, select the values for **Center Gateways** and **Satellite Gateways**. This star community acts as a settings template for the interoperable devices you specify in **Center Gateways** and **Satellite Gateways**.

- **Center Gateways**: For the Check Point CloudGuard Security Gateway.
- **Satellite Gateways**: For the CPE that connects to the Oracle DRG for each IPSec tunnel.

5. If this is a proof of concept (POC) scenario: On the **Encrypted Traffic** page, select the check box for **Accept all encrypted traffic on**. The default value for this setting allows the traffic between both center and satellite gateways. This setting is appropriate for a POC scenario. However, for a production scenario, Oracle recommends
that you instead create specific security policies under **Access Control** and on the **Policy** tab. That is covered in the final task in this process.
6. On the **Encryption** page, configure the Phase 1 and Phase 2 parameters that Oracle supports. For a list of those values, see [Supported IPSec Parameters](#) on page 2945.

If you're configuring VPN Connect for the Government Cloud, see [Required VPN Connect Parameters for Government Cloud](#) on page 152.

Notice that if you want to use IKEv2, for the **Encryption Method**, instead select **IKEv2 only**.
7. On the **Tunnel Management** page, select **Set Permanent Tunnels**. Oracle recommends that you:

- Select **On all tunnels in the community** to keep all the Oracle IPSec tunnels up all the time.
- In the **VPN Tunnel Sharing** section, select **One VPN tunnel per Gateway pair**.

The latter option generates only one pair of IPSec security associations (SAs), and each SA with only one security parameter index (SPI) (unidirectional).

When you use policy-based tunnels, every policy entry generates a pair of IPSec SAs, (also referred to as an *encryption domain*).

**Important:**

The Oracle VPN headend can support multiple encryption domains, but there are limitations. See Encryption domains for policy-based tunnels on page 2948 for full details.

Oracle creates a route-based IPSec connection, which means that everything is routed through an encryption domain that has 0.0.0.0/0 (any) for local traffic and 0.0.0.0/0 (any) for remote traffic. For more information, see Supported Encryption Domain or Proxy ID on page 2948.
8. On the **Shared Secret** page, select **Use only Shared Secret for all external members**, and add the shared secret that Oracle generated for the tunnel when creating the IPSec connection.

Currently Oracle supports only shared secret keys. Note that you can change the shared secret in the Oracle Console.

9. Click **OK** to save your changes.

Task 5: Create a security policy (recommended for a production scenario)

If this is a proof of concept (POC) scenario, earlier you selected **Accept all encrypted traffic** on the **Encrypted Traffic** page. If this is instead a production scenario, Oracle recommends creating security policies.

1. Under Security Policies, click Access Control, and then select the Policy tab.
2. Configure the required values.

3. Click **OK** to save your changes.
4. Click **Install Policy** to apply the configuration.

The IPSec tunnel should now be up.

**Verification**

Use options 2 and 4 in the following command to verify security associations (SAs).

```bash
vpn tunnelutil

**********  Select Option  **********

(1)     List all IKE SAs
(2)     * List all IPsec SAs
```
Networking

(3) List all IKE SAs for a given peer (GW) or user (Client)
(4) * List all IPsec SAs for a given peer (GW) or user (Client)
(5) Delete all IPsec SAs for a given peer (GW)
(6) Delete all IPsec SAs for a given User (Client)
(7) Delete all IPsec+IKE SAs for a given peer (GW)
(8) Delete all IPsec+IKE SAs for a given User (Client)
(9) Delete all IPsec SAs for ALL peers and users
(0) Delete all IPsec+IKE SAs for ALL peers and users

* To list data for a specific CoreXL instance, append "-i <instance number>" to your selection.

(Q) Quit

*******************************************

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see VPN Connect Metrics on page 3164.

If you have issues, see VPN Connect Troubleshooting on page 3166.

Cisco ASA Configuration Options

Choose the configuration based on the ASA software version:

- **9.7.1 or newer:** Route-based configuration
- **8.5 to 9.7.0:** Policy-based configuration
- **Older than 8.5:** Not supported by the Oracle configuration instructions. Consider upgrading to a newer version.

**Important:**

Oracle recommends using a route-based configuration to avoid interoperability issues and to achieve tunnel redundancy with a single Cisco ASA device.

The Cisco ASA does not support route-based configuration for software versions older than 9.7.1. For the best results, if your device allows it, Oracle recommends that you upgrade to a software version that supports route-based configuration.

With policy-based configuration, you can configure only a single tunnel between your Cisco ASA and your dynamic routing gateway (DRG).

**Cisco ASA: Route-Based**

This topic provides a route-based configuration for a Cisco ASA that is running software version 9.7.1 (or newer).

As a reminder, Oracle provides different configurations based on the ASA software:

- **9.7.1 or newer:** Route-based configuration (this topic)
- **8.5 to 9.7.0:** Policy-based configuration
- **Older than 8.5:** Not supported by the Oracle configuration instructions. Consider upgrading to a newer version.

**Important:**

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still
Networking

work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. The IP addresses in this diagram are examples only and not for literal use.

Best Practices

This section covers general best practices and considerations for using VPN Connect.

Configure All Tunnels for Every IPSec Connection

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

Have Redundant CPEs in Your On-Premises Network Locations

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

Routing Protocol Considerations

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.

- **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.
Networking

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

Other Important CPE Configurations

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

Specific to Cisco ASA: Caveats and Limitations

This section covers important characteristics and limitations that are specific to Cisco ASA.

Tunnel MTU and Path MTU Discovery

You have two options for addressing tunnel MTU and path MTU discovery with Cisco ASA:

- Option 1: TCP MSS adjustment on page 3022
- Option 2: Clear/set the Don't Fragment bit on page 3022

Option 1: TCP MSS adjustment

The maximum transmission unit (packet size) through the IPSec tunnel is less than 1500 bytes. You can fragment packets that are too large to fit through the tunnel. Or, you can signal back to the hosts that are communicating through the tunnel that they need to send smaller packets.

You can configure the Cisco ASA to change the maximum segment size (MSS) for any new TCP flows through the tunnel. The ASA looks at any TCP packets where the SYN flag is set and changes the MSS value to the configured value. This configuration might help new TCP flows avoid using path maximum transmission unit discovery (PMTUD).

Use the following command to change the MSS. This command is not part of the sample configuration in the CPE Configuration on page 3038 section of this topic. Apply the TCP MSS adjustment command manually, if needed.

```
sysopt connection tcpmss 1387
```

Option 2: Clear/set the Don't Fragment bit

Path MTU discovery requires that all TCP packets have the Don't Fragment (DF) bit set. If the DF bit is set and a packet is too large to go through the tunnel, the ASA drops the packet when it arrives. The ASA sends an ICMP packet back to the sender indicating that the received packet was too large for the tunnel. The ASA offers three options for handling the DF bit. Choose one of the options and apply it to the configuration:

- Set the DF bit (recommended): Packets have the DF bit set in their IP header. The ASA may still fragment the packet if the original received packet cleared the DF bit.
  
  ```
  crypto ipsec df-bit set-df ${outsideInterface}
  ```

- Clear the DF bit: The DF bit is cleared in the packet's IP header. Allows the packet to be fragmented and sent to the end host in Oracle Cloud Infrastructure for reassembly.

  ```
  crypto ipsec df-bit clear-df ${outsideInterface}
  ```

- Ignore (copy) the DF bit: The ASA looks at the original packet's IP header information and copies the DF bit setting.

  ```
  crypto ipsec df-bit copy-df ${outsideInterface}
  ```

VPN Traffic Might Enter One Tunnel and Exit Another
Networking

If VPN traffic enters an interface with the same security level as an interface toward the packet's next hop, you must allow that traffic. By default, the packets between interfaces that have identical security levels on your ASA are dropped.

Add the following command manually if you need to permit traffic between interfaces with the same security levels. This command is not part of the sample configuration in the CPE Configuration on page 3038 section.

```text
same-security-traffic permit inter-interface
```

**General Caveats and Limitations**

This section covers general characteristics and limitations of VPN Connect.

**Asymmetric Routing**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

**Route-Based or Policy-Based IPSec VPN**

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

**Note:**

Other vendors or industry documentation might use the term *proxy ID*, *security parameter index (SPI)*, or *traffic selector* when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels:** Also called *next-hop-based tunnels*. A route table lookup is performed on a packet's destination IP address. If that route's egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

- **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

**Encryption domain for route-based tunnels**

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4
If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

Important:

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's private IP address, as shown in the following diagram.
Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

**Supported IPSec Parameters**

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

**CPE Configuration**

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

The configuration template provided is for a Cisco router running Cisco ASA 9.7.1 software (or later). The template provides information for each tunnel that you must configure. Oracle recommends setting up all configured tunnels for maximum redundancy.
The configuration template refers to these items that you must provide:

- **CPE public IP address**: The internet-routable IP address that is assigned to the external interface on the CPE. You or your Oracle administrator provides this value to Oracle when creating the CPE object in the Oracle Console.
- **Inside tunnel interface (required if using BGP)**: The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these values when creating the IPSec connection in the Oracle Console.
- **BGP ASN (required if using BGP)**: Your BGP ASN.

In addition, you must:

- Configure internal routing that routes traffic between the CPE and your local network.
- Ensure that you permit traffic between your ASA and your Oracle VCN.
- Identify the IPSec profile used (the following configuration template references this group policy as `oracle-vcn-vpn-policy`).
- Identify the transform set used for your crypto map (the following configuration template references this transform set as `oracle-vcn-transform`).
- Identify the virtual tunnel interface names used (the following configuration template references these as variables `${tunnelInterfaceName1}` and `${tunnelInterfaceName2}`).

**Important:**

This following configuration template from Oracle Cloud Infrastructure is a starting point for what you need to apply to your CPE. Some of the parameters referenced in the template must be unique on the CPE, and the uniqueness can only be determined by accessing the CPE. Ensure that the parameters are valid on your CPE and do not overwrite any previously configured values. In particular, ensure these values are unique:

- Policy names or numbers
- Interface names or numbers
- Access list numbers (if applicable)

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

Oracle provides a separate configuration template for IKEv1 versus IKEv2.

Oracle also provides a tool that can generate the template for you, with some of the information automatically filled in. For more information, see Using the CPE Configuration Helper on page 2970.

**IKEv1 Configuration Template**

```bash
!------------------------------------------------------------------------------------------------------------------------------------------------------------
! IKEv1 Configuration Template
! The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.
!------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template involves setting up the following:
! ISAKMP Policy
! IPSec Configuration
! IPSec Tunnel Group Configuration
! VTI Interface Configuration
! IP Routing (BGP or Static)
!------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template has various parameters that you must define before applying the configuration.
!------------------------------------------------------------------------------------------------------------------------------------------------------------
! PARAMETERS REFERENCED:
```

---

Oracle Cloud Infrastructure User Guide 3026
Networking

! ${OracleInsideTunnelIpAddress1} = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.

! ${OracleInsideTunnelIpAddress2} = Inside tunnel IP address of Oracle-side for the second tunnel. You provide these values when creating the IPSec connection in the Oracle Console.

! ${bgpASN} = Your BGP ASN

! ${cpePublicIpAddress} = The public IP address for the CPE. This is the IP address of your outside interface

! ${oracleHeadend1} = Oracle public IP endpoint obtained from the Oracle Console.

! ${oracleHeadend2} = Oracle public IP endpoint obtained from the Oracle Console.

! ${sharedSecret1} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.

! ${sharedSecret2} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.

! ${outsideInterface} = The public interface or outside of tunnel interface which is configured with the CPE public IP address.

! ${tunnelInterfaceName1} = The name of the first VTI used on your ASA.

! ${tunnelInterfaceName2} = The name of the second VTI used on your ASA.

! ${cpeInsideTunnelIpAddress1} = The CPE's inside tunnel IP for the first tunnel.

! ${cpeInsideTunnelIpAddress2} = The CPE's inside tunnel IP for the second tunnel.

! ${cpeInsideTunnelNetmask1} = The CPE's inside tunnel netmask for the first tunnel.

! ${cpeInsideTunnelNetmask2} = The CPE's inside tunnel netmask for the second tunnel.

! ${vcnCidrNetwork} = VCN IP range

! ${vcnCidrNetmask} = Subnet mask for VCN

! ${onPremCidrNetwork} = On-premises IP range

! ${onPremCidrNetmask} = ON-premises subnet mask

----------------------------------------------------------------------------------------------

! ISAKMP Policy

! ISAKMP Phase 1 configuration.

IKEv1 is enabled on the outside interface.

IKEv1 policy is created for Phase 1 which specifies to use a Pre-Shared Key, AES256, SHA1, Diffie-Hellman Group 5, and a Phase 1 lifetime of 28800 seconds (8 hours).

If different parameters are required, modify this template before applying the configuration.

WARNING: The IKEv1 group policy is created with a priority of 10. Make sure this doesn't conflict with any pre-existing configuration on your ASA.

crypto ikev1 enable ${outsideInterface}

crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 5
  lifetime 28800

! IPSec Configuration

Create an IKEv1 transform set named 'oracle-vcn-transform' which defines a combination of IPSec (Phase 2) policy options. Specifically, AES256 for encryption and SHA1 for authentication.

If different parameters are required, modify this template before applying the configuration.
crypto ipsec ikev1 transform-set oracle-vcn-transform esp-aes-256 esp-sha-hmac

! A IPSec profile named 'oracle-vcn-vpn-policy' is created.
! The previously created transform set is added to this policy along with settings for enabling PFS Group 5 and the security association lifetime to 3600 seconds (1 hour).
! If different parameters are required, modify this template before applying the configuration.

crypto ipsec profile oracle-vcn-vpn-policy
  set ikev1 transform-set oracle-vcn-transform
  set pfs group5
  set security-association lifetime seconds 3600

! IPSec Tunnel Group Configuration

! A tunnel group is created for each Oracle VPN Headend. Each tunnel group defines the pre-shared key used for each respective tunnel.

tunnel-group $(oracleHeadend1) type ipsec-l2l
  ikev1 pre-shared-key $(sharedSecret1)

tunnel-group $(oracleHeadend2) type ipsec-l2l
  ikev1 pre-shared-key $(sharedSecret2)

! VTI Interface Configuration

! A virtual tunnel interface (VTI) is a logical interface representing the local end of a VPN tunnel to a remote VPN peer. Two VTIs are created representing two tunnels, one to each Oracle VPN Headend. The IP address of each VPN headend is provided when you create your IPSec connection in Oracle Console.
! All traffic routed to a VTI will be encrypted and sent across the tunnel towards Oracle Cloud Infrastructure.
! Each VTI configuration also references the previously created IPSec profile 'oracle-vcn-vpn-policy' for its IPSec parameters.

interface ${tunnelInterfaceName1}
  nameif ORACLE-VPN1
  ip address $(cpeInsideTunnelIpAddress1) $(cpeInsideTunnelNetmask1)
  tunnel source interface $(outsideInterface)
  tunnel destination $(oracleHeadend1)
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile oracle-vcn-vpn-policy

interface ${tunnelInterfaceName2}
  nameif ORACLE-VPN2
  ip address $(cpeInsideTunnelIpAddress2) $(cpeInsideTunnelNetmask2)
  tunnel source interface $(outsideInterface)
  tunnel destination $(oracleHeadend2)
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile oracle-vcn-vpn-policy

! IP Routing
! Pick either dynamic (BGP) or static routing. Uncomment the corresponding commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you want to use BGP.

! router bgp ${bgpASN}
address-family ipv4 unicast
neighbor ${OracleInsideTunnelIpAddress1} remote-as 31898
neighbor ${OracleInsideTunnelIpAddress1} activate
neighbor ${OracleInsideTunnelIpAddress2} remote-as 31898
neighbor ${OracleInsideTunnelIpAddress2} activate
network ${onPremCidrNetwork} mask ${onPremCidrNetmask}
no auto-summary
no synchronization
exit-address-family

Static Route Configuration
Each static route references the other VTI by its name if value.
 Uncomment below line if you want to use static routing.

route ORACLE-VPN1 ${VcnCidrNetwork} ${VcnCidrNetmask}
${OracleInsideTunnelIpAddress1} 1 track
route ORACLE-VPN2 ${VcnCidrNetwork} ${VcnCidrNetmask}
${OracleInsideTunnelIpAddress2} 100

Configuration for Tunnel Failover
 Uncomment the below IP SLA lines if using static routing.
 Use this IP SLA configuration for static route failover This IP SLA
 configuration is used for static route failover between the two tunnels.
 Make sure that the SLA monitor and tracking numbers used do not conflict
 with any existing configuration on your ASA.

sla monitor 10
! type echo protocol ipIcmpEcho ${oracleHeadend1} interface outside
! frequency 5
! sla monitor schedule 10 life forever start-time now
! track 1 rtr 10 reachability

IKEv2 Configuration Template

IKEv2 Configuration Template
The configuration consists of two IPSec tunnels. Oracle highly recommends
that you configure both tunnels for maximum redundancy.

The configuration template involves setting up the following:
IKEv2 Policy
IPSec Configuration
IPSec Tunnel Group Configuration
VTI Interface Configuration
IP Routing (BGP or Static)

The configuration template has various parameters that you must define
before applying the configuration.

PARAMETERS REFERENCED:
${OracleInsideTunnelIpAddress1} = Inside tunnel IP address of Oracle-side
for the first tunnel. You provide these values when creating the IPSec
connection in the Oracle Console.
${OracleInsideTunnelIpAddress2} = Inside tunnel IP address of Oracle-side
for the second tunnel. You provide these values when creating the IPSec
connection in the Oracle Console.
${bgpASN} = Your BGP ASN
${cpePublicIpAddress} = The public IP address for the CPE. This is the IP
address of your outside interface
${oracleHeadend1} = Oracle public IP endpoint obtained from the Oracle
Console.
Networking

! ${oracleHeadend2} = Oracle public IP endpoint obtained from the Oracle Console.
! ${sharedSecret1} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
! ${sharedSecret2} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
! ${outsideInterface} = The public interface or outside of tunnel interface which is configured with the CPE public IP address.
! ${tunnelInterfaceName1} = The name of the first VTI used on your ASA.
! ${tunnelInterfaceName2} = The name of the second VTI used on your ASA.
! ${cpeInsideTunnelIpAddress1} = The CPE's inside tunnel IP for the first tunnel.
! ${cpeInsideTunnelIpAddress2} = The CPE's inside tunnel IP for the second tunnel.
! ${cpeInsideTunnelNetmask1} = The CPE's inside tunnel netmask for the first tunnel.
! ${cpeInsideTunnelNetmask2} = The CPE's inside tunnel netmask for the second tunnel.
! ${vcnCidrNetwork} = VCN IP range
! ${vcnCidrNetmask} = Subnet mask for VCN
! ${onPremCidrNetwork} = On-premises IP range
! ${onPremCidrNetmask} = ON-premises subnet mask

! IKEv2 Policy

! IKEv2 is enabled on the outside interface.
! IKEv2 policy is created and specifies use of a Pre-Shared Key, AES256, SHA1, Diffie-Hellman Group 5, and a lifetime of 28800 seconds (8 hours).
! If different parameters are required, modify this template before applying the configuration.
! WARNING: The IKEv2 group policy is created with a priority of 10. Make sure this doesn't conflict with any pre-existing configuration on your ASA.

crypto ikev2 enable ${outsideInterface}
crypto ikev2 policy 10
  encryption aes-256
  integrity sha
  group 5
  prf sha
  lifetime seconds 28800

! IPSec Configuration

! Create an IKEv2 IPSec proposal named 'oracle_v2_ipsec_proposal' which defines AES256 for encryption and SHA1 for authentication.
! If different parameters are required, modify this template before applying the configuration.

crypto ipsec ikev2 ipsec-proposal oracle_v2_ipsec_proposal
  protocol esp encryption aes-256
  protocol esp integrity sha-1

! An IPSec profile named 'oracle-vcn-vpn-policy' is created.
! The previously created IPSec proposal is added to this policy along with settings for enabling PFS Group 5 and the security association lifetime to 3600 seconds (1 hour).
! If different parameters are required, modify this template before applying the configuration.

crypto ipsec profile oracle-vcn-vpn-policy
  set ikev2 ipsec-proposal oracle_v2_ipsec_proposal
  set pfs group5
set security-association lifetime seconds 3600

! IPSec Tunnel Group Configuration

group-policy oracle_v2_group_policy internal
group-policy oracle_v2_group_policy attributes
vpn-tunnel-protocol ikev2

! A tunnel group is created for each Oracle VPN Headend. Each tunnel group defines the pre-shared key used for each respective tunnel.
tunnel-group ${oracleHeadend1} type ipsec-l2l
tunnel-group ${oracleHeadend1} general-attributes
default-group-policy oracle_v2_group_policy
tunnel-group ${oracleHeadend1} ipsec-attributes
   ikev2 local-authentication pre-shared-key ${sharedSecret1}
   ikev2 remote-authentication pre-shared-key ${sharedSecret1}

tunnel-group ${oracleHeadend2} type ipsec-l2l
tunnel-group ${oracleHeadend2} general-attributes
default-group-policy oracle_v2_group_policy
tunnel-group ${oracleHeadend2} ipsec-attributes
   ikev2 local-authentication pre-shared-key ${sharedSecret2}
   ikev2 remote-authentication pre-shared-key ${sharedSecret2}

! VTI Interface Configuration

! A virtual tunnel interface (VTI) is a logical interface representing the local end of a VPN tunnel to a remote VPN peer. Two VTIs are created representing two tunnels, one to each Oracle VPN Headend. The IP address of each VPN headend is provided when you create your IPSec connection in Oracle Console.
! All traffic routed to a VTI will be encrypted and sent across the tunnel towards Oracle Cloud Infrastructure.
! Each VTI configuration also references the previously created IPSec profile 'oracle-vcn-vpn-policy' for its IPSec parameters.

interface ${tunnelInterfaceName1}
   nameif ORACLE-VPN1
   ip address ${cpeInsideTunnelIpAddress1} ${cpeInsideTunnelNetmask1}
   tunnel source interface ${outsideInterface}
   tunnel destination ${oracleHeadend1}
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile oracle-vcn-vpn-policy

interface ${tunnelInterfaceName2}
   nameif ORACLE-VPN2
   ip address ${cpeInsideTunnelIpAddress2} ${cpeInsideTunnelNetmask2}
   tunnel source interface ${outsideInterface}
   tunnel destination ${oracleHeadend2}
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile oracle-vcn-vpn-policy

! IP Routing
! Pick either dynamic (BGP) or static routing. Uncomment the corresponding commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you want to use BGP.

! router bgp ${bgpASN}
!   address-family ipv4 unicast
!     neighbor ${OracleInsideTunnelIpAddress1} remote-as 31898
!     neighbor ${OracleInsideTunnelIpAddress1} activate
Networking

! neighbor ${OracleInsideTunnelIpAddress2} remote-as 31898
! neighbor ${OracleInsideTunnelIpAddress2} activate
! network ${onPremCidrNetwork} mask ${onPremCidrNetmask}
! no auto-summary
! no synchronization
! exit-address-family

! Static Route Configuration
! Each static route references the other VTI by its nameif value.
! Uncomment below line if you want to use static routing.

! route ORACLE-VPN1 ${VcnCidrNetwork} ${VcnCidrNetmask}
${OracleInsideTunnelIpAddress1} 1 track
! route ORACLE-VPN2 ${VcnCidrNetwork} ${VcnCidrNetmask}
${OracleInsideTunnelIpAddress2} 100

! Configuration for Tunnel Failover

! Uncomment the below IP SLA lines if using static routing.
! Use this IP SLA configuration for static route failover This IP SLA configuration is used for static route failover between the two tunnels.
! Make sure that the SLA monitor and tracking numbers used do not conflict with any existing configuration on your ASA.

! sla monitor 10
! type echo protocol ipIcmpEcho ${oracleHeadend1} interface outside
! frequency 5
! sla monitor schedule 10 life forever start-time now
! track 1 rtr 10 reachability

Verification

The following ASA commands are included for basic troubleshooting. For more exhaustive information, refer to Cisco’s IPSec Troubleshooting document.

Use the following command to verify that ISAKMP security associations are being built between the two peers.

`show crypto isakmp sa`

Use the following command to verify the status of all your BGP connections.

`show bgp summary`

Use the following command to verify the ASA’s route table.

`show route`

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see VPN Connect Metrics on page 3164.

If you have issues, see VPN Connect Troubleshooting on page 3166.

Cisco ASA: Policy-Based

This topic provides a policy-based configuration for a Cisco ASA that is running software version 8.5 to 9.7.0.

As a reminder, Oracle provides different configurations based on the ASA software:

- **9.7.1 or newer**: Route-based configuration
- **8.5 to 9.7.0**: Policy-based configuration (this topic)
- **Older than 8.5**: Not supported by the Oracle configuration instructions. Consider upgrading to a newer version.
Important:

Oracle recommends using a route-based configuration to avoid interoperability issues and to achieve tunnel redundancy with a single Cisco ASA device.

The Cisco ASA does not support route-based configuration for software versions older than 9.7.1. For the best results, if your device allows it, Oracle recommends that you upgrade to a software version that supports route-based configuration.

With policy-based configuration, you can configure only a single tunnel between your Cisco ASA and your dynamic routing gateway (DRG).

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. The IP addresses in this diagram are examples only and not for literal use.

Important:

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor’s documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you’re already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor’s documentation for assistance.

Best Practices

This section covers best practices and considerations for using VPN Connect.

Specific to Cisco ASA: VPN filters

VPN filters let you further filter traffic either before it enters or after it exits a tunnel. Use VPN filters if you need additional granularity for filtering different traffic types or source/destination flows. For more information, see Cisco’s VPN Filter documentation.

VPN filter configuration is not included in the configuration template that appears in the CPE Configuration on page 3038 section. To use VPN filters, add the following configuration items manually.
• **Access control list (ACL)**: Create an ACL that the VPN filter can use to restrict the traffic permitted through the tunnels. If you have an ACL already used for a VPN filter, do not also use it for an interface access group.

```
access-list ${vpnFilterAclName} extended permit ip ${VcnCidrNetwork} ${VcnCidrNetmask} ${onPremCidrNetwork} ${onPremCidrNetmask}
```

• **Group policy**: Apply the VPN filter to your group policy.

```
group-policy oracle-vcn-vpn-policy attributes
    vpn-filter value ${vpnFilterAclName}
```

• **Tunnel group**: Apply the group policy to your tunnel group.

```
tunnel-group ${oracleHeadend1} general-attributes
default-group-policy oracle-vcn-vpn-policy
```

**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

**Routing Protocol Considerations**

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

• **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.

• **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

**Other Important CPE Configurations**

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

**Specific to Cisco ASA: Caveats and Limitations**

This section covers important characteristics and limitations that are specific to Cisco ASA.
**Tunnel MTU and Path MTU Discovery**

You have two options for addressing tunnel MTU and path MTU discovery with Cisco ASA:

- **Option 1: TCP MSS adjustment** on page 3035
- **Option 2: Clear/set the Don’t Fragment bit** on page 3035

**Option 1: TCP MSS adjustment**

The maximum transmission unit (packet size) through the IPSec tunnel is less than 1500 bytes. You can fragment packets that are too large to fit through the tunnel. Or, you can signal back to the hosts that are communicating through the tunnel that they need to send smaller packets.

You can configure the Cisco ASA to change the maximum segment size (MSS) for any new TCP flows through the tunnel. The ASA looks at any TCP packets where the SYN flag is set and changes the MSS value to the configured value. This configuration might help new TCP flows avoid using path maximum transmission unit discovery (PMTUD).

Use the following command to change the MSS. This command is not part of the sample configuration in the CPE Configuration on page 3038 section of this topic. Apply the TCP MSS adjustment command manually, if needed.

```bash
sysopt connection tcpmss 1387
```

**Option 2: Clear/set the Don’t Fragment bit**

Path MTU discovery requires that all TCP packets have the **Don’t Fragment** (DF) bit set. If the DF bit is set and a packet is too large to go through the tunnel, the ASA drops the packet when it arrives. The ASA sends an ICMP packet back to the sender indicating that the received packet was too large for the tunnel. The ASA offers three options for handling the DF bit. Choose one of the options and apply it to the configuration:

- **Set the DF bit (recommended):** Packets have the DF bit set in their IP header. The ASA may still fragment the packet if the original received packet cleared the DF bit.
  ```bash
  crypto ipsec df-bit set-df ${outsideInterface}
  ```

- **Clear the DF bit:** The DF bit is cleared in the packet's IP header. Allows the packet to be fragmented and sent to the end host in Oracle Cloud Infrastructure for reassembly.
  ```bash
  crypto ipsec df-bit clear-df ${outsideInterface}
  ```

- **Ignore (copy) the DF bit:** The ASA looks at the original packet's IP header information and copies the DF bit setting.
  ```bash
  crypto ipsec df-bit copy-df ${outsideInterface}
  ```

**VPN Traffic Might Enter One Tunnel and Exit Another**

If VPN traffic enters an interface with the same security level as an interface toward the packet's next hop, you must allow that traffic. By default, the packets between interfaces that have identical security levels on your ASA are dropped.

Add the following command manually if you need to permit traffic between interfaces with the same security levels. This command is not part of the sample configuration in the CPE Configuration on page 3038 section.

```bash
same-security-traffic permit inter-interface
```

**General Caveats and Limitations**

This section covers general characteristics and limitations of VPN Connect.
Networking

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

Note:

Other vendors or industry documentation might use the term proxy ID, security parameter index (SPI), or traffic selector when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels:** Also called next-hop-based tunnels. A route table lookup is performed on a packet's destination IP address. If that route's egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

- **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.
Important:

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE’s public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE’s private IP address, as shown in the following diagram.
Networking

**Note:**

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

**Supported IPSec Parameters**

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle’s BGP ASN on page 171.

**CPE Configuration**

**Important:**

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor’s support directly.

The following figure shows the basic layout of the IPSec connection.

![Basic Layout of IPSec Connection](image)

The configuration template provided is for a Cisco ASA running version 8.5 software (or later).

**Note:**

Cisco ASA versions 9.7.1 and newer support route-based configuration, which is the recommended method to avoid interoperability issues.

If you want tunnel redundancy with a single Cisco ASA device, you must use the route-based configuration. With policy-based configuration, you can configure only a single tunnel between your Cisco ASA and your dynamic routing gateway (DRG).

The configuration template refers to these items that you must provide:

- **CPE public IP address:** The internet-routable IP address that is assigned to the external interface on the CPE. You or your Oracle administrator provides this value to Oracle when creating the CPE object in the Oracle Console.
- **Inside tunnel interface (required if using BGP):** The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these values when creating the IPSec connection in the Oracle Console.
- **BGP ASN (required if using BGP):** Your BGP ASN.

In addition, you must:

- Configure internal routing that routes traffic between the CPE and your local network.
- Ensure that you permit traffic between your ASA and your Oracle VCN (the following configuration template references this access list with the variable \$\{outboundAclName\}).
- Identify the internal VPN group policy (the following configuration template references this group policy as oracle-vcn-vpn-policy).
- Identify the transform set used for your crypto map (the following configuration template references this transform set as oracle-vcn-transform).
- Identify the crypto map name and sequence number (the following configuration template references the map name as oracle-vpn-map-v1 and sequence number 1).
- Identify the operation number for IP SLA continuous ping (the following configuration template uses operation number 1).

### Important:

This following configuration template from Oracle Cloud Infrastructure is a starting point for what you need to apply to your CPE. The syntax for each CPE device configuration may be different and depends on the model and software versions. Be sure to compare your CPE model and version to the appropriate configuration template.

Some of the parameters referenced in the template must be unique on the CPE, and the uniqueness can only be determined by accessing the CPE. Ensure that the parameters are valid on your CPE and do not overwrite any previously configured values. In particular, ensure that the following values are unique:

- Policy names or numbers
- Crypto map names and sequence numbers
- Interface names
- Access list names or numbers (if applicable)

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see [Supported IPSec Parameters](#) on page 2945.

Oracle also provides a separate configuration template for IKEv1 versus IKEv2.

Oracle provides a tool that can generate the template for you, with some of the information automatically filled in. For more information, see [Using the CPE Configuration Helper](#) on page 2970.

### IKEv1 Configuration Template

```plaintext
! Ikev1 Configuration Template
! The configuration consists of a single IPSec tunnel.
! The configuration template involves setting up the following:
! Access Lists
! ISAKMP Policy
! Base VPN Policy
! IPSec Configuration
! IPSec Tunnel Group Configuration
! IP Routing (BGP or Static)
! Optional: Disable NAT for VPN Traffic
```

---
Networking

The configuration template has various parameters that you must define before applying the configuration.

PARAMETERS REFERENCED:

${OracleInsideTunnelIpAddress1} = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.

${bgpASN} = Your BGP ASN

${cpePublicIpAddress} = The public IP address for the CPE. This is the IP address of your outside interface

${outboundAclName} = ACL used to control traffic out of your inside and outside interfaces

${oracleHeadend1} = Oracle public IP endpoint obtained from the Oracle Console.

${sharedSecret1} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.

${outsideInterface} = The public interface or outside of tunnel interface which is configured with the CPE public IP address.

${vcnCidrNetwork} = VCN IP range

${vcnCidrNetmask} = Subnet mask for VCN

${onPremCidrNetwork} = On-premises IP range

${onPremCidrNetmask} = ON-premises subnet mask

${cryptoMapAclName} = Name of ACL which will be associated with the IPSec security association.

${vcnHostIp} = IP address of a VCN host. Used for IP SLA continuous ping to maintain tunnel UP state.

Access Lists

Permit Traffic Between Your ASA and Your Oracle VCN

Assuming there is an access-list controlling traffic in and out of your Internet facing interface, you will need to permit traffic between your CPE and the Oracle VPN Headend

WARNING: The new ACL entry you add to permit the traffic between your ASA and VPN headend needs to be above any deny statements you might have in your existing access-list

access-list ${outboundAclName} extended permit ip host ${oracleHeadend1}
host ${cpePublicIpAddress}

Crypto ACL

Create an ACL named ${cryptoMapAclName} which will later be associated with the IPSec security association using the 'crypto-map' command. This will define which source/destination traffic needs to be encrypted and sent across the VPN tunnel.

Keep this ACL to a single entry. In a policy based configuration each ACL line will establish a separate encryption domain.

The encryption domain used in this configuration sample will have a source/destination of any/VCN CIDR. Refer to the 'Encryption domain for policy-based tunnels' subsection for supported alternatives.

access-list ${cryptoMapAclName} extended permit ip any ${vcnCidrNetwork}
${vcnCidrNetmask}

ISAKMP Policy

ISAKMP Phase 1 configuration.
IKEv1 is enabled on the outside interface.
IKEv1 policy is created for Phase 1 which specifies to use a Pre-Shared Key, AES256, SHA1, Diffie-Hellman Group 5, and a Phase 1 lifetime of 28800 seconds (8 hours).
If different parameters are required, modify this template before applying the configuration.
! WARNING: The IKEv1 group policy is created with a priority of 10. Make sure this doesn't conflict with any pre-existing configuration on your ASA.

crypto ikev1 enable outside
crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 5
  lifetime 28800

! Base VPN Policy

! An internal VPN group policy named 'oracle-vcn-vpn-policy' is created to define some basic VPN tunnel settings
! Idle and session timeouts are disabled to maintain the tunnel UP state and tunnel protocol is set to IKEv1

group-policy oracle-vcn-vpn-policy internal
group-policy oracle-vcn-vpn-policy attributes
  vpn-idle-timeout none
  vpn-session-timeout none
  vpn-tunnel-protocol ikev1

! IPSec Configuration

! Create an IKEv1 transform set named 'oracle-vcn-transform' which defines a combination of IPSec (Phase 2) policy options. Specifically, AES256 for encryption and SHA1 for authentication.
! If different parameters are required, modify this template before applying the configuration.

crypto ipsec ikev1 transform-set oracle-vcn-transform esp-aes-256 esp-sha-hmac

! A crypto map is used to tie together the important traffic that needs encryption (via crypto map ACL) with defined security policies (from the transform set along with other crypto map statements), and the destination of the traffic to a specific crypto peer.
! In this configuration example, a single crypto map is created named 'oracle-vcn-map-v1' This crypto map references the previously created crypto map ACL, the 'oracle-vcn-transform' transform set and further defines PFS Group 5 and the security association lifetime to 3600 seconds (1 hour).
! WARNING: Make sure your crypto map name and sequence numbers do not overlap with existing crypto maps.
! WARNING: DO NOT use the 'originate-only' option with an Oracle IPSec VPN tunnel. It causes the tunnel's traffic to be inconsistently blackholed. The command is only for tunnels between two Cisco devices. Here's an example of the command that you should NOT use for the Oracle IPSec VPN tunnels:
crypto map <map name> <sequence number> set connection-type originate-only

crypto map oracle-vcn-map-v1 1 match address ${cryptoMapAclName}
crypto map oracle-vcn-map-v1 1 set pfs group5
crypto map oracle-vcn-map-v1 1 set peer ${oracleHeadend1}
crypto map oracle-vcn-map-v1 1 set ikev1 transform-set oracle-vcn-transform
crypto map oracle-vcn-map-v1 1 set security-association lifetime seconds 3600

! WARNING: The below command will apply the 'oracle-vcn-map-v1' crypto map to the outside interface. The Cisco ASA supports a single crypto map per interface. Make sure no other crypto map is applied to the outside interface before using this command.
crypto map oracle-vcn-map-v1 1 apply interface outside
crypto map oracle-vpn-map-v1 interface outside

! IPSec Tunnel Group Configuration

! This configuration matches the group policy 'oracle-vcn-vpn-policy' with an Oracle VPN headend endpoint.
! The pre-shared key for each Oracle VPN headend is defined in the corresponding tunnel group.

tunnel-group ${oracleHeadend1} type ipsec-l2l
tunnel-group ${oracleHeadend1} general-attributes
default-group-policy oracle-vcn-vpn-policy
tunnel-group ${oracleHeadend1} ipsec-attributes
ikev1 pre-shared-key ${sharedSecret1}

! IP SLA Configuration

! The Cisco ASA doesn't establish a tunnel if there's no interesting traffic trying to pass through the tunnel.
! You must configure IP SLA on your device for a continuous ping so that the tunnel remains up at all times.
! You must allow ICMP on the outside interface.
! Make sure that the SLA monitor number used is unique.

sla monitor 1
type echo protocol ipIcmpEcho ${vcnHostIp} interface outside
frequency 5
sla monitor schedule 1 life forever start-time now
icmp permit any ${outsideInterface}

! IP Routing
! Pick either dynamic (BGP) or static routing. Uncomment the corresponding commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you want to use BGP.

! router bgp ${bgpASN}
! address-family ipv4 unicast
! neighbor ${OracleInsideTunnelIpAddress1} remote-as 31898
! neighbor ${OracleInsideTunnelIpAddress1} activate
! network ${onPremCidrNetwork} mask ${onPremCidrNetmask}
! no auto-summary
! no synchronization
! exit-address-family

! Static Route Configuration
! Uncomment below line if you want to use static routing.

! route outside ${VcnCidrNetwork} ${VcnCidrNetmask}
${OracleInsideTunnelIpAddress1}

! Disable NAT for VPN Traffic

! If you are using NAT for traffic between your inside and outside interfaces, you might need to disable NAT for traffic between your on-premises network and the Oracle VCN.
! Two objects are created for this NAT exemption. 'obj-OnPrem' represents the on-premises network as a default route, and 'obj-oracle-vcn-1' represents the VCN CIDR block used in Oracle Cloud Infrastructure.
! If different address ranges are required, modify this template before applying the configuration.
Networking

! object network obj-onprem
! subnet 0.0.0.0 0.0.0.0
! object network obj-oracle-vcn-1
! subnet ${vcnCidrNetwork} ${vcnCidrNetmask}
! nat (inside, outside) source static obj-onprem obj-onprem destination
static obj-oracle-vcn-1 obj-oracle-vcn-1

IKEv2 Configuration Template

!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! IKEv2 Configuration Template
! The configuration consists of a single IPSec tunnel.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template involves setting up the following:
! Access Lists
! IKEv2 Policy
! Base VPN Policy
! IPSec Configuration
! IPSec Tunnel Group Configuration
! IP Routing (BGP or Static)
! Optional: Disable NAT for VPN Traffic
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template has various parameters that you must define before applying the configuration.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! PARAMETERS REFERENCED:
! ${OracleInsideTunnelIpAddress1} = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
! ${bgpASN} = Your BGP ASN
! ${cpePublicIpAddress} = The public IP address for the CPE. This is the IP address of your outside interface
! ${outboundAclName} = ACL used to control traffic out of your inside and outside interfaces
! ${oracleHeadend1} = Oracle public IP endpoint obtained from the Oracle Console.
! ${sharedSecret1} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
! ${outsideInterface} = The public interface or outside of tunnel interface which is configured with the CPE public IP address.
! ${vcnCidrNetwork} = VCN IP range
! ${vcnCidrNetmask} = Subnet mask for VCN
! ${onPremCidrNetwork} = On-premises IP range
! ${onPremCidrNetmask} = ON-premises subnet mask
! ${cryptoMapAclName} = Name of ACL which will be associated with the IPSec security association.
! ${vcnHostIp} = IP address of a VCN host. Used for IP SLA continuous ping to maintain tunnel UP state.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------

! Access Lists

! Permit Traffic Between Your ASA and Your Oracle VCN
! Assuming there is an access-list controlling traffic in and out of your Internet facing interface, you will need to permit traffic between your CPE and the Oracle VPN Headend
! WARNING: The new ACL entry you add to permit the traffic between your ASA and VPN headend needs to be above any deny statements you might have in your existing access-list

access-list ${outboundAclName} extended permit ip host ${oracleHeadend1}
host ${cpePublicIpAddress}

Oracle Cloud Infrastructure User Guide

3043
Networking

! Crypto ACL

! Create an ACL named `${cryptoMapAclName}` which will later be associated with the IPSec security association using the 'crypto-map' command. This will define which source/destination traffic needs to be encrypted and sent across the VPN tunnel.
! Keep this ACL to a single entry. In a policy based configuration each ACL line will establish a separate encryption domain.
! The encryption domain used in this configuration sample will have a source/destination of any/VCN CIDR. Refer to the 'Encryption domain for policy-based tunnels' subsection for supported alternatives.

access-list `${cryptoMapAclName}` extended permit ip any `${vcnCidrNetwork}`

! IKEv2 Policy

! IKEv2 is enabled on the outside interface.
! IKEv2 policy is created and specifies use of a Pre-Shared Key, AES256, SHA1, Diffie-Hellman Group 5, and a lifetime of 28800 seconds (8 hours).
! If different parameters are required, modify this template before applying the configuration.
! WARNING: The IKEv2 group policy is created with a priority of 10. Make sure this doesn't conflict with any pre-existing configuration on your ASA.

crypto ikev2 enable outside
crypto ikev2 policy 10
   encryption aes-256
   integrity sha384
   group 5
   prf sha
   lifetime seconds 28800

! Base VPN Policy

! An internal VPN group policy named 'oracle-vcn-vpn-policy' is created to define some basic VPN tunnel settings
! Idle and session timeouts are disabled to maintain the tunnel UP state and tunnel protocol is set to IKEv2

group-policy oracle-vcn-vpn-policy internal
group-policy oracle-vcn-vpn-policy-policy attributes
   vpn-idle-timeout none
   vpn-session-timeout none
   vpn-tunnel-protocol ikev2

! IPSec Configuration

! Create an IKEv2 IPSec proposal named 'oracle_v2_ipsec_proposal' which defines AES256 for encryption and SHA1 for authentication.
! If different parameters are required, modify this template before applying the configuration.

crypto ipsec ikev2 ipsec-proposal oracle_v2_ipsec_proposal
   protocol esp encryption aes-256
   protocol esp integrity sha-1

! A crypto map is used to tie together the important traffic that needs encryption (via crypto map ACL) with defined security policies (from the IPSec proposal along with other crypto map statements), and the destination of the traffic to a specific crypto peer.
! In this configuration example, a single crypto map is created named 'oracle-vpn-map-v2'. This crypto map references the previously created crypto map ACL, the 'oracle_v2_ipsec_proposal' IPSec proposal and further
Networking

defines PFS Group 5 and the security association lifetime to 3600 seconds (1 hour).

! WARNING: Make sure your crypto map name and sequence numbers do not overlap with existing crypto maps.

! WARNING: DO NOT use the 'originate-only' option with an Oracle IPSec VPN tunnel. It causes the tunnel's traffic to be inconsistently blackholed. The command is only for tunnels between two Cisco devices. Here's an example of the command that you should NOT use for the Oracle IPSec VPN tunnels:
crypto map <map name> <sequence number> set connection-type originate-only

crypto map oracle-vpn-map-v2 1 match address $\{cryptoMapAclName\}
crypto map oracle-vpn-map-v2 1 set pfs group5
crypto map oracle-vpn-map-v2 1 set peer $\{oracleHeadend1\}
crypto map oracle-vpn-map-v2 1 set ikev2 ipsec-proposal
oracle_v2_ipsec_proposal
crypto map oracle-vpn-map-v2 1 set security-association lifetime seconds 3600

! WARNING: The below command will apply the 'oracle-vpn-map-v2' crypto map to the outside interface. The Cisco ASA supports a single crypto map per interface. Make sure no other crypto map is applied to the outside interface before using this command.
crypto map oracle-vpn-map-v2 interface outside

! IPSec Tunnel Group Configuration

! This configuration matches the group policy 'oracle-vcn-vpn-policy' with an Oracle VPN headend endpoint.
! The pre-shared key for each Oracle VPN headend is defined in the corresponding tunnel group.
tunnel-group $\{oracleHeadend1\} type ipsec-l2l
tunnel-group $\{oracleHeadend1\} general-attributes
default-group-policy oracle-vcn-vpn-policy
tunnel-group $\{oracleHeadend1\} ipsec-attributes
ikev2 local-authentication pre-shared-key $\{sharedSecret1\}
ikev2 remote-authentication pre-shared-key $\{sharedSecret1\}

! IP SLA Configuration

! The Cisco ASA doesn't establish a tunnel if there's no interesting traffic trying to pass through the tunnel.
! You must configure IP SLA on your device for a continuous ping so that the tunnel remains up at all times.
! You must allow ICMP on the outside interface.
! Make sure that the SLA monitor number used is unique.
sla monitor 1
type echo protocol ipIcmpEcho $\{vcnHostIp\} interface outside
frequency 5
sla monitor schedule 1 life forever start-time now
icmp permit any $\{outsideInterface\}

! IP Routing
! Pick either dynamic (BGP) or static routing. Uncomment the corresponding commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you want to use BGP.

! router bgp $\{bgpASN\}
! address-family ipv4 unicast
Networking

! neighbor ${OracleInsideTunnelIpAddress1} remote-as 31898
! neighbor ${OracleInsideTunnelIpAddress1} activate
! network ${onPremCidrNetwork} mask ${onPremCidrNetmask}
! no auto-summary
! no synchronization
! exit-address-family

! Static Route Configuration
! Uncomment below line if you want to use static routing.

! route outside ${VcnCidrNetwork} ${VcnCidrNetmask} ${OracleInsideTunnelIpAddress1}

! Disable NAT for VPN Traffic

! If you are using NAT for traffic between your inside and outside interfaces, you might need to disable NAT for traffic between your on-premises network and the Oracle VCN.
! Two objects are created for this NAT exemption. 'obj-OnPrem' represents the on-premises network as a default route, and 'obj-oracle-vcn-1' represents the VCN CIDR block used in Oracle Cloud Infrastructure.
! If different address ranges are required, modify this template before applying the configuration.

! object network obj-onprem
! subnet 0.0.0.0 0.0.0.0
! object network obj-oracle-vcn-1
! subnet ${vcnCidrNetwork} ${vcnCidrNetmask}
! nat (inside,outside) source static obj-onprem obj-onprem destination static obj-oracle-vcn-1 obj-oracle-vcn-1

Verification

The following ASA commands are included for basic troubleshooting. For more exhaustive information, refer to Cisco's IPSec Troubleshooting document.

Use the following command to verify that ISAKMP security associations are being built between the two peers.

```
show crypto isakmp sa
```

Use the following command to verify the status of all your BGP connections.

```
show bgp summary
```

Use the following command to verify the ASA's route table.

```
show route
```

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see VPN Connect Metrics on page 3164.

If you have issues, see VPN Connect Troubleshooting on page 3166.

Cisco IOS

This topic provides a route-based configuration for a Cisco IOS device. The configuration was validated using a Cisco 2921 running IOS version 15.4(3)M3.

| Important: |
| Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor. |
If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are for example purposes only.

**Best Practices**

This section covers general best practices and considerations for using VPN Connect.

**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

**Routing Protocol Considerations**

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
• **Static routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see *Routing for the Oracle IPSec VPN* on page 2934.

**Other Important CPE Configurations**

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

**Asymmetric Routing**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see *Routing for the Oracle IPSec VPN* on page 2934.

**Route-Based or Policy-Based IPSec VPN**

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

**Note:**

Other vendors or industry documentation might use the term *proxy ID*, *security parameter index (SPI)*, or *traffic selector* when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

• **Route-based tunnels:** Also called *next-hop-based tunnels*. A route table lookup is performed on a packet's destination IP address. If that route's egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

• **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.
Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

**Encryption domain for policy-based tunnels**

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

**Important:**

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

**If Your CPE Is Behind a NAT Device**

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's private IP address, as show in the following diagram.
Note:

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Supported IPSec Parameters

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

**CPE Configuration**

Important:

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

The configuration template was validated using a Cisco 2921 running IOS version 15.4(3)M3. The template provides information for each tunnel that you must configure. Oracle recommends setting up all configured tunnels for maximum redundancy.
The configuration template refers to these items that you must provide:

- **CPE public IP address:** The internet-routable IP address that is assigned to the external interface on the CPE. You or your Oracle administrator provides this value to Oracle when creating the CPE object in the Oracle Console.
- **Inside tunnel interface (required if using BGP):** The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these values when creating the IPSec connection in the Oracle Console.
- **BGP ASN (required if using BGP):** Your BGP ASN.

In addition, you must:

- Configure internal routing that routes traffic between the CPE and your local network.
- Ensure that you permit traffic between your CPE and your Oracle VCN.
- Identify the IPSec profile used (the following configuration template references this group policy as `oracle-vpn`).
- Identify the transform set used for your crypto map (the following configuration template references this transform set as `oracle-vpn-transform`).

**Important:**

This following configuration template from Oracle Cloud Infrastructure is a starting point for what you need to apply to your CPE. Some of the parameters referenced in the template must be unique on the CPE, and the uniqueness can only be determined by accessing the CPE. Ensure the parameters are valid on your CPE and do not overwrite any previously configured values. In particular, ensure these values are unique:

- Policy names or numbers
- Interface names
- Keyrings
- Access list numbers (if applicable)

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

There's a separate configuration template for IKEv1 versus IKEv2.

**IKEv1 Configuration Template**

```
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! IKEv1 Configuration Template
! The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template involves setting up the following:
! Keyring (Pre-Shared Key)
! Basic ISAKMP Options
! ISAKMP and IPSec Policy Configuration
! IPSec Peers
! Virtual Tunnel Interfaces
! IP Routing (BGP or Static)
! Update Any Internet Facing Access List to Allow IPSec and ISAKMP Packets
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template has various parameters that you must define before applying the configuration.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! PARAMETERS REFERENCED:
! `${OracleInsideTunnelIpAddress1}` = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
```
$\{OracleInsideTunnelIpAddress2\} = \text{Inside tunnel IP address of Oracle-side for the second tunnel. You provide these values when creating the IPSec connection in the Oracle Console.}$

$\{bgpASN\} = \text{Your BGP ASN}$

$\{cpePublicIpAddress\} = \text{The public IP address for the CPE. This is the IP address of your outside interface}$

$\{oracleHeadend1\} = \text{Oracle public IP endpoint obtained from the Oracle Console.}$

$\{oracleHeadend2\} = \text{Oracle public IP endpoint obtained from the Oracle Console.}$

$\{sharedSecret1\} = \text{You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.}$

$\{sharedSecret2\} = \text{You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.}$

$\{outsideInterface\} = \text{The public interface or outside of tunnel interface which is configured with the CPE public IP address.}$

$\{vcnCidrNetwork\} = \text{VCN IP range}$

$\{vcnCidrNetmask\} = \text{Subnet mask for VCN}$

$\{onPremCidrNetwork\} = \text{On-premises IP range}$

$\{onPremCidrNetmask\} = \text{ON-premises subnet mask}$

---

### Keyring (Pre-Shared Key)

For authentication during IKE a separate keyring is defined for each Oracle VPN Headend peer.

Add the pre-shared key for each Oracle VPN headend under the corresponding keyring.

```plaintext
crypto keyring oracle-vpn-$\{oracleHeadend1\}
   local-address $\{cpePublicIpAddress\}
   pre-shared-key address $\{oracleHeadend1\} key $\{sharedSecret1\}
crypto keyring oracle-vpn-$\{oracleHeadend2\}
   local-address $\{cpePublicIpAddress\}
   pre-shared-key address $\{oracleHeadend2\} key $\{sharedSecret2\}
```

### Basic ISAKMP Options

Optional IPSec settings are included here.

All optional settings included are recommended by Oracle. Remove or comment out any unneeded commands prior to applying this configuration.

WARNING: These settings are global and may impact other IPSec connections

- Enables fragmentation of IKE packets prior to encryption.
  ```plaintext
crypto isakmp fragmentation
```

- Enables Dead Peer Detection (DPD)
  ```plaintext
crypto isakmp keepalive 10 10
```

The Router will clear the DF-bit in the IP header. Allows the packet to be fragmented and sent to the end host in Oracle Cloud Infrastructure for reassembly.

```plaintext
crypto ipsec df-bit clear
```

- Increases security association anti-replay window. An increased window size is helpful for scenarios where packets are regularly being dropped due to delays.
  ```plaintext
crypto ipsec security-association replay window-size 128
```

### ISAKMP and IPSec Policy Configuration

An ISAKMP policy is created for Phase 1 which specifies to use a Pre-Shared Key, AES256, SHA384, Diffie-Hellman Group 5, and a Phase 1 lifetime of 28800 seconds (8 hours).
If different parameters are required, modify this template before applying the configuration.

**WARNING:** The ISAKMP group policy is created with a priority of 10. Make sure this doesn't conflict with any pre-existing configuration before applying.

```plaintext
crypto isakmp policy 10
  encr aes 256
  hash sha384
  authentication pre-share
  group 5
  lifetime 28800
```

Create an IPSec transform set named 'oracle-vpn-transform' which defines a combination of IPSec (Phase 2) policy options. Specifically, AES256 for encryption and SHA1 for authentication. This is also where tunnel mode is set for IPSec.

If different parameters are required, modify this template before applying the configuration.

```plaintext
crypto ipsec transform-set oracle-vpn-transform esp-aes 256 esp-sha-hmac
  mode tunnel
```

A IPSec profile named 'oracle-vpn' is created.

The previously created transform set is added to this policy along with settings for enabling PFS Group 5 and the security association lifetime to 3600 seconds (1 hour).

If different parameters are required, modify this template before applying the configuration.

```plaintext
crypto ipsec profile oracle-vpn
  set pfs group5
  set security-association lifetime seconds 3600
  set transform-set oracle-vpn-transform
```

**IPSec Peers**

Two ISAKMP profiles are created for each Oracle VPN Headend.

An ISAKMP profile is used as a repository for various Phase 1 commands tied to a specific IPSec peer. In this case, we match the previously created keyrings to an Oracle VPN headend.

```plaintext
crypto isakmp profile oracle-vpn-`{oracleHeadend1}`
  keyring oracle-vpn-`{oracleHeadend1}`
  self-identity address
  match identity address `{oracleHeadend1}` 255.255.255.255

crypto isakmp profile oracle-vpn-`{oracleHeadend2}`
  keyring oracle-vpn-`{oracleHeadend2}`
  self-identity address
  match identity address `{oracleHeadend2}` 255.255.255.255
```

**Virtual Tunnel Interfaces**

Each tunnel interface is a logical interface representing the local end of a VPN tunnel to a remote VPN peer. Each tunnel interface represents a single tunnel to a different Oracle VPN Headend. The IP address of each VPN headend is provided when you create your IPSec connection in Oracle Console.

All traffic routed to a tunnel interface will be encrypted and sent across the tunnel towards Oracle Cloud Infrastructure.

Each tunnel interface configuration also references the previously created IPSec profile 'oracle-vpn' for its IPSec parameters.

**WARNING:** When doing static routing you do NOT have to set IPs on the tunnel interfaces unless you have pre-configured inside tunnel interfaces.
in Oracle Console when creating your IPSec connection. Inside tunnel interfaces are required if using BGP.

```bash
interface Tunnel${tunnelNumber1}
 ip address ${cpeInsideTunnelIpAddress1} ${cpeInsideTunnelNetmask1}
tunnel source ${cpePublicIpAddress}
tunnel mode ipsec ipv4
tunnel destination ${oracleHeadend1}
tunnel protection ipsec profile oracle-vpn

interface Tunnel${tunnelNumber2}
 ip address ${cpeInsideTunnelIpAddress2} ${cpeInsideTunnelNetmask2}
tunnel source ${cpePublicIpAddress}
tunnel mode ipsec ipv4
tunnel destination ${oracleHeadend2}
tunnel protection ipsec profile oracle-vpn
```

```
! IP Routing
! Pick either dynamic (BGP) or static routing. Uncomment the corresponding commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you want to use BGP.

! router bgp ${bgpASN}
! neighbor ${OracleInsideTunnelIpAddress1} remote-as 31898
! neighbor ${OracleInsideTunnelIpAddress2} remote-as 31898
! network ${onPremCidrNetwork} mask ${onPremCidrNetmask}

! Static Route Configuration
! Uncomment below lines if you want to use static routing.
! ip route ${vcnCidrNetwork} ${vcnCidrNetmask} Tunnel${tunnelNumber1}
! ip route ${vcnCidrNetwork} ${vcnCidrNetmask} Tunnel${tunnelNumber2}

! Update Any Internet Facing Access List to Allow IPSec and ISAKMP Packets
! You may need to allow IPSec and ISAKMP packets out your internet facing interface.
! Uncomment below lines to create a new ACL allowing IPSec and ISAKMP traffic and apply it to the outside interface.

! ip access-list extended INTERNET-INGRESS
! permit udp host ${oracleHeadend1} host ${cpePublicIpAddress} eq isakmp
! permit esp host ${oracleHeadend1} host ${cpePublicIpAddress}
! permit udp host ${oracleHeadend2} host ${cpePublicIpAddress} eq isakmp
! permit esp host ${oracleHeadend2} host ${cpePublicIpAddress}
! permit icmp any any echo
! permit icmp any any echo-reply
! permit icmp any any unreachable

! interface ${outsideInterface}
! ip address ${cpePublicIpAddress} $(netmask)
! ip access-group INTERNET-INGRESS in
```

**IKEv2 Configuration Template**

```
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! IKEv2 Configuration Template
! The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template involves setting up the following:
! Keyring (Pre-Shared Key)
```
Networking

IKEv2 and IPSec Policy Configuration
IPSec Peers
Virtual Tunnel Interfaces
IP Routing (BGP or Static)
Update Any Internet Facing Access List to Allow IPSec and ISAKMP Packets

The configuration template has various parameters that you must define before applying the configuration.

PARAMETERS REFERENCED:
${OracleInsideTunnelIpAddress1} = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
${OracleInsideTunnelIpAddress2} = Inside tunnel IP address of Oracle-side for the second tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
${bgpASN} = Your BGP ASN
${cpePublicIpAddress} = The public IP address for the CPE. This is the IP address of your outside interface
${oracleHeadend1} = Oracle public IP endpoint obtained from the Oracle Console.
${oracleHeadend2} = Oracle public IP endpoint obtained from the Oracle Console.
${sharedSecret1} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
${sharedSecret2} = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
${outsideInterface} = The public interface or outside of tunnel interface which is configured with the CPE public IP address.
${vcnCidrNetwork} = VCN IP range
${vcnCidrNetmask} = Subnet mask for VCN
${onPremCidrNetwork} = On-premises IP range
${onPremCidrNetmask} = ON-premises subnet mask

Keyring (Pre-Shared Key)

For authentication during IKE a separate keyring is defined for each Oracle VPN Headend peer.
Add the pre-shared key for each Oracle VPN headend under the corresponding keyring.

crypto ikev2 keyring oracle-vpn-\${oracleHeadend1}
peer oracle_vpn
  address \${oracleHeadend1}
  pre-shared-key local \${sharedSecret1}
  pre-shared-key remote \${sharedSecret1}

crypto ikev2 keyring oracle-vpn-\${oracleHeadend2}
peer oracle_vpn
  address \${oracleHeadend2}
  pre-shared-key local \${sharedSecret2}
  pre-shared-key remote \${sharedSecret2}

Optional IPSec settings are included here.
All optional settings included are recommended by Oracle. Remove or comment out any unneeded commands prior to applying this configuration.
WARNING: These settings are global and may impact other IPSec connections

The Router will clear the DF-bit in the IP header. Allows the packet to be fragmented and sent to the end host in Oracle Cloud Infrastructure for reassembly.
crypto ipsec df-bit clear

Oracle Cloud Infrastructure User Guide
! Increases security association anti-replay window. An increased window size is helpful for scenarios where packets are regularly being dropped due to delays.
crypto ipsec security-association replay window-size 128

! IKEv2 and IPSec Policy Configuration

! An IKEv2 proposal is created and specifies use of a Pre-Shared Key, AES256, SHA384, and Diffie-Hellman Group 5.
! If different parameters are required, modify this template before applying the configuration.
crypto ikev2 proposal oracle_v2_proposal
  encryption aes-cbc-256
  integrity sha384
  group 5
crypto ikev2 policy oracle_v2_policy
  proposal oracle_v2_proposal

! Create an IPSec transform set named 'oracle-vpn-transform' which defines a combination of IPSec (Phase 2) policy options. Specifically, AES256 for encryption and SHA1 for authentication. This is also where tunnel mode is set for IPSec.
! If different parameters are required, modify this template before applying the configuration.
crypto ipsec transform-set oracle-vpn-transform esp-aes 256 esp-sha-hmac
  mode tunnel

! An IPSec profile named 'oracle_v2_ipsec_profile_tunnel#' is created for each tunnel.
! The previously created transform set is added to this policy along with settings for enabling PFS Group 5 and the security association lifetime to 3600 seconds (1 hour).
! If different parameters are required, modify this template before applying the configuration.
crypto ipsec profile oracle_v2_ipsec_profile_tunnel1
  set ikev2-profile oracle_v2_profile_tunnel1
  set pfs group5
  set security-association lifetime seconds 3600
  set transform-set oracle-vpn-transform
crypto ipsec profile oracle_v2_ipsec_profile_tunnel2
  set ikev2-profile oracle_v2_profile_tunnel2
  set pfs group5
  set security-association lifetime seconds 3600
  set transform-set oracle-vpn-transform

! IPSec Peers

! Two IKEv2 profiles are created for each Oracle VPN Headend.
crypto ikev2 profile oracle-vpn-$(oracleHeadend1)
  keyring oracle-vpn-$(oracleHeadend1)
  identity local address ${cpePublicIpAddress}
  match identity remote address ${oracleHeadend1} 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
crypto ikev2 profile oracle-vpn-$(oracleHeadend2)
keyring oracle-vpn-$(oracleHeadend2)
identity local address ${cpePublicIpAddress}
match identity remote address $(oracleHeadend2) 255.255.255.255
authentication remote pre-share
authentication local pre-share

! Virtual Tunnel Interfaces

! Each tunnel interface is a logical interface representing the local end
of a VPN tunnel to a remote VPN peer. Each tunnel interface represents a
single tunnel to a different Oracle VPN Headend. The IP address of each
VPN headend is provided when you create your IPSec connection in Oracle
Console.
! Each tunnel interface configuration also references the previously created
IPSec profile 'oracle-vpn' for its IPSec parameters.
! WARNING: When doing static routing you do NOT have to set IPs on the
tunnel interfaces unless you have pre-configured inside tunnel interfaces
in Oracle Console when creating your IPSec connection. Inside tunnel
interfaces are required if using BGP.

interface Tunnel${tunnelNumber1}
ip address ${cpeInsideTunnelIpAddress1} ${cpeInsideTunnelNetmask1}
tunnel source ${cpePublicIpAddress}
tunnel mode ipsec ipv4
tunnel destination ${oracleHeadend1}
tunnel protection ipsec profile oracle_v2_ipsec_profile_tunnel1

interface Tunnel${tunnelNumber2}
ip address ${cpeInsideTunnelIpAddress2} ${cpeInsideTunnelNetmask2}
tunnel source ${cpePublicIpAddress}
tunnel mode ipsec ipv4
tunnel destination ${oracleHeadend2}
tunnel protection ipsec profile oracle_v2_ipsec_profile_tunnel2

! IP Routing
! Pick either dynamic (BGP) or static routing. Uncomment the corresponding
commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you want to use BGP.

! router bgp ${bgpASN}
  ! neighbor ${OracleInsideTunnelIpAddress1} remote-as 31898
  ! neighbor ${OracleInsideTunnelIpAddress2} remote-as 31898
  ! network ${onPremCidrNetwork} mask ${onPremCidrNetmask}

! Static Route Configuration
! Uncomment below lines if you want to use static routing.
! ip route ${vcnCidrNetwork} ${vcnCidrNetmask} Tunnel${tunnelNumber1}
! ip route ${vcnCidrNetwork} ${vcnCidrNetmask} Tunnel${tunnelNumber2}

! Update Any Internet Facing Access List to Allow IPSec and ISAKMP Packets
! You may need to allow IPSec and ISAKMP packets out your internet facing
interface.
! Uncomment below lines to create a new ACL allowing IPSec and ISAKMP
traffic and apply it to the outside interface.

! ip access-list extended INTERNET-INGRESS
  ! permit udp host $(oracleHeadend1) host ${cpePublicIpAddress} eq isakmp
  ! permit esp host $(oracleHeadend1) host ${cpePublicIpAddress}
  ! permit udp host $(oracleHeadend2) host ${cpePublicIpAddress} eq isakmp
Networking

! permit esp host ${oracleHeadend2} host ${cpePublicIpAddress}
! permit icmp any any echo
! permit icmp any any echo-reply
! permit icmp any any unreachable

! interface ${outsideInterface}
! ip address ${cpePublicIpAddress} $(netmask)
! ip access-group INTERNET-INGRESS in

**Verification**

The following IOS commands are included for basic troubleshooting.

Use the following command to verify that ISAKMP security associations are being built between the two peers.

```bash
show crypto isakmp sa
```

Use the following command to verify the status of all your BGP connections or neighbors.

```bash
show ip bgp summary
show ip bgp neighbors
```

Use the following command to verify the route table.

```bash
show ip route
```

A **Monitoring service** is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see **VPN Connect Metrics** on page 3164.

If you have issues, see **VPN Connect Troubleshooting** on page 3166.

**FortiGate**

This topic provides configuration for a FortiGate that is running software version 6.0.4.

FortiGate experience is recommended. For more details on how to use FortiGate products, visit their official site. For FortiGate documentation for high availability (HA) or manual deployment, see the **Fortinet Document Library**.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.</td>
</tr>
</tbody>
</table>

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor’s documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you’re already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor’s documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are for example purposes only.
Networking

Best Practices

This section covers general best practices and considerations for using VPN Connect.

Configure All Tunnels for Every IPSec Connection

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

Have Redundant CPEs in Your On-Premises Network Locations

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

Routing Protocol Considerations

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
- **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

Other Important CPE Configurations

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.
Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels:** Also called next-hop-based tunnels. A route table lookup is performed on a packet's destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.
- **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR
Networking

blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

Important:

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

• VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
• Policy-based routing is not available in all ADs. The release notes list available ADs.
• Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
• The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
• An encryption domain must always be between two CIDR blocks of the same IP version.

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's private IP address, as show in the following diagram.
**Note:**

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

**Supported IPSec Parameters**

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

**CPE Configuration**

**Important:**

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

By default, FortiGate provisions the IPSec tunnel in route-based mode. This topic focuses on FortiGate with a route-based VPN configuration.

If necessary, you can have FortiGate provision the IPSec tunnel in policy-based mode. To enable the feature, go to System, and then to Feature Visibility. Under Additional Features, enable the Policy-based IPsec VPN feature.
About Using IKEv2

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

If you want to use IKEv2, there’s a variation on one of the tasks presented in the next section. Specifically, in task 2, when configuring authentication, select IKE version 2.

Configuration Process

**Important:*******

Before starting, ensure you have a valid license or trial license to configure FortiGate.

Task 1: Use the wizard to create the VPN

1. Go to VPN, and then to **IPsec Wizard** to create a new VPN tunnel.
2. On the **VPN Creation Wizard** page, specify the following items:
   - **Name:** Description used to identify the IPSec tunnel. Avoid entering confidential information.
   - **Template Type:** Site to Site
   - **Remote Device Type:** Cisco
   - **NAT Configuration:** No NAT between sites

3. Click **Next**.

4. On the **Authentication** page, specify the following items:
   - **Remote Device:** IP Address
   - **IP Address:** IP address for the Oracle VPN headend. Oracle generated this value when creating the IPSec tunnel.
   - **Outgoing Interface:** The WAN interface configured for external traffic.
   - **Authentication Method:** Pre-shared Key. Oracle supports only shared secret keys.
   - **Pre-shared Key:** The shared secret. Oracle generated this value when creating the IPSec tunnel.

5. Click **Next**.

6. On the **Policy & Routing** page, specify the following items:
   - **Local Interface:** The LAN interface configured for internal traffic.
   - **Local Subnets:** The subnet used for internal traffic.
   - **Remote Subnets:** The Oracle VCN subnets that will be used for the IPSec tunnel.
   - **Internet Access:** None
7. Click Create.

A summary message is shown with details about the configuration. Notice that the wizard automatically creates security policies with the subnets that you specified and adds the required static routes.

![VPN Creation Wizard](image)

Task 2: Add Phase 1 and Phase 2 parameters to each IPSec tunnel

You must convert each newly created IPSec tunnel into a custom tunnel to add the recommended parameters for Phase 1 and Phase 2.

Perform the following steps for each tunnel.

1. Go to VPN, and then click IPsec Tunnels.
2. Select the tunnel and click Edit to view the Edit VPN Tunnel page.
3. Click **Convert to Custom Tunnel**.

![Networking Diagram]

- **ROI**: Remote Gateway: Static IP Address (129.213.6.50), Interface: port1
- **Authentication**
  - Authentication Method: Pre-shared Key
  - IKE Version: 1, Mode: Main (ID protection)
- **Phase 1 Proposal**
  - Algorithms: AES256-SHA384
  - Diffie-Hellman Group: 5
- **XAUTH**
  - Type: Disabled
- **Phase 2 Selectors**
  - Name | Local Address | Remote Address
  - OCI-DRG-CPE1 | OCI-DRG-CPE1_local | OCI-DRG-CPE1_remote
4. Edit the relevant sections to match the required settings shown in the following screenshots. Remember to click the check mark icon in the top-right corner of each section after making your changes.

The IP address shown in the first screenshot is an example address.

Notice that if you want to use IKEv2, on the Authentication screen, instead select IKE Version 2.
5. After configuring all sections, click **OK** to save and close the dialogs.

Task 3: Verify the IPSec connection

At this point, the IPSec tunnel will not be established by default because FortiGate uses the IP address assigned on the WAN interface. In this case, this IP address is a private IP address because Oracle does 1:1 NAT. This private IP address will be used as the local IKE ID and will not match the one expected on the Oracle DRG. To resolve this, you can manually change the local IKE ID on your FortiGate by using the CPE's CLI, or you can change the value that Oracle uses in the Oracle Console (see the instructions that follow). Either way, this fixes the incompatibility and brings up the IPSec tunnel.

To change the CPE IKE identifier that Oracle uses (Oracle Console)
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

   A list of the IPSec connections in the compartment that you’re viewing is displayed. If you don’t see the one you’re looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. For the IPSec connection you’re interested in, click the Actions icon (three dots), and then click Edit.

   The current CPE IKE identifier that Oracle is using is displayed at the bottom of the dialog.

3. Enter your new values for CPE IKE Identifier Type and CPE IKE Identifier, and then click Save Changes.

Redundancy with BGP Over IPSec

For redundancy, Oracle recommends using BGP over IPSec. By default, if you have two connections of the same type (for example, two IPSec VPNs that both use BGP), and you advertise the same routes across both connections, Oracle prefers the oldest established route when responding to requests or initiating connections. If you want to force routing to be symmetric, Oracle recommends using BGP and AS path prepending with your routes to influence which path Oracle uses when responding to and initiating connections. For more information, see Routing Details for Connections to Your On-Premises Network on page 2942.

The Oracle DRG uses /30 or /31 as subnets for configuring IP addresses on the interface tunnels. Remember that the IP address must be part of the IPSec VPN’s encryption domain and must be allowed in the firewall policy to reach the peer VPN through the interface tunnel. You might need to implement a static route through the tunnel interface for the peer IP address.

Oracle’s BGP ASN in commercial regions is 31898. If you’re configuring VPN Connect for the Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle’s BGP ASN on page 154.

For your side, you can use a private ASN. Private ASNs are in the range 64512–65534.

Task 1: Edit the tunnel interface

In the first task, you add the BGP IP address to the newly created FortiGate tunnel interface.

Perform the following steps for each tunnel.

1. Go to Network, and then Interface.

2. Select the interface you’re interested in and click Edit.

   ![FortiGate VM64-OPC Interface Configuration](image)

3. Configure the following items:
   - **IP**: Enter the BGP IP address that you assigned to the FortiGate end of the tunnel interface. The following screenshot shows an example value of 192.168.66.2.
   - **Remote IP/Network Mask**: Add the BGP IP address that you assigned to the Oracle end of the tunnel interface. Include either a /30 or /31 mask, depending on how you specified the addresses in the Oracle
Networking

Console. In the following screenshot, 192.168.66.0/30 was used, where 192.168.66.2 is assigned to the FortiGate end, and 192.168.66.1 is assigned to the Oracle end.

- **Ping access** (recommended): In the **Administrative Access** section, enable ping access.

![Edit Interface](image)

**Task 2: Add a static route for the Oracle IP address**

For each tunnel, add a /32 static route towards the Oracle IP address through the tunnel, as shown in the following screenshot.

![Static Routes](image)

**Task 3: Configure BGP**

Perform the following steps for each tunnel.

1. Go to **Network**, and then **BGP**.
2. Enter the following items:

- **Local AS**: Your BGP ASN. You can use a private ASN. Private ASNs are in the range 64512–65534.
- **Router ID**: A value to provide a unique identity for this BGP router among its peers.
- **Neighbors**: Click Create New and enter the BGP IP address for the Oracle end of the tunnel, and the Oracle BGP ASN (31898 for commercial regions). If you're configuring VPN Connect for connecting to the Government Cloud, see Oracle's BGP ASN on page 154.
- **Networks**: Optionally use this field to advertise a specific subnet over BGP. You can also advertise subnets by using the Redistribute section in the Advanced Options section.

3. Click OK.
**Verification**

The following CLI command is useful for gathering statistical data such as the number of packets encrypted versus decrypted, the number of bytes sent versus received, the encryption domain (SPI) identifier, and so on. This kind of information can be critical for determining an issue with the VPN.

```plaintext
diagnose vpn tunnel list
```

The following command indicates a lack of firewall policy, a lack of forwarding route, and policy ordering issues. If there are no communication issues, this command returns blank output.

```plaintext
diagnose debug flow
```

The following command verifies BGP neighbor status information. Remember that an "Active" state doesn't mean that the BGP session is up. "Active" refers to a BGP state message. For more information, see BGP Background and Concepts in the FortiGate documentation.

```plaintext
get router info bgp summary
```

The following command provides more detailed information about a BGP neighbor.

```plaintext
get router info bgp neighbors
```

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see VPN Connect Metrics on page 3164.

If you have issues, see VPN Connect Troubleshooting on page 3166.

**Furukawa Electric**

This configuration was validated using a Furukawa Electric series FITELnet-F220/F221 running Firmware 01.00(00) [0]00.00.0 [2019/07/05 15:00].

> **Important:**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec VPN connection. Even if you configure one tunnel as primary and another as backup, traffic from your VCN to your on-premises network can use any tunnel that is "up" on your device. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

**Before Starting**

Before configuring your CPE, ensure that you:

- Configure your internet provider settings.
- Configure firewall rules to open UDP port 500, UDP port 4500, and ESP.

**Supported Encryption Domain or Proxy ID**

The values for the encryption domain (also known as a proxy ID, security parameter index (SPI), or traffic selector) depend on whether your CPE supports route-based tunnels or policy-based tunnels. For more information about the correct encryption domain values to use, see Supported Encryption Domain or Proxy ID on page 2948.

**Parameters from API or Console**

Get the following parameters from the Oracle Cloud Infrastructure Console or API.

```plaintext
${vpn-ip#}
```

- Oracle VPN headend IPSec tunnel endpoints. There is one value for each tunnel.
- Example values: 129.146.12.52, 129.146.13.52
Networking

${sharedSecret#}
• The IPSec ISAKMP pre-shared-key. There is one value for each tunnel.
• Example value: EXAMPLEDPfAMkD7nTH3SWr6OFabdT6exXn6enSlsKbE

${cpePublicIpAddress}
• The public IP address for the CPE (previously made available to Oracle via the Console).

${VcnCidrBlock}
• When creating the VCN, your company selected this CIDR to represent the IP aggregate network for all VCN hosts.
• Example Value: 10.0.0.0/20

Parameters Based on Current CPE Configuration and State
The following parameters are based on your current CPE configuration.

${tunnelNumber#}
• An interface number to identify the specific tunnel. You need one unused unit number per tunnel.
• Example value: 1, 2

${isakmpPolicy}
• The ISAKMP policy name.
• Example value: isakmp-policy

${ipsecPolicy#}
• The IPSec policy name.
• Example value: ipsec-policy

${isakmpProfile#}
• The ISAKMP profile name. You need one unused ISAKMP profile name per tunnel.
• Example values: OCI-VPN-profile1, OCI-VPN-profile2

${selector}
• The selector name.
• Example value: OCI-VPN-selector

${map#}
• The map name. You need one unused map name per tunnel.
• Example values: OCI-VPN-MAP1, OCI-VPN-MAP2

${customer-bgp-asn}
• Your BGP ASN.
• Example value: 65000

${oracle-bgp-asn#}
• Oracle's BGP ASN.
• Example value: 31898

${customer-interface-ip#}
• The inside tunnel interface for CPE.
• Example value: 10.0.0.16/31

${oracle-interface-ip#}
• The inside tunnel interface for ORACLE.
• Example value: 10.0.0.17/31
$\{router-id\}

- The BGP router ID.
- Example value: 10.0.0.16

**Config Template Parameter Summary**

Each region has multiple Oracle IPSec headends. The following template allows you to set up multiple tunnels on your CPE, each to a corresponding headend. In the following table, "User" is you/your company.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Source</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>${vpn-ip1}</td>
<td>Console/API</td>
<td>129.146.12.52</td>
</tr>
<tr>
<td>${sharedSecret1}</td>
<td>Console/API</td>
<td>(long string)</td>
</tr>
<tr>
<td>${vpn-ip2}</td>
<td>Console/API</td>
<td>129.146.13.52</td>
</tr>
<tr>
<td>${sharedSecret2}</td>
<td>Console/API</td>
<td>(long string)</td>
</tr>
<tr>
<td>${cpePublicIpAddress}</td>
<td>User</td>
<td>203.0.113.1</td>
</tr>
<tr>
<td>${VcnCidrBlock}</td>
<td>User</td>
<td>10.0.0.0/20</td>
</tr>
<tr>
<td>${tunnelNumber1}</td>
<td>User</td>
<td>1</td>
</tr>
<tr>
<td>${tunnelNumber1}</td>
<td>User</td>
<td>2</td>
</tr>
<tr>
<td>${isakmpPolicy}</td>
<td>User</td>
<td>isakmp-policy</td>
</tr>
<tr>
<td>${ipsecPolicy}</td>
<td>User</td>
<td>ipsec-policy</td>
</tr>
<tr>
<td>${isakmpProfile1}</td>
<td>User</td>
<td>OCI-VPN-profile1</td>
</tr>
<tr>
<td>${isakmpProfile2}</td>
<td>User</td>
<td>OCI-VPN-profile2</td>
</tr>
<tr>
<td>${selector}</td>
<td>User</td>
<td>OCI-VPN-selector</td>
</tr>
<tr>
<td>${map1}</td>
<td>User</td>
<td>OCI-VPN-MAP1</td>
</tr>
<tr>
<td>${map2}</td>
<td>User</td>
<td>OCI-VPN-MAP2</td>
</tr>
<tr>
<td>${customer-bgp-asn}</td>
<td>Console/API/User</td>
<td>65000</td>
</tr>
<tr>
<td>${oracle-bgp-asn1}</td>
<td>Console/API</td>
<td>31898</td>
</tr>
<tr>
<td>${oracle-bgp-asn2}</td>
<td>Console/API</td>
<td>31898</td>
</tr>
<tr>
<td>${customer-interface-ip1}</td>
<td>Console/API/User</td>
<td>10.0.0.16/31</td>
</tr>
<tr>
<td>${customer-interface-ip2}</td>
<td>Console/API/User</td>
<td>10.0.0.18/31</td>
</tr>
<tr>
<td>${oracle-interface-ip1}</td>
<td>Console/API/User</td>
<td>10.0.0.17</td>
</tr>
<tr>
<td>${oracle-interface-ip2}</td>
<td>Console/API/User</td>
<td>10.0.0.19</td>
</tr>
<tr>
<td>${router-id}</td>
<td>User</td>
<td>10.0.0.16</td>
</tr>
</tbody>
</table>

**Important:**

The following ISAKMP and IPSec policy parameter values are applicable to VPN Connect in the commercial cloud. For the Government Cloud, you must use the values listed in Required VPN Connect Parameters for Government Cloud on page 152.
**Networking**

### ISAKMP Policy Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAKMP protocol version</td>
<td>Version 1</td>
</tr>
<tr>
<td>Exchange type</td>
<td>Main mode</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Pre-shared keys</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES-256-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>HMAC-SHA1-96</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>Group 5</td>
</tr>
<tr>
<td>IKE session key lifetime</td>
<td>28,800 seconds (8 hours)</td>
</tr>
</tbody>
</table>

### IPSec Policy Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec protocol</td>
<td>ESP, tunnel-mode</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES-CBC/256</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>HMAC-SHA1-96/160</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>Group 5</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>Enabled</td>
</tr>
<tr>
<td>IPSec session key lifetime</td>
<td>3600 seconds (1 hour)</td>
</tr>
</tbody>
</table>

### CPE Configuration

**ISAKMP and IPSec Configuration**

```
crypto ipsec policy ${ipsecPolicy}
    set pfs group5
    set security-association transform-keysize aes 256 256 256
    set security-association transform esp-aes esp-sha-hmac
exit
!
crypto ipsec selector ${selector}
    src 1 ipv4 any
    dst 1 ipv4 any
exit
!
crypto isakmp policy ${isakmpPolicy}
    authentication pre-share
    encryption aes
    encryption-keysize aes 256 256 256
    group 5
    hash sha
exit
!
crypto isakmp profile ${isakmpProfile1}
    local-address ${cpePublicIpAddress}
    set isakmp-policy ${isakmpPolicy}
    set ipsec-policy ${ipsecPolicy}
    set peer ${vpn-ip1}
    ike-version 1
    local-key ascii ${sharedSecret1}
exit
```
Networking

! crypto isakmp profile ${isakmpProfile2}
  local-address ${cpePublicIpAddress}
  set isakmp-policy ${isakmpPolicy}
  set ipsec-policy ${ipsecPolicy}
  set peer ${vpn-ip2}
  ike-version 1
  local-key ascii ${sharedSecret2}
exit
!
crypto map ${map1} ipsec-isakmp
  match address ${selector}
  set isakmp-profile ${isakmpProfile1}
exit
!
crypto map ${map2} ipsec-isakmp
  match address ${selector}
  set isakmp-profile ${isakmpProfile2}
exit
!
interface Tunnel ${tunnelNumber1}
  tunnel mode ipsec map ${map1}
  ip address ${customer-interface-ip1}
exit
!
interface Tunnel ${tunnelNumber2}
  tunnel mode ipsec map ${map2}
  ip address ${customer-interface-ip2}
exit

BGP Configuration

ip route ${vcnCidrBlock} Tunnel ${tunnelNumber1}
ip route ${vcnCidrBlock} Tunnel ${tunnelNumber2}

Static Routes Configuration

router bgp ${customer-bgp-asn}
  bgp router-id ${router-id}
  bgp log-neighbor-changes
  neighbor ${oracle-interface-ip1} ebgp-multihop 10
  neighbor ${oracle-interface-ip1} enforce-multihop
  neighbor ${oracle-interface-ip1} remote-as ${oracle-bgp-asn1}
  neighbor ${oracle-interface-ip1} update-source tunnel ${tunnelNumber1}
  neighbor ${oracle-interface-ip2} ebgp-multihop 10
  neighbor ${oracle-interface-ip2} enforce-multihop
  neighbor ${oracle-interface-ip2} remote-as ${oracle-bgp-asn2}
  neighbor ${oracle-interface-ip2} update-source tunnel ${tunnelNumber2}
!
  address-family ipv4 unicast
  redistribute connected
  exit

Juniper MX

This topic provides configuration for a Juniper MX that is running software version JunOS 15.0 (or newer).

Important:
Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.
If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor’s documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you’re already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor’s documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are for example purposes only.

**Best Practices**

This section covers general best practices and considerations for using VPN Connect.

**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

**Routing Protocol Considerations**

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
• **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see *Routing for the Oracle IPSec VPN* on page 2934.

**Other Important CPE Configurations**

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor’s support.

*Caveats and Limitations*

This section covers general important characteristics and limitations of VPN Connect to be aware of.

**Asymmetric Routing**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see *Routing for the Oracle IPSec VPN* on page 2934.

**Route-Based or Policy-Based IPSec VPN**

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

**Note:**

Other vendors or industry documentation might use the term *proxy ID*, *security parameter index (SPI)*, or *traffic selector* when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

• **Route-based tunnels**: Also called *next-hop-based tunnels*. A route table lookup is performed on a packet's destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

• **Policy-based tunnels**: The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.
Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

**Encryption domain for policy-based tunnels**

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an *encryption domain*.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

**Important:**

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

**If Your CPE Is Behind a NAT Device**

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's *public* IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's *private* IP address, as shown in the following diagram.
Note:
Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Supported IPSec Parameters
For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

CPE Configuration

Important:
The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

The configuration template provided is for a Juniper MX router running JunOS 15.0 (or newer). The template provides information for each tunnel that you must configure. Oracle recommends setting up all configured tunnels for maximum redundancy.
The configuration template refers to these items that you must provide:

- **CPE public IP address:** The internet-routable IP address that is assigned to the external interface on the CPE. You or your Oracle administrator provides this value to Oracle when creating the CPE object in the Oracle Console.

- **Inside tunnel interface (required if using BGP):** The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these values when creating the IPSec connection in the Oracle Console.

- **BGP ASN (required if using BGP):** Your BGP ASN.

In addition, you must:

- Configure the Juniper MX public interface (the CPE public IP address is bound to this interface).
- Configure internal routing that routes traffic between the CPE and your local network.
- Configure the tunnel interfaces. See the next section for more information.

### About the Tunnel Interfaces

In the following configuration template, the tunnel interfaces are referred to with the following variables:

- **msInterface#** - one per tunnel
  - These interfaces correspond to one of the four encryption ASICs on the MS-MPC card.
  - You can distribute load across the ASICs by spreading your tunnels across them.
  - Example values: ms-2/3/0, ms-2/3/1
- **insideMsUnit#** and **outsideMsUnit#** - one pair per tunnel
  - For every tunnel, you need an ms-mpc interface pair of units.
  - One represents the outside of the IPSec tunnel. The other represents the inside of the tunnel.
  - The router forwards packets from your on-premises network to your VCN into the inside unit.
    - The encryption ASIC then encrypts the packets based on the rules and policies.
    - Then the encrypted packet egresses out the outside unit as an ESP packet, ready to be forwarded to the Oracle VPN headend routers.
  - There are over 16,000 possible values for unit numbers.
    - One way to allocate the units is to offset them by 8,000.
    - You can pick values between 0 - 7999 for insideMsUnit# and 8000-15999 for outsideMsUnit#.

**Important:**

This following configuration template from Oracle Cloud Infrastructure is a starting point for what you need to apply to your CPE. Some of the parameters referenced in the template must be unique on the CPE, and the uniqueness can only be determined by accessing the CPE. Ensure the parameters are valid on your CPE and do not overwrite any previously configured values. In particular, ensure these values are unique:

- Policy names or numbers
- Interface names
- Access list numbers (if applicable)

To find parameters that you must define before applying the configuration, search for the keyword USER_DEFINED in the template.

### About Using IKEv2

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see [Supported IPSec Parameters](#) on page 2945.
You specify the IKE version when defining the IKE policy. In the following configuration, there's a comment showing how to configure the IKE policy for IKEv1 versus IKEv2.

**Configuration Template**

```bash
# Configuration Template
# The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.

# The configuration template involves setting up the following:
# PHASE 1
# PHASE 2
# SETTING THE TUNNEL INTERFACES FOR ORACLE
# SETTING THE SERVICES FOR ORACLE.
# SETTING BGP/STATIC ROUTING
# SETTING ROUTING-INSTANCES FOR ORACLE (OPTIONAL).

# The configuration template has various parameters that you must define before applying the configuration.
# Search in the template for the keyword "USER_DEFINED" to find those parameters.

# PARAMETERS REFERENCED:
# oracle_headend_1 = Oracle public IP endpoint obtained from the Oracle Console.
# oracle_headend_2 = Oracle public IP endpoint obtained from the Oracle Console.
# connection_presharedkey_1 = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
# connection_presharedkey_2 = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
# cpe_public_ip_address = The internet-routable IP address that is assigned to the public interface on the CPE. You provide this when creating the CPE object in the Oracle Console.
# cpe_public_interface = The name of the Juniper interface where the CPE IP address is configured. Eg: ge-0/0/1.0
# msInterface1 = The interface correspond to one of the four encryption ASICs on the MS-MPC card. Eg: ms-2/3/0, ms-2/3/1
# msInterface2 = Second tunnel interface that needs to be configured. Eg: ms-2/3/0, ms-2/3/1
# insideMsUnit1 = The inside interface of the MS-MPC interface pair for tunnel_1
# insideMsUnit2 = The inside interface of the MS-MPC interface pair for tunnel_2
# outsideMsUnit1 = The outside interface of the MS-MPC interface pair for tunnel_1
# outsideMsUnit2 = The outside interface of the MS-MPC interface pair for tunnel_2
# inside_tunnel_interface_ip_address = The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these when creating the IPSec connection in the Oracle Console.
# inside_tunnel_interface_ip_address_neighbor = The neighbor IP address between the MX and Oracle end points of the inside tunnel interface.
# bgp_asn = Your ASN
# vcn_range = VCN IP Range

# OPTIONAL PARAMETERS:
# customer_on-prem_to_oracle = Name of the routing instance to be defined on the CPE for the tunnel interfaces connecting to the Oracle headends.
```
Networking

# internet_routing_instance = Name of the routing instance to be defined on the CPE for the tunnel interfaces that are connected to the Internet.

# IPSec Tunnel 1

# #1: Internet Key Exchange (IKE) Configuration (Phase 1)
# Defining the IKE Proposal for Oracle
# This IKE (Phase 1) configuration template uses AES256, SHA384, Diffie-Hellman Group 5, and 28800 second (8 hours) IKE session key lifetime.
# If different parameters are required, modify this template before applying the configuration.

set services ipsec-vpn ike proposal oracle-ike-proposal authentication-method pre-shared-keys
set services ipsec-vpn ike proposal oracle-ike-proposal authentication-algorithm sha-384
set services ipsec-vpn ike proposal oracle-ike-proposal encryption-algorithm aes-256-cbc
set services ipsec-vpn ike proposal oracle-ike-proposal lifetime-seconds 28800
set services ipsec-vpn ike proposal oracle-ike-proposal dh-group group5

# Defining the IKE Policy for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# If using IKEv1, uncomment the following two lines, and comment out the line after (the line with "version 2" at the end)
# set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 mode main
# set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 version 1

set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 version 2
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 proposals oracle-ike-proposal
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 local-id ipv4_addr <cpe_public_ip_address>
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 remote-id ipv4_addr <oracle_headend_1>
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_1 pre-shared-key ascii-text <connection_presharedkey_1>

# Setting up Public Interface with the CPE Public IP.
# USER_DEFINED: Replace the parameters in the section below as needed

set interfaces <cpe_public_interface> unit 0 family inet address <cpe_public_ip_address>

# #2: IPSec Configuration

# Defining the IPSec (Phase 2) Proposal for Oracle
# The IPSec proposal defines the protocol, authentication, encryption, and lifetime parameters for the IPsec security association.
# The configuration template sets AES256 for encryption, SHA256 for authentication, enables PFS group 14, and sets the IPSec session key lifetime to 3600 seconds (1 hour).
# The IPsec policy incorporates the Diffie-Hellman group and the IPsec proposal.
# If different parameters are required, modify this template before applying the configuration.

set services ipsec-vpn ipsec proposal oracle-ipsec-proposal
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal protocol esp
Networking

set services ipsec-vpn ipsec proposal oracle-ipsec-proposal authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal encryption-algorithm aes-256-cbc
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal lifetime-seconds 3600

# Defining the IPSec (PHASE 2) policy for Oracle
set services ipsec-vpn ipsec policy oracle-ipsec-policy perfect-forward-secrecy keys group14
set services ipsec-vpn ipsec policy oracle-ipsec-policy proposals oracle-ipsec-proposal

# Defining Security Association for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed.
# The IKE and IPSec policies are associated with the tunnel interface. Eg: ms-2/3/0.101
# The IPsec Dead Peer Detection option causes periodic messages to be sent to ensure a Security Association remains operational.

set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 from ipsec-inside-interface <msInterface1>.<insideMsUnit1>
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then remote-gateway <oracle_headend_1>
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then dynamic ike-policy oracle-ike-policy-tunnel_1
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then dynamic ipsec-policy oracle-ipsec-policy
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then tunnel-mtu 1430
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then initiate-dead-peer-detection
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then dead-peer-detection
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then dead-peer-detection interval 5
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 then dead-peer-detection threshold 4
set services ipsec-vpn rule oracle-vpn-tunnel_1 term 1 match-direction input

# #3: Tunnel Interface Configuration

# Defining the Tunnel Interfaces
# USER_DEFINED: Replace the parameters in the section below as needed.

set interfaces <msInterface1> unit <insideMsUnit1> description oracle-vpn-tunnel-1-INSIDE
set interfaces <msInterface1> unit <insideMsUnit1> family inet
    address <inside_tunnel_interface_ip_address>
set interfaces <msInterface1> unit <insideMsUnit1> service-domain inside

set interfaces <msInterface1> unit <outsideMsUnit1> description oracle-vpn-tunnel-1-OUTSIDE
set interfaces <msInterface1> unit <outsideMsUnit1> family inet
set interfaces <msInterface1> unit <outsideMsUnit1> service-domain outside

# #4: Service Set Configuration

# USER_DEFINED: Replace the parameters in the section below as needed
# Service set configuration to direct traffic to the tunnel interfaces and associating the appropriate IPSec-VPN-Rule.
set services service-set oracle-vpn-tunnel_1 next-hop-service inside-service-interface <msInterface1>,<insideMsUnit1>
set services service-set oracle-vpn-tunnel_1 next-hop-service outside-service-interface <msInterface1>,<outsideMsUnit1>
set services service-set oracle-vpn-tunnel_1 ipsec-vpn-options local-gateway <cpe_public_ip_address>
set services service-set oracle-vpn-tunnel_1 ipsec-vpn-rules oracle-vpn-tunnel-tunnel_1

# This option causes the router to reduce the Maximum Segment Size of TCP packets to prevent packet fragmentation.
set services service-set oracle-vpn-tunnel_1 tcp-mss 1387

# #5a: Border Gateway Protocol (BGP) Configuration

# USER_DEFINED: Replace the parameters in the section below as needed

# BGP is used within the tunnel to exchange prefixes between the Dynamic Routing Gateway and your CPE. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
# The configuration template uses a basic route policy to advertise a default route to the DRG.
# To advertise additional prefixes to the Oracle VCN, add additional prefixes to the term ORACLE-DEFAULT policy. Make sure the prefix is present in the routing table of the device with a valid next-hop.

# You configure the local BGP Autonomous System Number (BGP ASN) when you set up the IPSec connection in the Oracle Console. If you later need to change the ASN, you must recreate the CPE object and IPSec connection in the Oracle Console.

set policy-options policy-statement ORACLE-DEFAULT term default from route-filter 0.0.0.0/0 exact
set policy-options policy-statement ORACLE-DEFAULT term default then accept
set policy-options policy-statement ORACLE-DEFAULT term reject then reject
set protocols bgp group ebgp type external
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> export ORACLE-DEFAULT
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> peer-as 31898
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> local-as <bgp_asn>

# #5b: Static Route Configuration

# USER_DEFINED: Replace the parameters in the section below as needed
# In case you plan to use static routing to get traffic through the IPSec tunnels, you can point the routes down to the tunnel interfaces. You should redistribute these routes into your on-premises network. Configuration for CPE to VCN static routes:

set routing-options static route <vcn_range> next-hop <msInterface1>,<insideMsUnit1>

##6: Routing Instances Configuration (Optional)
# USER_DEFINED: Replace the parameters in the section below as needed.
# If you are using routing-instances on your CPE, you need to make sure you account for them in your configuration. Merge the following configuration into the template provided above.

```
set routing-instances <customer_on-prem_to_oracle>
    interface <msInterface1>.<insideMsUnit1>
set routing-instances <internet_routing_instance> interface <msInterface1>.<outsideMsUnit1>
set services service-set oracle-vpn-tunnel-tunnel_1 ipsec-vpn-options local-gateway <cpe_public_ip_address> routing-instance <internet_routing_instance>
```

# IPSec Tunnel 2

# #1: Internet Key Exchange (IKE) Configuration (Phase 1)

# Defining the IKE Proposal for Oracle
# This IKE (Phase 1) configuration template uses AES256, SHA384, Diffie-Hellman Group 5, and 28800 second (8 hours) IKE session key lifetime.
# If different parameters are required, modify this template before applying the configuration.

```
set services ipsec-vpn ike proposal oracle-ike-proposal authentication-method pre-shared-keys
set services ipsec-vpn ike proposal oracle-ike-proposal authentication-algorithm sha-384
set services ipsec-vpn ike proposal oracle-ike-proposal encryption-algorithm aes-256-cbc
set services ipsec-vpn ike proposal oracle-ike-proposal lifetime-seconds 28800
set services ipsec-vpn ike proposal oracle-ike-proposal dh-group group5
```

# Defining the IKE Policy for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# If using IKEv1, uncomment the following two lines, and comment out the line after (the line with "version 2" at the end)
# set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 mode main
# set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 version 1

```
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 version 2
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 version 1
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 proposals oracle-ike-proposal
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 local-id ipv4_addr <cpe_public_ip_address>
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 remote-id ipv4_addr <oracle_headend_2>
set services ipsec-vpn ike policy oracle-ike-policy-tunnel_2 pre-shared-key ascii-text <connection_presharedkey_2>
```

# Setting up Public Interface with the CPE Public IP.
# USER_DEFINED: Replace the parameters in the section below as needed

```
set interfaces <cpe_public_interface> unit 0 family inet address <cpe_public_ip_address>
```

# #2: IPSec Configuration

# Defining the IPSec (Phase 2) Proposal for Oracle
# The IPSec proposal defines the protocol, authentication, encryption, and lifetime parameters for the IPsec security association.
Networking

# The configuration template sets AES256 for encryption, SHA256 for authentication, enables PFS group 14, and sets the IPSec session key lifetime to 3600 seconds (1 hour).
# The IPsec policy incorporates the Diffie-Hellman group and the IPsec proposal.
# If different parameters are required, modify this template before applying the configuration.

```bash
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal protocol esp
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal encryption-algorithm aes-256-cbc
set services ipsec-vpn ipsec proposal oracle-ipsec-proposal lifetime-seconds 3600

# Defining the IPSec (PHASE 2) policy for Oracle

set services ipsec-vpn ipsec policy oracle-ipsec-policy perfect-forward-secrecy keys group14
set services ipsec-vpn ipsec policy oracle-ipsec-policy proposals oracle-ipsec-proposal

# Defining Security Association for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# The IKE and IPSEC policies are associated with the tunnel interface. Eg: ms-2/3/0.101
# The IPsec Dead Peer Detection option causes periodic messages to be sent to ensure a Security Association remains operational.

set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 from ipsec-inside-interface <msInterface2>.<insideMsUnit2>
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then remote-gateway <oracle_headend_2>
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then dynamic ike-policy oracle-ike-policy-tunnel_2
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then dynamic ipsec-policy oracle-ipsec-policy
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then tunnel-mtu 1420
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then initiate-dead-peer-detection
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then dead-peer-detection
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then dead-peer-detection interval 5
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then dead-peer-detection threshold 4
set services ipsec-vpn rule oracle-vpn-tunnel_2 term 1 then match-direction input

# #3: Tunnel Interface Configuration

# Defining the Tunnel Interfaces
# USER_DEFINED: Replace the parameters in the section below as needed.

set interfaces <msInterface2> unit <insideMsUnit2> description oracle-vpn-tunnel-2-INSIDE
set interfaces <msInterface2> unit <insideMsUnit2> family inet address <inside_tunnel_interface_ip_address>
set interfaces <msInterface2> unit <outsideMsUnit2> service-domain inside

set interfaces <msInterface2> unit <outsideMsUnit2> description oracle-vpn-tunnel-2-OUTSIDE
```

Oracle Cloud Infrastructure User Guide
Networking

set interfaces <msInterface2> unit <outsideMsUnit2> family inet
set interfaces <msInterface2> unit <outsideMsUnit2> service-domain outside

# #4: Service Set Configuration

# USER_DEFINED: Replace the parameters in the section below as needed
# Service set configuration to direct traffic to the tunnel interfaces and
# associating the appropriate IPSec-VPN-Rule.

set services service-set oracle-vpn-tunnel_2 next-hop-service inside-
service-interface <msInterface2>.<insideMsUnit2>
set services service-set oracle-vpn-tunnel_2 next-hop-service outside-
service-interface <msInterface2>.<outsideMsUnit2>
set services service-set oracle-vpn-tunnel_2 ipsec-vpn-options local-
gateway <cpe_public_ip_address>
set services service-set oracle-vpn-tunnel_2 ipsec-vpn-rules oracle-vpn-
tunnel-tunnel_2

# This option causes the router to reduce the Maximum Segment Size of TCP
# packets to prevent packet fragmentation.

set services service-set oracle-vpn_tunnel_1 tcp-mss 1387

# #5a: Border Gateway Protocol (BGP) Configuration

# USER_DEFINED: Replace the parameters in the section below as needed

# BGP is used within the tunnel to exchange prefixes between the dynamic
# routing gateway and your CPE. The DRG dynamically learns the routes from
# your on-premises network. On the Oracle side, the DRG advertises the VCN's
# subnets.
# The configuration templates uses a basic route policy to advertise a
default route to the DRG.
# To advertise additional prefixes to the Oracle VCN, add additional
prefixes to the term ORACLE-DEFAULT policy. Make sure the prefix is present
in the routing table of the device with a valid next-hop.

# You configure the local BGP Autonomous System Number (BGP ASN) when you
set up the IPsec connection in the Oracle Console. If you later need to
change the ASN, you must recreate the CPE object and IPsec connection in
the Oracle Console.

set policy-options policy-statement ORACLE-DEFAULT term default from route-
filter 0.0.0.0/0 exact
set policy-options policy-statement ORACLE-DEFAULT term default then accept
set policy-options policy-statement ORACLE-DEFAULT term reject then reject
set protocols bgp group ebgp type external
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> export ORACLE-
DEFAULT
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> peer-as 31898
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> local-as <bgp_asn>

# #5b: Static Route Configuration

# USER_DEFINED: Replace the parameters in the section below as needed
# In case you plan to use static routing to get traffic through the IPSec
tunnels, you can point the routes down to the tunnel interfaces. You should
redistribute these routes into your on-premises network. Configuration for CPE to VCN static routes:

```
set routing-options static route <vcn_range> next-hop <msInterface2>.<insideMsUnit2>
```

## 6: Routing Instances Configuration (Optional)

### USER_DEFINED: Replace the parameters in the section below as needed.

If you are using routing-instances on your CPE, you need to make sure you account for them in your configuration. Merge the following configuration into the template provided above.

```
set routing-instances <customer_on-prem_to_oracle>
  interface <msInterface2>.<insideMsUnit2>
set routing-instances <internet_routing_instance>
  interface <msInterface2>.<outsideMsUnit2>
set services service-set oracle-vpn-tunnel-tunnel_2 ipsec-vpn-options local-gateway <cpe_public_ip_address> routing-instance <internet_routing_instance>
```

**Verification**

Use the following command to verify security associations (SAs).

```
show services ipsec-vpn ipsec security-associations detail
```

Use the following command to check the BGP status.

```
show bgp summary
```

Use the following commands to check the routes advertised to and received from Oracle Cloud Infrastructure. If you’ve configured the CPE to use routing instances, use the commands with `table <table-name>` at the end.

```
show route advertising-protocol bgp <neighbor-address>
show route receive-protocol bgp <neighbor-address>
show route advertising-protocol bgp <neighbor-address> table <table-name>
show route receive-protocol bgp <neighbor-address> table <table-name>
```

A **Monitoring service** is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see [VPN Connect Metrics](#) on page 3164.

If you have issues, see [VPN Connect Troubleshooting](#) on page 3166.

**Juniper SRX**

This topic provides configuration for a Juniper SRX that is running software version JunOS 11.0 (or newer).

**Important:**

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor’s documentation and make any necessary adjustments.
If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are for example purposes only.

![Diagram of IPSec connection to Oracle Cloud Infrastructure](image)

**Best Practices**

This section covers general best practices and considerations for using VPN Connect.

**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

**Routing Protocol Considerations**

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing:** The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
- **Static routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.
Other Important CPE Configurations

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels**: Also called *next-hop-based tunnels*. A route table lookup is performed on a packet’s destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

- **Policy-based tunnels**: The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address**: Any (0.0.0.0/0)
- **Destination IP address**: Any (0.0.0.0/0)
- **Protocol**: IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.
Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

---

Important:

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can’t overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

---

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE’s private IP address, as show in the following diagram.
Note:
Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as cpe.example.com. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Supported IPSec Parameters
For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

CPE Configuration

Important:
The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

The configuration template provided is for a Juniper SRX router running JunOS 11.0 software (or later). The template provides information for each tunnel that you must configure. Oracle recommends setting up all configured tunnels for maximum redundancy.
The configuration template refers to these items that you must provide:

- **CPE public IP address**: The internet-routable IP address that is assigned to the external interface on the CPE. You or your Oracle administrator provides this value to Oracle when creating the CPE object in the Oracle Console.

- **Inside tunnel interface (required if using BGP)**: The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these values when creating the IPSec connection in the Oracle Console.

- **BGP ASN (required if using BGP)**: Your BGP ASN.

In addition, you must:

- Configure the outside tunnel interface (the CPE public IP address is bound to this interface).
- Configure the tunnel interface IDs (referred to as st0.1 and st0.2 in the following configuration template). You need multiple tunnel unit numbers per IPSec connection.
- Configure internal routing that routes traffic between the CPE and your local network.
- Identify the security zone for the outside interface (the following configuration template references this zone as `internet_untrust`).
- Identify the security zone for the inside interface (the following configuration template references this zone as `oracle_trust`).
- Identify the security zone for the tunnel interface (the following configuration template references this zone as `oracle_vpn`).

### Important:

This following configuration template from Oracle Cloud Infrastructure is a starting point for what you need to apply to your CPE. Some of the parameters referenced in the template must be unique on the CPE, and the uniqueness can only be determined by accessing the CPE. Ensure the parameters are valid on your CPE and do not overwrite any previously configured values. In particular, ensure these values are unique:

- Policy names or numbers
- Interface names
- Access list numbers (if applicable)

To find parameters that you must define before applying the configuration, search for the keyword `USER_DEFINED` in the template.

### About Using IKEv2

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

You specify the IKE version when defining the IKE gateway. In the following configuration, there's a comment showing how to configure the IKE gateway for IKEv1 versus IKEv2.

### Configuration Template

```bash
# Configuration Template
# The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.

# The configuration template involves setting up the following:
# PHASE 1
# PHASE 2
# SETTING THE SECURITY ZONES FOR ORACLE
# SETTING THE SECURITY POLICIES FOR ORACLE
```
# SETTING THE SECURITY SETTING FOR ORACLE

# SETTING BGP/STATIC ROUTING

# The configuration template has various parameters that you must define before applying the configuration.
# Search in the template for the keyword "USER_DEFINED" to find those parameters.

# PARAMETERS REFERENCED:
# oracle_headend_1 = Oracle public IP endpoint obtained from the Oracle Console.
# oracle_headend_2 = Oracle public IP endpoint obtained from the Oracle Console.
# connection_presharedkey_1 = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
# connection_presharedkey_2 = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
# outside_public_interface = The public interface or outside of tunnel interface which is configured with the CPE public IP address. Example: ge-0/0/1.0
# cpe_public_ip_address = The internet-routable IP address that is assigned to the public interface on the CPE. You provide this when creating the CPE object in the Oracle Console.
# inside_tunnel_interface = The internal-facing interface for the on-premises network behind the SRX that needs to reach the Oracle VCN. Example: ge-0/0/0.0
# inside_tunnel_interface_ip_address = The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these when creating the IPSec connection in the Oracle Console.
# inside_tunnel_interface_ip_address_neighbor = The neighbor IP address between the SRX and Oracle end points of the inside tunnel interface.
# internal_network_ip_range = Internal on-premise network behind the SRX that needs to reach resources in the Oracle VCN.
# bgp_asn = Your ASN
# vcn_range = VCN IP Range

# IPSec Tunnel 1
# #1: Internet Key Exchange (IKE) Configuration (Phase 1)
# Defining the IKE Proposal for Oracle
# This IKE (Phase 1) configuration template uses AES256, SHA384, Diffie-Hellman Group 5, and 28800 second (8 hours) IKE session key lifetime.
# If different parameters are required, modify this template before applying the configuration.

set security ike proposal oracle-ike-proposal authentication-method pre-shared-keys
set security ike proposal oracle-ike-proposal authentication-algorithm sha-384
set security ike proposal oracle-ike-proposal encryption-algorithm aes-256-cbc
set security ike proposal oracle-ike-proposal lifetime-seconds 28800
set security ike proposal oracle-ike-proposal dh-group group5

# Defining the IKE Policy for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed

set security ike policy ike_pol_oracle-vpn-<oracle_headend_1> mode main
set security ike policy ike_pol_oracle-vpn-<oracle_headend_1> proposals oracle-ike-proposal
set security ike policy ike_pol_oracle-vpn-<oracle_headend_1> pre-shared-key ascii-text <connection_presharedkey_1>

# Setting up Public Interface with the CPE Public IP.
# USER_DEFINED: Replace the parameters in the section below as needed
set interfaces <outside_public_interface> unit 0 family inet
   address <cpe_public_ip_address>

# Defining the IKE Gateway for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed.
# This option enables IPsec Dead Peer Detection, which causes periodic messages to be sent to ensure a Security Association remains operational.
# If you want to use IKEv1 instead, comment out the line below that ends with "version v2-only".

set security ike gateway gw_oracle-<oracle_headend_1> ike-policy
   ike_pol_oracle-vpn-<oracle_headend_1>
set security ike gateway gw_oracle-<oracle_headend_1> external-interface <outside_public_interface>
set security ike gateway gw_oracle-<oracle_headend_1> address <oracle_headend_1>
set security ike gateway gw_oracle-<oracle_headend_1> dead-peer-detection
set security ike gateway gw_oracle-<oracle_headend_1> version v2-only
set security ike gateway gw_oracle-<oracle_headend_1> local-identity inet <cpe_public_ip_address>

# #2: IPSec Configuration

# Defining the IPsec (Phase 2) Proposal for Oracle
# The IPsec proposal defines the protocol, authentication, encryption, and lifetime parameters for the IPsec security association.
# The configuration template sets AES256 for encryption, SHA1 for authentication, enables PFS group 5, and sets the IPsec session key lifetime to 3600 seconds (1 hour).
# The IPsec policy incorporates the Diffie-Hellman group and the IPsec proposal.
# If different parameters are required, modify this template before applying the configuration.

set security ipsec vpn-monitor-options
set security ipsec proposal oracle-ipsec-proposal protocol esp
set security ipsec proposal oracle-ipsec-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal oracle-ipsec-proposal encryption-algorithm aes-256-cbc
set security ipsec proposal oracle-ipsec-proposal lifetime-seconds 3600

# Defining the IPsec (PHASE 2) policy for Oracle
set security ipsec policy ipsec_pol_oracle-vpn perfect-forward-secrecy keys group5
set security ipsec policy ipsec_pol_oracle-vpn proposals oracle-ipsec-proposal

# Defining Security Association for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# The IPsec Policy and IKE gateways are associated with a tunnel interface (st0.1). If other tunnels are defined on your router, you must specify a unique interface name (for example, st0.2).
# The df-bit clear option allows the SRX to fragment the packet and send it to the end host in Oracle Cloud Infrastructure to reassemble the packet.

set security ipsec vpn oracle-vpn-<oracle_headend_1> bind-interface st0.1
set security ipsec vpn oracle-vpn-<oracle_headend_1> vpn-monitor
set security ipsec vpn oracle-vpn-<oracle_headend_1> ike gateway
gw_oracle-<oracle_headend_1>
set security ipsec vpn oracle-vpn-<oracle_headend_1> ike ipsec-policy
ipsec_pol_oracle-vpn
set security ipsec vpn oracle-vpn-<oracle_headend_1> df-bit clear
set security ipsec vpn establish-tunnels immediately

# #3: Tunnel Interface Configuration

# Defining the Tunnel Interface
# USER_DEFINED: Replace the parameters in the section below as needed

set interfaces st0.1 family inet
   address <inside_tunnel_interface_ip_address>
set interfaces st0.1 family inet mtu 1430
set interfaces <inside_tunnel_interface> unit 0 family inet
   address <internal_network_ip_range>

# Setting the Security Zones for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# Tunnel interface st0.1, inside_tunnel_interface and
outside_public_interface are each defined in its own security zones.

set security zones security-zone oracle_vpn interfaces st0.1
set security zones security-zone oracle_trust
   interfaces <inside_tunnel_interface>
set security zones security-zone internet_untrust
   interfaces <outside_public_interface>

# The security zone protecting outside interface of the router must be
configured to allow IKE and ping inbound traffic.

set security zones security-zone internet_untrust
   interfaces <outside_public_interface> host-inbound-traffic system-services
      ike
set security zones security-zone internet_untrust
   interfaces <outside_public_interface> host-inbound-traffic system-services
      ping

# The security zone protecting the logical tunnel interface must be
configured to allow BGP inbound traffic.

set security zones security-zone oracle_vpn interfaces st0.1
   host-inbound-traffic protocols bgp

# This option causes the router to reduce the Maximum Segment Size of TCP
packets to prevent packet fragmentation.

set security flow tcp-mss ipsec-vpn mss 1387

# #4: Policies

# Setting the Security Policies for Oracle
# Policies basically define the permitted flow of traffic between defined
security zones.
# The configuration template permits any ipv4 traffic sourced and destined
between security zones oracle_trust and oracle_vpn.

set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-
   out match source-address any-ipv4
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-
   out match destination-address any-ipv4
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-
   out match application any
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out match source-identity any
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out then permit

# #5a: Border Gateway Protocol (BGP) Configuration

# USER_DEFINED: Replace the parameters in the section below as needed

# BGP is used within the tunnel to exchange prefixes between the dynamic routing gateway and your CPE. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
# The configuration template uses a basic route policy to advertise a default route to the DRG.
# To advertise additional prefixes to the Oracle VCN, add additional prefixes to the term ORACLE-DEFAULT policy. Make sure the prefix is present in the routing table of the device with a valid next-hop.

# You configure the local BGP Autonomous System Number (BGP ASN) when you set up the IPSec connection in the Oracle Console. If you later need to change the ASN, you must recreate the CPE object and IPSec connection in the Oracle Console.

set policy-options policy-statement ORACLE-DEFAULT term default from route-filter 0.0.0.0/0 exact
set policy-options policy-statement ORACLE-DEFAULT term default then accept
set policy-options policy-statement ORACLE-DEFAULT term reject then reject
set protocols bgp group ebgp type external
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> export ORACLE-DEFAULT
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> peer-as 31898
set protocols bgp group ebgp
neighbor <inside_tunnel_interface_ip_address_neighbor> local-as <bgp_asn>

# #5b: Static Route Configuration

# USER_DEFINED: Replace the parameters in the section below as needed
# In case you plan to use static routing to get traffic through the IPSec tunnels, you can point the routes down to the tunnel interfaces. You should redistribute these routes into your on-premises network. Configuration for CPE to VCN static routes:

set routing-options static route <vcn_range> next-hop st0.1

# IPSec Tunnel 2

# #1: Internet Key Exchange (IKE) Configuration (Phase 1)
# Defining the IKE Proposal for Oracle
# This IKE (Phase 1) configuration template uses AES256, SHA384, Diffie-Hellman Group 5, and 28800 second (8 hours) IKE session key lifetime.
# If different parameters are required, modify this template before applying the configuration.
set security ike proposal oracle-ike-proposal authentication-method pre-shared-keys
set security ike proposal oracle-ike-proposal authentication-algorithm sha-384
set security ike proposal oracle-ike-proposal encryption-algorithm aes-256-cbc
set security ike proposal oracle-ike-proposal lifetime-seconds 28800
set security ike proposal oracle-ike-proposal dh-group group5

# Defining the IKE Policy for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed

set security ike policy ike_pol_oracle-vpn-<oracle_headend_2> mode main
set security ike policy ike_pol_oracle-vpn-<oracle_headend_2> proposals oracle-ike-proposal
set security ike policy ike_pol_oracle-vpn-<oracle_headend_2> pre-shared-key ascii-text "connection_presharedkey_2"

# Setting up Public Interface with the CPE Public IP.
# USER_DEFINED: Replace the parameters in the section below as needed

set interfaces <outside_public_interface> unit 0 family inet
    address <cpe_public_ip_address>

# Defining the IKE Gateway for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed.
# This option enables IPsec Dead Peer Detection, which causes periodic messages to be sent to ensure a Security Association remains operational.
# If you want to use IKEv1 instead, comment out the line below that ends with "version v2-only".

set security ike gateway gw_oracle-<oracle_headend_2> ike-policy ike_pol_oracle-vpn-<oracle_headend_2>
set security ike gateway gw_oracle-<oracle_headend_2> external-interface <outside_public_interface>
set security ike gateway gw_oracle-<oracle_headend_2> address <oracle_headend_2>
set security ike gateway gw_oracle-<oracle_headend_2> dead-peer-detection
set security ike gateway gw_oracle-<oracle_headend_2> version v2-only
set security ike gateway gw_oracle-<oracle_headend_2> local-identity inet <cpe_public_ip_address>

# Defining the IPSec (PHASE 2) policy for Oracle
# The IPSec policy incorporates the Diffie-Hellman group and the IPSec proposal.
# If different parameters are required, modify this template before applying the configuration.

set security ipsec vpn-monitor-options
set security ipsec proposal oracle-ipsec-proposal protocol esp
set security ipsec proposal oracle-ipsec-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal oracle-ipsec-proposal encryption-algorithm aes-256-cbc
set security ipsec proposal oracle-ipsec-proposal lifetime-seconds 3600

# Defining the IPSec (PHASE 2) policy for Oracle
# Defining Security Association for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# The IPSec Policy and IKE gateways are associated with a tunnel interface (st0.2). If other tunnels are defined on your router, you must specify a unique interface name.
# The df-bit clear option allows the SRX to fragment the packet and send it to the end host in Oracle Cloud Infrastructure to reassemble the packet.

```plaintext
set security ipsec policy ipsec_pol_oracle-vpn perfect-forward-secrecy keys group5
set security ipsec policy ipsec_pol_oracle-vpn proposals oracle-ipsec-proposal
```

# #3: Tunnel Interface Configuration

# Defining the Tunnel Interface
# USER_DEFINED: Replace the parameters in the section below as needed

```plaintext
set interfaces st0.2 family inet
  address <inside_tunnel_interface_ip_address>
set interfaces st0.2 family inet mtu 1430
set interfaces <inside_tunnel_interface> unit 0 family inet
  address <internal_network_ip_range>
```

# Setting the Security Zones for Oracle
# USER_DEFINED: Replace the parameters in the section below as needed
# Tunnel interface st0.2, inside_tunnel_interface and outside_public_interface are each defined in its own security zones.

```plaintext
set security zones security-zone oracle_vpn interfaces st0.2
set security zones security-zone oracle_trust
  interfaces <inside_tunnel_interface>
set security zones security-zone internet_untrust
  interfaces <outside_public_interface>
```

# The security zone protecting outside interface of the router must be configured to allow IKE and ping inbound traffic.

```plaintext
set security zones security-zone internet_untrust
  interfaces <outside_public_interface> host-inbound-traffic system-services
  ike
set security zones security-zone internet_untrust
  interfaces <outside_public_interface> host-inbound-traffic system-services
  ping
```

# The security zone protecting the logical tunnel interface must be configured to allow BGP inbound traffic.

```plaintext
set security zones security-zone internet_untrust
  interfaces <outside_public_interface> host-inbound-traffic protocols bgp
```

# This option causes the router to reduce the Maximum Segment Size of TCP packets to prevent packet fragmentation.

```plaintext
set security flow tcp-mss ipsec-vpn mss 1387
```
# #4: Policies

# Setting the Security Policies for Oracle
# Policies basically define the permitted flow of traffic between defined
# security zones.
# The configuration template permits any IPv4 traffic sourced and destined
# between security zones oracle_trust and oracle_vpn.

```
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out match source-address any-ipv4
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out match destination-address any-ipv4
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out match application any
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out match source-identity any
set security policies from-zone oracle_trust to-zone oracle_vpn policy vpn-out then permit
```

# #5a: Border Gateway Protocol (BGP) Configuration

# USER_DEFINED: Replace the parameters in the section below as needed

# BGP is used within the tunnel to exchange prefixes between the dynamic
# routing gateway and your CPE. The DRG dynamically learns the routes from
# your on-premises network. On the Oracle side, the DRG advertises the VCN's
# subnets.
# The configuration template uses a basic route policy to advertise a
default route to the DRG.
# To advertise additional prefixes to the Oracle VCN, add additional
# prefixes to the term ORACLE-DEFAULT policy. Make sure the prefix is present
# in the routing table of the device with a valid next-hop.

```
set policy-options policy-statement ORACLE-DEFAULT term default from route-filter 0.0.0.0/0 exact
set policy-options policy-statement ORACLE-DEFAULT term default then accept
set policy-options policy-statement ORACLE-DEFAULT term reject then reject
set protocols bgp group ebgp type external
set protocols bgp group ebgp
   neighbor <inside_tunnel_interface_ip_address_neighbor> export ORACLE-DEFAULT
set protocols bgp group ebgp
   neighbor <inside_tunnel_interface_ip_address_neighbor> peer-as 31898
set protocols bgp group ebgp
   neighbor <inside_tunnel_interface_ip_address_neighbor> local-as <bgp_asn>
```

# #5b: Static Route Configuration

# USER_DEFINED: Replace the parameters in the section below as needed
# In case you plan to use static routing to get traffic through the IPSec
# tunnels, you can point the routes down to the tunnel interfaces. You should
# redistribute these routes into your on-premises network. Configuration for
# CPE to VCN static routes:
set routing-options static route <vcn_range> next-hop st0.2

**Verification**

Use the following command to verify security associations (SAs).

`show security ipsec security-associations`

Use the following command to check the BGP status.

`show bgp summary`

Use the following commands to check the routes advertised to and received from Oracle Cloud Infrastructure.

`show route advertising-protocol bgp <neighbor-address>`
`show route receive-protocol bgp <neighbor-address>`

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see VPN Connect Metrics on page 3164.

If you have issues, see VPN Connect Troubleshooting on page 3166.

**Libreswan**

Libreswan is an open source IPSec implementation that is based on FreeS/WAN and Openswan. Most Linux distributions include Libreswan or make it easy to install. You can install it on hosts in either your on-premises network or a cloud provider network. For an example of setting up a Libreswan host in another cloud provider to connect to your Oracle Cloud Infrastructure virtual cloud network (VCN), see Access to Other Clouds with Libreswan on page 3310.

This topic provides configuration for CPE that is running Libreswan. Virtual tunnel interface (VTI) support for this route-based configuration requires minimum Libreswan version 3.18 and a recent Linux 3.x or 4.x kernel. This configuration was validated using Libreswan version 3.29.

**Important:**

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are an example only.
Networking

Best Practices

This section covers general best practices and considerations for using VPN Connect.

Configure All Tunnels for Every IPSec Connection

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

Have Redundant CPEs in Your On-Premises Network Locations

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

Routing Protocol Considerations

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing:** The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
- **Static routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

Other Important CPE Configurations

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.
Networking

Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

Note:

Other vendors or industry documentation might use the term proxy ID, security parameter index (SPI), or traffic selector when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels:** Also called next-hop-based tunnels. A route table lookup is performed on a packet's destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

- **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR
blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

**Important:**

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can’t overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

**If Your CPE Is Behind a NAT Device**

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE’s public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE’s private IP address, as show in the following diagram.
Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Supported IPSec Parameters

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

CPE Configuration

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

Default Libreswan Configuration Files

The default Libreswan installation creates the following files:

- `etc/ipsec.conf`: The root of the Libreswan configuration.
- `/etc/ipsec.secrets`: The root of the location where Libreswan looks for secrets (the tunnel pre-shared keys).
- `/etc/ipsec.d/`: A directory for storing the `.conf` and `.secrets` files for your Oracle Cloud Infrastructure tunnels (for example: `oci-ipsec.conf` and `oci-ipsec.secrets`). Libreswan encourages you to create these files in this folder.

The default `etc/ipsec.conf` file includes this line:

```plaintext
include /etc/ipsec.d/* .conf
```
Networking

The default etc/ipsec.secrets file includes this line:

```
include /etc/ipsec.d/*.secrets
```

The preceding lines automatically merge all the .conf and .secrets files in the /etc/ipsec.d directory into the main configuration and secrets files that Libreswan uses.

About Using IKEv2

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

You specify the IKE version when setting up the IPSec configuration file in task 3 in the next section. In that example file, there’s a comment showing how to configure IKEv1 versus IKEv2.

Configuration Process

Libreswan supports both route-based and policy-based tunnels. The tunnel types can coexist without interfering with each other. The Oracle VPN headends use route-based tunnels. Oracle recommends that you configure Libreswan with the Virtual Tunnel Interface (VTI) configuration syntax.

For details about the specific parameters used in this document, see Supported IPSec Parameters on page 2945.

Task 1: Prepare the Libreswan instance

Depending on the Linux distribution you're using, you might need to enable IP forwarding on your interface to allow clients to send and receive traffic through Libreswan. In the /etc/sysctl.conf file, set the following values and apply the updates with sudo sysctl -p.

If you're using an interface other than eth0, change eth0 in the following example to your interface (lines 5 and 7).

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.eth0.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
```

Task 2: Determine the required configuration values

The Libreswan configuration uses the following variables. Determine the values before proceeding with the configuration.

- `${cpeLocalIP}`: The IP address of your Libreswan device.
- `${cpePublicIpAddress}`: The public IP address for Libreswan. This is the IP address of your outside interface. Depending on your network topology, the value might be different from `${cpeLocalIP}`.
- `${oracleHeadend1}`: For the first tunnel, the Oracle public IP endpoint obtained from the Oracle Console.
- `${oracleHeadend2}`: For the second tunnel, the Oracle public IP endpoint obtained from the Oracle Console.
- `${vti1}`: The name of the first VTI used. For example, vti1.
- `${vti2}`: The name of the second VTI used. For example, vti2.
- `${sharedSecret1}`: The pre-shared key for the first tunnel. You can use the default Oracle-provided pre-shared key, or provide your own when you set up the IPSec connection in the Oracle Console.
- `${sharedSecret2}`: The pre-shared key for the second tunnel. You can use the default Oracle-provided pre-shared key, or provide your own when you set up the IPSec connection in the Oracle Console.
- `${vcnCidrNetwork}`: The VCN IP range.

Task 3: Set up the configuration file: /etc/ipsec.d/oci-ipsec.conf
Networking

Libreswan configuration uses the concept of left and right to define the configuration parameters for your local CPE device and the remote gateway. Either side of the connection (the conn in the Libreswan configuration) can be left or right, but the configuration for that connection must be consistent. In this example:

- **left**: Your local Libreswan CPE
- **right**: The Oracle VPN headend

Use the following template for your /etc/ipsec.d/oci-ipsec.conf file. The file defines the two tunnels that Oracle creates when you set up the IPSec connection.

```plaintext
conn oracle-tunnel-1
left=${cpeLocalIP}
    # leftid=${cpePublicIpAddress} # See preceding note about 1-1 NAT device
right=${oracleHeadend1}
authby=secret
leftsubnet=0.0.0.0/0
rightsubnet=0.0.0.0/0
auto=start
mark=5/0xffffffff # Needs to be unique across all tunnels
vti-interface=${vti1}
vti-routing=no
ikev2=no # To use IKEv2, change to ikev2=insist
ike=aes_cbc256-sha2_384;modp1536
phase2alg=aes_gcm256;modp1536
encapsulation=yes
ike_lifetime=28800s
salifetime=3600s

conn oracle-tunnel-2
left=${cpeLocalIP}
    # leftid=${cpePublicIpAddress} # See preceding note about 1-1 NAT device
right=${oracleHeadend2}
authby=secret
leftsubnet=0.0.0.0/0
rightsubnet=0.0.0.0/0
auto=start
mark=6/0xffffffff # Needs to be unique across all tunnels
vti-interface=${vti2}
vti-routing=no
ikev2=no # To use IKEv2, change to ikev2=insist
ike=aes_cbc256-sha2_384;modp1536
phase2alg=aes_gcm256;modp1536
encapsulation=yes
ike_lifetime=28800s
salifetime=3600s
```

Task 4: Set up the secrets file: /etc/ipsec.d/oci-ipsec.secrets

Use the following template for your /etc/ipsec.d/oci-ipsec.secrets file. It contains two lines per IPSec connection (one line per tunnel).

```plaintext
${cpePublicIpAddress} ${oracleHeadend1}: PSK "${sharedSecret1}"
${cpePublicIpAddress} ${oracleHeadend2}: PSK "${sharedSecret2}"
```

Task 5: Restart the Libreswan configuration

After setting up your configuration and secrets files, you must restart the Libreswan service.
Networking

**Important:**

Restarting the Libreswan service may impact existing tunnels.

The following command rereads the config file and restarts the Libreswan service.

```
service ipsec restart
```

Task 6: Configure IP routing

Use the following `ip` command to create static routes that send traffic to your VCN through the IPSec tunnels. If you're logged in with an unprivileged user account, you might need to use `sudo` before the command.

**Important:**

Static routes created with the `ip route` command do not persist through a reboot. To determine how to make your routes persist, refer to the documentation of your Linux distribution of choice.

```
ip route add ${VcnCidrBlock} nexthop dev ${vti1} nexthop dev ${vti2}
ip route show
```

**Verification**

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see [VPN Connect Metrics](#) on page 3164.

If you have issues, see [VPN Connect Troubleshooting](#) on page 3166.

**Checking the Libreswan Status**

Check the current state of your Libreswan tunnels by using the following command.

```
ipsec status
```

The tunnel is established if you see a line that includes the following:

```
STATE_MAIN_I4: ISAKMP SA established
```

If you're using IKEv2, you see the following:

```
STATE_V2_IPSEC_I (IPsec SA established)
```

In the future, if you need to open a support ticket with Oracle about your Libreswan tunnel, include the output of the preceding `ipsec status` command.

**Checking the Tunnel Interface Status**

Check if the virtual tunnel interfaces are up or down by using the `ifconfig` command or the `ip link show` command. You can also use applications such as `tcpdump` with the interfaces.

Here's an example of the `ifconfig` output with a working Libreswan implementation that shows the available VTIs.

```
ifconfig
<output trimmed>
vti01: flags=209<UP,POINTOPOINT,RUNNING,NOARP> mtu 8980
    inet6 fe80::5efe:a00:2 prefixlen 64 scopeid 0x20<link>
tunnel txqueuelen 1000 (IPIP Tunnel)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
```
Here's an example of the `ip link show` output:

```bash
ip link show
<output trimmed>
9: vti01@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 8980 qdisc noqueue
   state UNKNOWN mode DEFAULT group default qlen 1000
   link/ipip 10.0.0.2 peer 129.213.240.52
10: vti02@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 8980 qdisc noqueue
   state UNKNOWN mode DEFAULT group default qlen 1000
   link/ipip 10.0.0.2 peer 129.213.240.51
```

Also, in the Oracle Console, each IPSec tunnel should now be in the UP state.

**NEC IX Series**

This topic provides a route-based IPSec VPN configuration for NEC IX Series devices. This configuration was validated using an IX3315 running Firmware Ver.10.2.16 and IX2106 running Firmware Ver.10.2.16.

**Important:**

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. The IP addresses in this diagram are examples only and not for literal use.
Networking

Best Practices
This section covers general best practices and considerations for using VPN Connect.

Configure All Tunnels for Every IPSec Connection
Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two headends are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

Have Redundant CPEs in Your On-Premises Network Locations
Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

Routing Protocol Considerations
When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
- **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

Other Important CPE Configurations
Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.


Caveats and Limitations

This section covers general important characteristics and limitations of VPN Connect to be aware of.

Asymmetric Routing

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

Note:

Other vendors or industry documentation might use the term proxy ID, security parameter index (SPI), or traffic selector when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels:** Also called next-hop-based tunnels. A route table lookup is performed on a packet's destination IP address. If that route's egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.
- **Policy-based tunnels:** The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address:** Any (0.0.0.0/0)
- **Destination IP address:** Any (0.0.0.0/0)
- **Protocol:** IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR
Networking blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.

**Important:**

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can't overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

**If Your CPE Is Behind a NAT Device**

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE's public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE's private IP address, as shown in the following diagram.
Networking

**Note:**

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as `cpe.example.com`. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

**Supported IPSec Parameters**

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

**CPE Configuration**

**Important:**

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

The configuration template provided is for an IX3315 running Firmware Ver.10.2.16 or IX2106 running Firmware Ver.10.2.16 software (or later). The template provides information for each tunnel that you must configure. Oracle recommends setting up all configured tunnels for maximum redundancy.

The configuration template refers to these items that you must provide:

- **CPE public IP address:** The internet-routable IP address that is assigned to the external interface on the CPE. You or your Oracle administrator provides this value to Oracle when creating the CPE object in the Oracle Console.
- **Inside tunnel interface (required if using BGP):** The IP addresses for the CPE and Oracle ends of the inside tunnel interface. You provide these values when creating the IPSec connection in the Oracle Console.
- **BGP ASN (required if using BGP):** Your BGP ASN.

In addition, you must:

- Configure internal routing for traffic between the CPE and your local network.
- Ensure that you permit traffic between your NEC IX Series and your Oracle VCN.
- Identify the IKE policy used (the following configuration template references this IKE policy as `$<ikePolicy1>` and `$<ikePolicy2>`).
• Identify the IPSec policy used (the following configuration template references this IPSec policy as $<ipsecPolicy1>$ and $<ipsecPolicy2>$).
• Identify the virtual tunnel interface names used (the following configuration template references these as variables $<tunnelInterfaceNumber1>$ and $<tunnelInterfaceNumber2>$).

Important:
This following configuration template from Oracle Cloud Infrastructure is a starting point for what you need to apply to your CPE. Some of the parameters referenced in the template must be unique on the CPE, and the uniqueness can only be determined by accessing the CPE. Ensure the parameters are valid on your CPE and do not overwrite any previously configured values. In particular, ensure these values are unique:

• Policy names or numbers
• Interface names
• Access list numbers (if applicable)

To find parameters that you must define before applying the configuration, search for the keyword USER_DEFINED in the template.

About Using IKEv2
Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

You specify the IKE version when defining the IKE gateway. In the following configuration, there's a comment showing how to configure the IKE gateway for IKEv1 versus IKEv2.

IKEv1 Configuration Template

!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! IKEv1 Configuration Template
! The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------

! The configuration template involves setting up the following:
! Configure ISAKMPv1 and IPSec Policies
! Configure Keepalive Setting of ICMP
! Configure Virtual Tunnel Interfaces
! IP Routing (BGP or Static)

!-------------------------------------------------------------------------------------------------------------------------------------------------------------

! The configuration template has various parameters that you must define before applying the configuration.

!-------------------------------------------------------------------------------------------------------------------------------------------------------------

! PARAMETERS REFERENCED:
! $<OracleHeadendIpAddress1>$ = Oracle public IP endpoint obtained from the Oracle Console.
! $<OracleHeadendIpAddress2>$ = Oracle public IP endpoint obtained from the Oracle Console.
! $<sharedSecret1>$ = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
! $<sharedSecret2>$ = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
! $<cpePublicIpAddress>$ = The public IP address for the CPE. This is the IP address of your outside interface.
! $<vcnCidrBlock>$ = VCN CIDR block. For example, 10.0.0.0/20.
! $<tunnelInterfaceNumber1>$ = The number of your tunnel interface for the first tunnel. For example, 1.
! $<tunnelInterfaceNumber2> = The number of your tunnel interface for the second tunnel. For example, 2.
! $<ikePolicy1> = The name of your IKE Policy. For example, ike-policy1.
! $<ikePolicy2> = The name of your IKE Policy. For example, ike-policy2.
! $<ipsecPolicy1> = The name of your IPSec Policy. For example, ipsec-policy1.
! $<ipsecPolicy2> = The name of your IPSec Policy. For example, ipsec-policy2.
! $<lanInterfaceNumber> = The number of your LAN interface. For example, 1.0.
! $<lanIpAddress> = The IP address of the LAN interface for your CPE.
! $<OracleInsideTunnelIpAddress1> = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
! $<OracleInsideTunnelIpAddress2> = Inside tunnel IP address of Oracle-side for the second tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
! $<cpeInsideTunnelIpAddress1> = The CPE's inside tunnel IP for the first tunnel.
! $<cpeInsideTunnelIpAddress2> = The CPE's inside tunnel IP for the second tunnel.
! $<bgpASN> = Your BGP ASN.

! Configure ISAKMPv1 and IPSec Policies

    ip access-list sec-list permit ip src any dest any
    ike nat-traversal
    ike proposal ike-prop encryption aes-256 hash sha2-256 group 1536-bit
    ike policy $<ikePolicy1> peer $<OracleHeadendIpAddress1> key $<sharedSecret1>
    ike policy $<ikePolicy2> peer $<OracleHeadendIpAddress2> key $<sharedSecret2>

    ipsec autokey-proposal ipsec-prop esp-aes-256 esp-sha lifetime time 3600
    ipsec autokey-map $<ipsecPolicy1> sec-list peer $<OracleHeadendIpAddress1>
    ipsec-prop pfs 1536-bit
    ipsec autokey-map $<ipsecPolicy2> sec-list peer $<OracleHeadendIpAddress2>
    ipsec-prop pfs 1536-bit

! Configure Keepalive Setting of ICMP

    watch-group watch_tunnel1 10
    event 20 ip unreach-host $<lanIpAddress> Tunnel$<tunnelInterfaceNumber1>
    source GigaEthernet$<lanInterfaceNumber>
    action 10 ip shutdown-route $<vcnCidrBlock> Tunnel $<tunnelInterfaceNumber1>
    action 20 ipsec clear-sa Tunnel$<tunnelInterfaceNumber1>

    network-monitor watch_tunnel1 enable

    watch-group watch_tunnel2 10
    event 20 ip unreach-host $<lanIpAddress> Tunnel$<tunnelInterfaceNumber2>
    source GigaEthernet$<lanInterfaceNumber>
    action 10 ip shutdown-route $<vcnCidrBlock> Tunnel $<tunnelInterfaceNumber2>
    action 20 ipsec clear-sa Tunnel$<tunnelInterfaceNumber2>

    network-monitor watch_tunnel2 enable

! Configure Virtual Tunnel Interfaces

    interface Tunnel$<tunnelInterfaceNumber1>
    tunnel mode ipsec
Networking

```
ip address $<cpeInsideTunnelIpAddress1>
ip tcp adjust-mss auto
ipsec policy tunnel ipsec-policy1 out
no shutdown

interface Tunnel$<tunnelInterfaceNumber2>
tunnel mode ipsec
ip address $<cpeInsideTunnelIpAddress2>
ip tcp adjust-mss auto
ipsec policy tunnel ipsec-policy2 out
no shutdown

! IP Routing
! Select dynamic (BGP) or static routing. Uncomment the corresponding
commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you select BGP.

! ip ufs-cache enable cache

! route-map pri1 permit 10
! set metric 5
! set local-preference 200

! route-map pri2 permit 10
! set metric 10
! set local-preference 150

! router bgp $<bgpASN>
! neighbor $<OracleInsideTunnelIpAddress1> remote-as 31898
! neighbor $<OracleInsideTunnelIpAddress1> timers 10 30
! neighbor $<OracleInsideTunnelIpAddress2> remote-as 31898
! neighbor $<OracleInsideTunnelIpAddress2> timers 10 30
! address-family ipv4 unicast
! neighbor $<OracleInsideTunnelIpAddress1> route-map pri1 in
! neighbor $<OracleInsideTunnelIpAddress1> route-map pri1 out
! neighbor $<OracleInsideTunnelIpAddress2> route-map pri2 in
! neighbor $<OracleInsideTunnelIpAddress2> route-map pri2 out
! network 192.168.100.0/24

! Static Route Configuration
! Uncomment below lines if you select static routing.

! ip ufs-cache enable
! ip route $<vcnCidrBlock> Tunnel0.0
! ip route $<vcnCidrBlock> Tunnel1.0

IKEv2 Configuration Template

!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! IKEv2 Configuration Template
! The configuration consists of two IPSec tunnels. Oracle highly recommends that you configure both tunnels for maximum redundancy.
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
! The configuration template involves setting up the following:
! Keyring (Pre-Shared Key)
! Configure ISAKMP and IPSec Policies
! Configure Virtual Tunnel Interfaces
! IP Routing (BGP or Static)
!-------------------------------------------------------------------------------------------------------------------------------------------------------------
```
The configuration template has various parameters that you must define before applying the configuration.

**PARAMETERS REFERENCED:**

- $<OracleHeadendIpAddress1>$ = Oracle public IP endpoint obtained from the Oracle Console.
- $<OracleHeadendIpAddress2>$ = Oracle public IP endpoint obtained from the Oracle Console.
- $<sharedSecret1>$ = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
- $<sharedSecret2>$ = You provide when you set up the IPSec connection in the Oracle Console, or you can use the default Oracle-provided value.
- $<cpePublicIpAddress>$ = The public IP address for the CPE. This is the IP address of your outside interface.
- $<vcnCidrBlock>$ = VCN CIDR block. For example, 10.0.0.0/20.
- $<tunnelInterfaceNumber1>$ = The number of your tunnel interface for the first tunnel. For example, 1.
- $<tunnelInterfaceNumber2>$ = The number of your tunnel interface for the second tunnel. For example, 2.
- $<lanInterfaceNumber>$ = The number of your LAN interface. For example, 1.0.
- $<wanInterfaceNumber>$ = The WAN interface or outside of tunnel interface which is configured with the CPE public IP address. For example, 0.1.
- $<OracleInsideTunnelIpAddress1>$ = Inside tunnel IP address of Oracle-side for the first tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
- $<OracleInsideTunnelIpAddress2>$ = Inside tunnel IP address of Oracle-side for the second tunnel. You provide these values when creating the IPSec connection in the Oracle Console.
- $<cpeInsideTunnelIpAddress1>$ = The CPE's inside tunnel IP for the first tunnel.
- $<cpeInsideTunnelIpAddress2>$ = The CPE's inside tunnel IP for the second tunnel.
- $<bgpASN>$ = Your BGP ASN.

**Keyring (Pre-Shared Key)**

For authentication during IKE a separate keyring is defined for each Oracle VPN Headend peer.

Add the pre-shared key for each Oracle VPN headend under the corresponding keyring.

```bash
ikev2 authentication psk id ipv4 $<OracleHeadendIpAddress1> key char $<sharedSecret1>
ikev2 authentication psk id ipv4 $<OracleHeadendIpAddress2> key char $<sharedSecret2>
```

Configure ISAKMP and IPSec Policies

```bash
ikev2 default-profile
dpd interval 10
source-address GigaEthernet$<wanInterfaceNumber>
child-pfs 1536-bit
child-proposal enc aes-cbc-256
child-proposal integrity sha1
sa-proposal enc aes-cbc-256
sa-proposal integrity sha2-384
sa-proposal dh 1536-bit
```

Configure Virtual Tunnel Interfaces

```bash
interface Tunnel$<tunnelInterfaceNumber1>
tunnel mode ipsec-iKEv2
ip address $<cpeInsideTunnelIpAddress1>
```
Networking

```
ip tcp adjust-mss auto
ikey2 connect-type auto
ikey2 ipsec pre-fragment
ikey2 outgoing-interface GigaEthernet<$wanInterfaceNumber>
ikey2 peer $<OracleHeadendIpAddress1> authentication psk id ipv4
$<OracleHeadendIpAddress1>
n0 shutdown

interface Tunnel<$tunnelInterfaceNumber2>
tunnel mode ipsec-ikey2
ip address $<cpeInsideTunnelIpAddress2>
ip tcp adjust-mss auto
ikey2 connect-type auto
ikey2 ipsec pre-fragment
ikey2 outgoing-interface GigaEthernet<$wanInterfaceNumber>
ikey2 peer $<OracleHeadendIpAddress2> authentication psk id ipv4
$<OracleHeadendIpAddress2>
n0 shutdown

! IP Routing
! Select dynamic (BGP) or static routing. Uncomment the corresponding commands prior to applying configuration.

! Border Gateway Protocol (BGP) Configuration
! Uncomment below lines if you select BGP.

! ip ufs-cache enable cache

! route-map pri1 permit 10
! set metric 5
! set local-preference 200

! route-map pri2 permit 10
! set metric 10
! set local-preference 150

! router bgp $<bgpASN>
! neighbor $<OracleInsideTunnelIpAddress1> remote-as 31898
! neighbor $<OracleInsideTunnelIpAddress1> timers 10 30
! neighbor $<OracleInsideTunnelIpAddress2> remote-as 31898
! neighbor $<OracleInsideTunnelIpAddress2> timers 10 30
! address-family ipv4 unicast
! neighbor $<OracleInsideTunnelIpAddress1> route-map pri1 in
! neighbor $<OracleInsideTunnelIpAddress1> route-map pri1 out
! neighbor $<OracleInsideTunnelIpAddress2> route-map pri2 in
! neighbor $<OracleInsideTunnelIpAddress2> route-map pri2 out
! network 192.168.100.0/24

! Static Route Configuration
! Uncomment below lines if you select static routing.

! ip ufs-cache enable
! ip route $<vcnCidrBlock> Tunnel0.0
! ip route $<vcnCidrBlock> Tunnel1.0
```

Openswan

If you want to use Openswan to create an IPSec VPN to Oracle Cloud Infrastructure, see Libreswan on page 3102.

How Openswan and Libreswan Are Related

Openswan is a well-known IPSec implementation for Linux. It began as a fork of the now-defunct FreeS/WAN project in 2003. Unlike the FreeS/WAN project, it didn't exclusively target the GNU/Linux operation system, but
Networking

expanded its use to other operating systems. In 2012, FreeS/WAN renamed itself to The Libreswan Project because of a lawsuit over a trademark of the name openswan.

As a result, when you try to install or query the Openswan package on Oracle Linux, by default the Libreswan package is installed or shown instead. The following yum search query command illustrates this behavior:

```bash
$ sudo yum search openswan
Loaded plugins: langpacks, ulninfo
Matched: openswan ============================================
NetworkManager--libreswan.x86_64 : NetworkManager VPN plugin for libreswan
NetworkManager--libreswan-gnome.x86_64 : NetworkManager VPN plugin for libreswan-GNOME files
libreswan.x86_64 : IPsec implementation with IKEv1 and IKEv2 keying protocols
```

Libreswan is maintained by The Libreswan Project and has been under active development for over 15 years, going back to the FreeS/WAN Project. For more information, see the project's history.

**Palo Alto**

This topic provides configuration for a Palo Alto device. The configuration was validated using PAN-OS version 8.0.0.

Palo Alto experience is required.

**Important:**

Oracle provides configuration instructions for a set of vendors and devices. Make sure to use the configuration for the correct vendor.

If the device or software version that Oracle used to verify the configuration does not exactly match your device or software, the configuration might still work for you. Consult your vendor's documentation and make any necessary adjustments.

If your device is for a vendor not in the list of verified vendors and devices, or if you're already familiar with configuring your device for IPSec, see the list of supported IPSec parameters and consult your vendor's documentation for assistance.

VPN Connect is the IPSec VPN that Oracle Cloud Infrastructure offers for connecting your on-premises network to a virtual cloud network (VCN).

The following diagram shows a basic IPSec connection to Oracle Cloud Infrastructure with redundant tunnels. IP addresses used in this diagram are only examples.

**Best Practices**

This section covers general best practices and considerations for using VPN Connect.
**Configure All Tunnels for Every IPSec Connection**

Oracle deploys two IPSec headends for each of your connections to provide high availability for your mission-critical workloads. On the Oracle side, these two heads are on different routers for redundancy purposes. Oracle recommends configuring all available tunnels for maximum redundancy. This is a key part of the "Design for Failure" philosophy.

**Have Redundant CPEs in Your On-Premises Network Locations**

Each of your sites that connects with IPSec to Oracle Cloud Infrastructure should have redundant edge devices (also known as customer-premises equipment (CPE)). You add each CPE to the Oracle Console and create a separate IPSec connection between your dynamic routing gateway (DRG) and each CPE. For each IPSec connection, Oracle provisions two tunnels on geographically redundant IPSec headends. For more information, see the Connectivity Redundancy Guide (PDF).

**Routing Protocol Considerations**

When you create an IPSec VPN, it has two redundant IPSec tunnels. Oracle encourages you to configure your CPE to use both tunnels (if your CPE supports it). Note that in the past, Oracle created IPSec VPNs that had up to four IPSec tunnels.

The following two routing types are available, and you choose the routing type separately for each tunnel in the IPSec VPN:

- **BGP dynamic routing**: The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from your on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
- **Static routing**: When you set up the IPSec connection to the DRG, you specify the particular routes to your on-premises network that you want the VCN to know about. You also must configure your CPE device with static routes to the VCN's subnets. These routes are not learned dynamically.

For more information about routing with VPN Connect, including Oracle recommendations on how to manipulate the BGP best path selection algorithm, see Routing for the Oracle IPSec VPN on page 2934.

**Other Important CPE Configurations**

Ensure access lists on your CPE are configured correctly to not block necessary traffic from or to Oracle Cloud Infrastructure.

If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.

**Caveats and Limitations**

This section covers general important characteristics and limitations of VPN Connect to be aware of.

**Asymmetric Routing**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec connection. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

When you use multiple tunnels to Oracle Cloud Infrastructure, Oracle recommends that you configure your routing to deterministically route traffic through the preferred tunnel. If you want to use one IPSec tunnel as primary and another as backup, configure more-specific routes for the primary tunnel (BGP) and less-specific routes (summary or default route) for the backup tunnel (BGP/static). Otherwise, if you advertise the same route (for example, a default route) through all tunnels, return traffic from your VCN to your on-premises network will route to any of the available tunnels (because Oracle uses asymmetric routing).

For specific Oracle routing recommendations about how to force symmetric routing, see Routing for the Oracle IPSec VPN on page 2934.
Networking

Route-Based or Policy-Based IPSec VPN

The IPSec protocol uses Security Associations (SAs) to determine how to encrypt packets. Within each SA, you define encryption domains to map a packet's source and destination IP address and protocol type to an entry in the SA database to define how to encrypt or decrypt a packet.

Note:

Other vendors or industry documentation might use the term proxy ID, security parameter index (SPI), or traffic selector when referring to SAs or encryption domains.

There are two general methods for implementing IPSec tunnels:

- **Route-based tunnels**: Also called next-hop-based tunnels. A route table lookup is performed on a packet's destination IP address. If that route’s egress interface is an IPSec tunnel, the packet is encrypted and sent to the other end of the tunnel.

- **Policy-based tunnels**: The packet's source and destination IP address and protocol are matched against a list of policy statements. If a match is found, the packet is encrypted based on the rules in that policy statement.

The Oracle VPN headends use route-based tunnels but can work with policy-based tunnels with some caveats listed in the following sections.

Encryption domain for route-based tunnels

If your CPE supports route-based tunnels, use that method to configure the tunnel. It's the simplest configuration with the most interoperability with the Oracle VPN headend.

Route-based IPSec uses an encryption domain with the following values:

- **Source IP address**: Any (0.0.0.0/0)
- **Destination IP address**: Any (0.0.0.0/0)
- **Protocol**: IPv4

If you need to be more specific, you can use a single summary route for your encryption domain values instead of a default route.

Encryption domain for policy-based tunnels

When you use policy-based tunnels, every policy entry (a CIDR block on one side of the IPSec connection) that you define generates an IPSec security association (SA) with every eligible entry on the other end of the tunnel. This pair is referred to as an encryption domain.

In this diagram, the Oracle DRG end of the IPSec tunnel has policy entries for three IPv4 CIDR blocks and one IPv6 CIDR block. The on-premises CPE end of the tunnel has policy entries two IPv4 CIDR blocks and two IPv6 CIDR blocks. Each entry generates an encryption domain with all possible entries on the other end of the tunnel. Both sides of an SA pair must use the same version of IP. The result is a total of eight encryption domains.
Important:

If your CPE supports only policy-based tunnels, be aware of the following restrictions.

- VPN Connect supports multiple encryption domains, but has an upper limit of 50 encryption domains.
- Policy-based routing is not available in all ADs. The release notes list available ADs.
- Depending on when your tunnel was created you might not be able to edit an existing tunnel to use policy-based routing and might need to replace the tunnel with a new IPSec tunnel.
- The CIDR blocks used on the Oracle DRG end of the tunnel can’t overlap the CIDR blocks used on the on-premises CPE end of the tunnel.
- An encryption domain must always be between two CIDR blocks of the same IP version.

If Your CPE Is Behind a NAT Device

In general, the CPE IKE identifier configured on your end of the connection must match the CPE IKE identifier that Oracle is using. By default, Oracle uses the CPE’s public IP address, which you provide when you create the CPE object in the Oracle Console. However, if your CPE is behind a NAT device, the CPE IKE identifier configured on your end might be the CPE’s private IP address, as shown in the following diagram.
Networking

Note:

Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as cpe.example.com. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Supported IPSec Parameters

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

CPE Configuration

Important:

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for your CPE. If you need support or further assistance, contact your CPE vendor's support directly.

The following figure shows the basic layout of the IPSec connection.

Important Details About the Configuration Instructions

- **Commits**: For PAN to activate the configuration, you must perform the commit action after any configuration change.
- **Example IP addresses**: The example configuration uses IP addresses from class A 10.0.0.0/8 (RFC1918) and 198.51.100.0/24 (RFC5735). When you perform the configuration on the CPE, use the correct IP addressing plan for your networking topology.

The example configuration uses the following variables and values:

- **Inside tunnel1 interface - CPE**: 198.51.100.1/30
- **Inside tunnel2 interface - CPE**: 198.51.100.5/30
- **Inside tunnel1 interface - Oracle**: 198.51.100.2/30
- **Inside tunnel2 interface - Oracle**: 198.51.100.6/30
- **CPE ASN**: 64511
- **On-premises network**: 10.200.1.0/24
- **VCN CIDR block**: 10.200.0.0/24
• CPE public IP address: 10.100.0.100/24
• Oracle VPN headend (DRG) IP address 1: 10.150.128.1/32
• Oracle VPN headend (DRG) IP address 2: 10.150.127.1/32
• Tunnel number 1: tunnel.1
• Tunnel number 2: tunnel.2
• Exit interface: ethernet1/1

About Using IKEv2

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

If you want to use IKEv2, there are special variations of some steps presented in the next section. Here is a summary of the special steps:

• For task 2 (defining the ISAKMP peers), when you add the IKE gateway:
  • On the General tab, for the Version, select IKEv2 only mode.
  • On the Advanced Options tab, select the IKE crypto profile associated with the IKEv2 tunnel.
• For task 5 (configuring the IPSec sessions), configure the proxy ID.

Configuration Process

The following process includes BGP configuration for the IPSec connection. If you instead want to use static routing, perform tasks 1–5, and then skip to CPE Configuration on page 3124.

Task 1: Configure the ISAKMP Phase 1 policy

In this example, the same ISAKMP policy is used for both tunnels.

1. Go to Network, to IKE Crypto, and then click Add.
2. Configure the parameters as shown in the next screenshot. For a list of the values, see Supported IPSec Parameters on page 2945. If you're configuring VPN Connect for the Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152.

The next screenshot shows the final result for this task:

Task 2: Define the ISAKMP peers
1. Go to **Network**, to **IKE Gateways**, and then click **Add**.
Networking

2. For peer 1, configure the parameters as shown in the next screenshots.

   a. On the **General** tab:
      - **Version**: For IKEv1, select **IKEv1 only mode**. If you want to use IKEv2, select **IKEv2 only mode**. Notice that if you're using IKEv2, later in task 5 you also add proxy IDs.
      - **Interface**: The interface that owns the public IP address on the CPE. Change **ethernet1/1** to the particular value for your networking topology.
      - **Peer IP addresses**: The public IP address that Oracle assigned to the Oracle headend of the tunnel. Change the value to the correct IP address for your first tunnel.
      - **Pre-shared Key**: The shared secret that Oracle automatically assigned during IPSec tunnel creation. If you want, you can specify a different value. Enter the same value here and in the Oracle Console.
      - **Local Identification** and **Peer Identification**: The IKE IDs. The **Local Identification** is the CPE's public IP address. The **Remote Identification** is the Oracle VPN headend IP address for the first tunnel.

   ![IKE Gateway Configuration Screenshot](image)

   b. On the **Advanced Options** tab, ensure that the values are set for the first peer according to the following screenshot.
If you are using IKEv2 instead, select the IKE crypto profile associated with the IKEv2 tunnel.
3. For peer 2, configure the parameters as shown in the next screenshots.

   a. On the General tab:

      • **Version**: For IKEv1, select **IKEv1 only mode**. If you want to use IKEv2, select **IKEv2 only mode**. For IKEv2, notice that you also need to provide a proxy ID later in task 5.
      • **Interface**: The interface that owns the public IP address on the CPE. Change `ethernet1/1` to the particular value for your networking topology.
      • **Peer IP addresses**: The public IP address that Oracle assigned to the Oracle headend of the tunnel. Change the value to the correct IP address for your second tunnel.
      • **Pre-shared Key**: The shared secret that Oracle automatically assigned during IPSec tunnel creation. If you want, you can specify a different value. Enter the same value here and in the Oracle Console.
      • **Local Identification** and **Peer Identification**: The IKE IDs. The **Local Identification** is the CPE's public IP address. The **Remote Identification** is the Oracle VPN headend IP address for the second tunnel.

   ![IKE Gateway Configuration](image)

   b. On the Advanced Options tab, ensure that the values are set for the second peer according to this screenshot:
Networking

If you are using IKEv2 instead, select the IKE crypto profile associated with the IKEv2 tunnel.

The next screenshot shows the final result for this task:

Task 3: Define the IPSec Phase 2 policy

In this example, the same IPSec crypto profile is used for both tunnels.
1. Go to **Network**, to **IPSec Crypto**, and then click **Add**.
2. Configure the parameters as shown in the next screenshot.

![IPSec Crypto Profile](image)

The next screenshot shows the final result for this task:

![Virtual Tunnel Interfaces](image)

**Task 4: Configure the virtual tunnel interfaces**

1. Go to **Network**, to **Interfaces**, to **Tunnel**, and then click **Add**.
2. For peer 1, configure the parameters as shown in the next screenshots.
   
   a. On the Config tab, assign the interface according to your virtual router and security zone configuration. In this example, the default virtual router and ipsec_tunnel security zone are used.
   
   ![Tunnel Interface Configuration](image1.png)
   
   b. On the IPv4 tab, ensure that the values are set for the first peer according to the following screenshot. In this example, the IP address for the tunnel interface is ipsec_address_static1 = 198.51.100.1/30. Configure your tunnel IP address according to your networking IP addressing plan.
   
   ![Tunnel Interface IPv4 Configuration](image2.png)
3. For peer 2, configure the parameters as shown in the next screenshots.

a. On the **Config** tab, assign the interface according to your virtual router and security zone configuration. In this example, the default virtual router and ipsec_tunnel security zone are used.

![Tunnel Interface](image)

b. On the **IPv4** tab, ensure that the values are set for the second peer according to the following screenshot. In this example, the IP address for the tunnel interface is ipsec_address_static2 = 198.51.100.5/30. Configure your tunnel IP address according to your networking IP addressing plan.

![Tunnel Interface](image)

The next screenshot shows the final result for this task:

![Tunnel Interface](image)

Task 5: Configure the IPSec sessions

1. Go to **Network**, to **IPSec Tunnels**, and then click **Add**.
2. For peer 1, configure the parameters on the **General** tab as shown in the next screenshot.

Notice that if you're using IKEv1, you do not need to add specific proxy IDs to the **Proxy IDs** tab. They are not needed for an IKEv1 route-based VPN configuration.

However, for IKEv2, do add proxy IDs to the **Proxy IDs** tab for better interoperability. Ensure that you also configured the IKE gateway to use IKEv2 earlier in task 2.

3. For peer 2, configure the parameters on the **General** tab as shown in the next screenshot.

If you are using IKEv2, also add proxy IDs on the **Proxy IDs** tab.

![General Tab Configuration](image)

Task 6: Configure BGP over IPSec

**Note:**

If you want to use static routing instead of BGP, skip task 6 and go to **Configuring Static Routing** on page 3148.

BGP over IPSec requires IP addresses on the tunnel interfaces on both ends.

The screenshots in this example use these subnets for the tunnel interfaces:

- 198.51.100.0/30
- CPE: 198.51.100.1/30
- DRG: 198.51.100.2/30
- 198.51.100.4/30
- CPE: 198.51.100.5/30
- DRG: 198.51.100.6/30

Replace the example values with the BGP IP addresses you specified in the Oracle Console for the inside tunnel interfaces.
This task consists of three subtasks, each with multiple steps.

Subtask 6-a: Configure the BGP parameters

1. Go to **Network**, to **Virtual Routers**, to **default**, and then to **BGP**. This example uses the default virtual router. Also, the example uses 10.200.1.10 for the router ID and 64511 for the ASN. Use the correct virtual router based on your networking configuration, and use the correct router ID and ASN for your environment.

2. On the **General** tab, configure the parameters as shown in the next screenshot.

3. On the **Advanced** tab, configure the parameters as shown in the next screenshot.
4. On the **Peer Group** tab:

a. Add the first Peer Group, and under the **Peer Group Name**, add the first session. Add the BGP session with the DRG.

![Peer Group Configuration](image1)

b. For the first tunnel, on the **Addressing** tab, configure the parameters as shown in the next screenshot. Oracle's BGP ASN in commercial regions is 31898. If you're configuring VPN Connect for the Government Cloud, see Oracle's BGP ASN on page 154.

![Addressing Configuration](image2)

c. On the **Connection Options** tab, configure the parameters as shown in the next screenshot.
d. On the **Advanced** tab, configure the parameters as shown in the next screenshot.
e. On the **Peer Group** tab, add the second Peer Group, and under the **Peer Group Name**, add the second session. Add the BGP session with the DRG.

f. For the second tunnel, on the **Addressing** tab, configure the parameters as shown in the next screenshot.
g. On the **Connection Options** tab, configure the parameters as shown in the next screenshot.
h. On the Advanced tab, configure the parameters as shown in the next screenshot.
The next screenshot shows the final Peer Group configuration:

<table>
<thead>
<tr>
<th>Name</th>
<th>Route</th>
<th>Type</th>
<th>Peer AS</th>
<th>Peer AS No</th>
<th>Peer Address</th>
<th>Local Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRG1</td>
<td>Yes</td>
<td>mtp</td>
<td>31898</td>
<td>199.10.100.2</td>
<td>peer_address_dr1</td>
<td></td>
</tr>
<tr>
<td>DRG2</td>
<td>Yes</td>
<td>mtp</td>
<td>31898</td>
<td>199.10.100.6</td>
<td>peer_address_dr2</td>
<td></td>
</tr>
</tbody>
</table>

Network
5. On the **Import** tab, configure the parameters as shown in the next screenshots. Here you configure tunnel.1 as the primary and tunnel.2 as the backup for the VCN route received from the DRG by way of BGP (10.200.0.0/24). From the BGP perspective, both tunnels are in the Established state.

a. For the first rule, on the **General** tab, configure the parameters as shown in the next screenshot.

![Virtual Router - BGP - Import Rule](image)

b. On the **Match** tab, configure the parameters as shown in the next screenshot.

![Virtual Router - BGP - Import Rule](image)

c. On the **Action** tab, configure the parameters as shown in the next screenshot.
Networking

d. For the second rule, on the **General** tab, configure the parameters as shown in the next screenshot.

![General tab configuration screenshot](image)

e. On the **Match** tab, configure the parameters as shown in the next screenshot.

![Match tab configuration screenshot](image)
f. On the **Action** tab, configure the parameters as shown in the next screenshot.
6. On the **Export** tab, configure the parameters as shown in the next screenshots. Here you configure a policy to force the DRG to prefer tunnel.1 for the returning path to the on-premises network CIDR (10.200.1.0/24).

   a. On the **General** tab, configure the parameters as shown in the next screenshot.

   ![General Tab Screenshot]

   b. On the **Match** tab, configure the parameters as shown in the next screenshot.

   ![Match Tab Screenshot]

   c. On the **Action** tab, configure the parameters as shown in the next screenshot.
The next screenshot shows the final Export configuration:

Notice that no configuration is required for the **Conditional Adv** or **Aggregate** tabs.
7. On the **Redist Rules** tab, configure the parameters as shown in the next screenshot. Here you announce the on-premises network CIDR in BGP.

Subtask 6-b: Wait for the BGP sessions to establish and then check the BGP status

1. Go to **Network**, to **IPSec Tunnels**, to the **Virtual Router** column, and then click **Show Routes**.

2. Go to **BGP**, and then to the **Peer** tab to verify that the BGP session is established. Any other value means that the BGP session has not been established successfully and route exchange will not occur.
3. On the **Local RIB** tab: The prefixes are received from the DRG, with tunnel.1 being preferred.

![Virtual Router - default](image)

4. On the **RIB Out** tab: The on-premises network CIDR is sent by way of BGP to DRG1 with as_path of 64511, and for DRG2, with an as_path of 64511, 64511. In this way, based on the BGP Best Path Algorithm, the route preferred by the DRG to reach the on-premises network CIDR uses the connection over tunnel.1.

![Virtual Router - default](image)

Subtask 6-c: Confirm that the BGP routes have been inserted in the routing table

To view the routes, go to **Routing**, and then to the **Route Table** tab.

![Virtual Router - default](image)

**Configuring Static Routing**

Use the instructions here if your CPE does not support BGP over IPSec, or you do not want to use BGP over IPSec.

In this task, you configure static routes to direct traffic through the tunnel interfaces to reach the DRG and finally the VCN hosts.

1. Follow tasks 1–5 in the preceding section.
2. Configure static routes:
   a. Go to Network, to Virtual Routers, to default, to Static Routes, and then click Add.
   b. For Route 1, configure the parameters as shown in the next image.
   c. For Route 2, configure the parameters as shown in the next image.
3. (Recommended) Enable ECMP for traffic sent through the two tunnels. The metric for both routes is set to 10. Here are some important notes about enabling ECMP:

- First check to see if your networking design allows for ECMP.
- Enabling or disabling ECMP on an existing virtual router causes the system to restart the virtual router. The restart might cause existing sessions to be terminated.
- This example uses the default virtual router. Use the correct virtual router for your network environment.

To enable ECMP, go to Network, to Virtual Routers, to default, to Router Settings, to ECMP, and then select the check box for Enable.

Here are screenshots that show the final configuration after this task is complete:

Changing the IKE Identifier

If the CPE is behind a NAT device with a private IP address on the exit interface that the tunnel interfaces use as the source, you must specify the public IP address of the NAT device as the local IKE ID. You can do this by setting the Local Identification value in the IKE Gateway configuration:
Verifying IPSec Tunnel Status

Use this command to verify the IKE SA:

```
show vpn ike-sa
```

Use this command to verify the IPSec tunnel configuration:

```
show vpn tunnel name <tunnel_name>
```

To verify the BGP status, look for **Established:**
To verify the BGP status from the command line:

```
show routing protocol bgp peer peer-name <name>
```

To verify that the routes are installed in the routing table:

```
show routing route
```

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see VPN Connect Metrics on page 3164.

If you have issues, see VPN Connect Troubleshooting on page 3166.

**WatchGuard**

You can configure a WatchGuard Firebox as your CPE device for an IPSec VPN.

To download the configuration instructions, go to the WatchGuard knowledge base article.

**Yamaha RTX Series**

This configuration was validated using an RTX1210 running Firmware Rev.14.01.28 and RTX830 running Firmware Rev.15.02.03.

---

**Important:**

Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec VPN connection. Even if you configure one tunnel as primary and another as backup, traffic from your VCN to your on-premises network can use any tunnel that is "up" on your device. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.

---

**Before Starting**

Before configuring your CPE:

- Configure your internet provider settings.
- Configure firewall rules to open UDP port 500, UDP port 4500, and ESP.

**Supported Encryption Domain or Proxy ID**

The values for the encryption domain (also known as a proxy ID, security parameter index (SPI), or traffic selector) depend on whether your CPE supports route-based tunnels or policy-based tunnels. For more information about the correct encryption domain values to use, see Supported Encryption Domain or Proxy ID on page 2948.

**Parameters from API or Console**

Get the following parameters from the Oracle Cloud Infrastructure Console or API.

- `$(ipAddress#)`
  - Oracle VPN headend IPSec tunnel endpoints. There is one value for each tunnel.
  - Example value: 129.146.12.52

- `$(sharedSecret#)`
  - The IPSec IKE pre-shared-key. There is one value for each tunnel.
  - Example value: EXAMPLEDPfAMkD7nTH3SWr6OFabdT6exXn6enSlsKbE

- `$(cpePublicIpAddress)`
  - The public IP address for the CPE (previously made available to Oracle via the Console).

- `$(VcnCidrBlock)`
When creating the VCN, your company selected this CIDR to represent the IP aggregate network for all VCN hosts.

Example Value: 10.0.0.0/20

**Parameters Based on Current CPE Configuration and State**

The following parameters are based on your current CPE configuration.

`${tunnelInterface#}`

- An interface number to identify the specific tunnel.
- Example value: 1

`${ipsecPolicy#}`

- The SA policy to be used for the selected inline interface.
- Example value: 1

`${localAddress}`

- The public IP address of your CPE.
- Example value: 146.56.2.52

**Config Template Parameter Summary**

Each region has multiple Oracle IPSec headends. The following template allows you to set up multiple tunnels on your CPE, each to a corresponding headend. In the table, "User" is you/your company.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Source</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${ipAddress1}</code></td>
<td>Console/API</td>
<td>129.146.12.52</td>
</tr>
<tr>
<td><code>${sharedSecret1}</code></td>
<td>Console/API</td>
<td>(long string)</td>
</tr>
<tr>
<td><code>${ipAddress2}</code></td>
<td>Console/API</td>
<td>129.146.13.52</td>
</tr>
<tr>
<td><code>${sharedSecret2}</code></td>
<td>Console/API</td>
<td>(long string)</td>
</tr>
<tr>
<td><code>${cpePublicIpAddress}</code></td>
<td>User</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td><code>${VcnCidrBlock}</code></td>
<td>User</td>
<td>10.0.0.0/20</td>
</tr>
</tbody>
</table>

**Important:**

The following ISAKMP and IPSec policy parameter values are applicable to VPN Connect in the commercial cloud. For the Government Cloud, you must use the values listed in Required VPN Connect Parameters for Government Cloud on page 152.

**ISAKMP Policy Options**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAKMP protocol version</td>
<td>Version 1</td>
</tr>
<tr>
<td>Exchange type</td>
<td>Main mode</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Pre-shared keys</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES-256-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>SHA-256</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>Group 5</td>
</tr>
<tr>
<td>IKE session key lifetime</td>
<td>28800 seconds (8 hours)</td>
</tr>
</tbody>
</table>
**IPSec Policy Options**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec protocol</td>
<td>ESP, tunnel-mode</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES-256-cbc</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>HMAC-SHA1-96</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>Group 5</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>Enabled</td>
</tr>
<tr>
<td>IPSec session key lifetime</td>
<td>3600 seconds (1 hour)</td>
</tr>
</tbody>
</table>

**CPE Configuration**

**ISAKMP and IPSec Configuration**

```bash
tunnel select 1
description tunnel OCI-VPN1
ipsec tunnel 1
  ipsec sa policy 1 1 esp aes256-cbc sha-hmac
  ipsec ike duration ipsec-sa 1 3600
  ipsec ike duration isakmp-sa 1 28800
  ipsec ike encryption 1 aes256-cbc
  ipsec ike group 1 modp1536
  ipsec ike hash 1 sha256
  ipsec ike keepalive log 1 off
  ipsec ike keepalive use 1 on dpd 5 4
  ipsec ike local address 1 ${cpePublicIpAddress}
  ipsec ike local id 1 0.0.0.0/0
  ipsec ike nat-traversal 1 on
  ipsec ike pfs 1 on
  ipsec ike pre-shared-key 1 text ${sharedSecret1}
  ipsec ike remote address 1 ${ipAddress1}
  ipsec ike remote id 1 0.0.0.0/0
ip tunnel tcp mss limit auto
tunnel enable 1
tunnel select 2
description tunnel OCI-VPN2
ipsec tunnel 2
  ipsec sa policy 2 2 esp aes256-cbc sha-hmac
  ipsec ike duration ipsec-sa 2 3600
  ipsec ike duration isakmp-sa 2 28800
  ipsec ike encryption 2 aes256-cbc
  ipsec ike group 2 modp1536
  ipsec ike hash 2 sha256
  ipsec ike keepalive log 2 off
  ipsec ike keepalive use 2 on dpd 5 4
  ipsec ike local address 2 ${cpePublicIpAddress}
  ipsec ike local id 2 0.0.0.0/0
  ipsec ike nat-traversal 2 on
  ipsec ike pfs 2 on
  ipsec ike pre-shared-key 2 text ${sharedSecret2}
  ipsec ike remote address 2 ${ipAddress2}
  ipsec ike remote id 2 0.0.0.0/0
ip tunnel tcp mss limit auto
tunnel enable 2
ipsec auto refresh on```
Static Routes Configuration

```
ip route $(VcnCidrBlock) gateway tunnel 1 hide gateway tunnel 2 hide
```

Working with VPN Connect

This topic contains some details about working with VPN Connect and the related components. Also see these topics:

- [VPN Connect Overview](#) on page 2933
- [VPN Connect Quickstart](#) on page 2939
- [Setting Up VPN Connect](#) on page 2949
- [CPE Configuration](#) on page 2967
- [Using the CPE Configuration Helper](#) on page 2970
- [VPN Connect FAQ](#)
- [VPN Connect Metrics](#) on page 3164
- [VPN Connect Troubleshooting](#) on page 3166

Updated VPN Connect service

VPN Connect v2 improves availability and reliability of IPSec connections and makes possible new functionality. Regions that can provide VPN Connect v2 are listed in [VPN Connect v2 availability](#) on page 3156. Where available, all newly created IPSec connections are created using VPN Connect v2. The process for setting up VPN Connect v2 is identical to setting up VPN Connect v1.

New functions that depend on VPN Connect v2 include:

- [Multiple encryption domains](#)
- [Logging for VPN Connect](#)

Regions that support VPN Connect v2 will continue to support VPN Connect v1. If you have VPN Connect in one of these regions and want to use one of the added features available for VPN Connect v2, you will need to create a new connection and end the older connection. There is no migration path to change a v1 connection to a v2 connection currently.

VPN Connect v2 availability

VPN Connect v2 is available in the following regions:

<table>
<thead>
<tr>
<th>Commercial Regions</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia East (Sydney)</td>
<td>Available</td>
</tr>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td>Not Available</td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>Available</td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>Available</td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>Available</td>
</tr>
<tr>
<td>Chile Central (Santiago)</td>
<td>Not Available</td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>Available</td>
</tr>
<tr>
<td>India (Hyderabad)</td>
<td>Available</td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>Not Available</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>Available</td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td>Not Available</td>
</tr>
<tr>
<td>Netherlands Northwest (Amsterdam)</td>
<td>Available</td>
</tr>
</tbody>
</table>
### Commercial Regions and Status

<table>
<thead>
<tr>
<th>Commercial Regions</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saudi Arabia West (Jeddah)</td>
<td>Not Available</td>
</tr>
<tr>
<td>South Korea (Chuncheon)</td>
<td>Available</td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td>Not Available</td>
</tr>
<tr>
<td>Switzerland North (Zurich)</td>
<td>Available</td>
</tr>
<tr>
<td>UAE East (Dubai)</td>
<td>Not Available</td>
</tr>
<tr>
<td>UK South (London)</td>
<td>Available</td>
</tr>
<tr>
<td>UK West (Newport)</td>
<td>Not Available</td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td>Available</td>
</tr>
<tr>
<td>US West (Phoenix)</td>
<td>Available</td>
</tr>
<tr>
<td>US West (San Jose)</td>
<td>Not Available</td>
</tr>
</tbody>
</table>

### Viewing Tunnel Status and Configuration

When you successfully create the IPSec connection, Oracle produces important configuration information for each of the resulting IPSec tunnels. For an example, see task 2h in the overall setup process. You can view that information and the status of the tunnels at any time. This includes the BGP status if the tunnel is configured to use BGP dynamic routing.

**To view the status and configuration information for the IPSec tunnels**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **VPN Connections**.

   A list of the IPSec connections in the compartment that you’re viewing is displayed. If you don’t see the one you’re looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. Click the IPSec connection you're interested in.

   Each tunnel's details are displayed, including the IPSec status, the BGP status (if the tunnel uses BGP dynamic routing), and the Oracle VPN IP address (the VPN headend).

3. To view a tunnel's shared secret:
   a. Click the tunnel you're interested in.
   b. Next to the **Shared Secret** field, click **Show**.

### Using the CPE Configuration Helper

After you set up VPN Connect, your network engineer must configure the customer-premises equipment (CPE) at your end of the connection. The configuration includes details about your virtual cloud network (VCN) and the IPSec tunnels in the VPN Connect. The CPE Configuration Helper generates the information for your network engineer. For more information, see Using the CPE Configuration Helper on page 2970.

### Changing the Static Routes

You can change the static routes for an existing IPSec connection. You can provide up to 10 static routes.

Remember that an IPSec connection can use either static routing or BGP dynamic routing. You associate the static routes with the overall IPSec connection and not the individual tunnels. If an IPSec connection has static routes associated with it, Oracle uses them for routing a tunnel's traffic only if the tunnel itself is configured to use static routing. If it's configured to use BGP dynamic routing, the IPSec connection's static routes are ignored.

**Important:**

The IPSec connection goes down while it is reprovisioned with your static route changes.
To edit the static routes

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

   A list of the IPSec connections in the compartment that you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. For the IPSec connection you're interested in, click the Actions icon (three dots), and then click Edit.

   The current static routes are displayed.

3. Make your changes and click Save Changes.

Changing the CPE IKE Identifier That Oracle Uses

If your CPE is behind a NAT device, you might need to give Oracle your CPE IKE identifier. You can either specify it when you create the IPSec connection, or later edit the IPSec connection and change the value. Oracle expects the value to be an IP address or fully qualified domain name (FQDN). When you specify the value, you also specify which type it is.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IPSec connection goes down while it is reprovisioned to use your CPE IKE identifier.</td>
</tr>
</tbody>
</table>

To change the CPE IKE identifier that Oracle uses

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

   A list of the IPSec connections in the compartment that you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. For the IPSec connection you're interested in, click the Actions icon (three dots), and then click Edit.

   The current CPE IKE identifier that Oracle is using is displayed at the bottom of the dialog.

3. Enter your new values for CPE IKE Identifier Type and CPE IKE Identifier, and then click Save Changes.

Using IKEv2

Oracle supports Internet Key Exchange (IKE) version 1 and version 2 (IKEv2).

If you want to use IKEv2 and your CPE supports it, you must:

- Configure each IPSec tunnel to use IKEv2 in the Oracle Console. See the following procedures.
- Configure your CPE to use IKEv2 encryption parameters that the CPE supports. For a list of parameters that Oracle supports, see Supported IPSec Parameters on page 2945.

New IPSec connection: using IKEv2

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you create a new IPSec connection manually, you can specify IKEv2 when you create the IPSec connection in the Oracle Console. See the procedure that immediately follows.</td>
</tr>
<tr>
<td>If you instead use the VPN quickstart workflow, the IPSec connection is configured to use IKEv1 only. However, after the workflow is complete, you can edit the resulting IPSec tunnels in the Oracle Console and change them to use IKEv2.</td>
</tr>
</tbody>
</table>

To manually set up a new IPSec connection that uses IKEv2:

1. While creating the IPSec connection in the Oracle Console, in the Advanced Options section, click the Tunnel 1 tab.
2. From the IKE Version menu, select IKEv2.
3. Repeat the preceding step for the Tunnel 2 tab.
4. Later when configuring your CPE, configure it to use only IKEv2 and related IKEv2 encryption parameters that the CPE supports.

**Existing IPSec connection: upgrading to IKEv2**

**Important:**

Oracle recommends performing the following process for one tunnel at a time to avoid disruption in your overall connection. If your connection is not redundant (for example, does not have multiple tunnels), expect downtime while you upgrade to IKEv2.

1. Change the tunnel's IKE version in the Oracle Console:
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **VPN Connections**.
   b. Click the IPSec connection you're interested in.
   c. Click the tunnel to view its details.
   d. Click **Edit**.
   e. From the **IKE Version** menu, select IKEv2.
   f. Click **Save Changes**.

2. Update your CPE configuration for the tunnel to use IKEv2 and the related encryption parameters that the CPE supports. For a list of parameters that Oracle supports, see **Supported IPSec Parameters** on page 2945.

3. If the security associations did not rekey immediately, force a rekey for that tunnel on your CPE. In other words, clear the phase 1 and phase 2 security associations and do not wait for them to expire. Some CPE devices wait for the SAs to expire before rekeying. Forcing the rekey lets you confirm immediately that the IKE version configuration is correct.

4. To verify, ensure that the security associations for the tunnel rekey correctly. If they don't, confirm that the correct IKE version is set in the Oracle Console and on your CPE, and that the CPE is using the desired parameters.

After you've confirmed the first tunnel is up and running again, repeat the preceding steps for the second tunnel.

**Changing the Shared Secret That an IPSec Tunnel Uses**

When you set up an IPSec VPN, by default Oracle provides each tunnel's shared secret (also called the pre-shared key). You might have a particular shared secret that you want to use instead. You can specify each tunnel's shared secret when you create the IPSec connection, or you can edit the tunnels and provide each new shared secret then. For the shared secret, only numbers, letters, and spaces are allowed. Oracle recommends using a different shared secret for each tunnel.

**Important:**

When you change a tunnel's shared secret, both the overall IPSec connection and the tunnel go into the Provisioning state while the tunnel is reprovisioned with the new shared secret. The other tunnel in the IPSec connection remains in the Available state. However, while the first tunnel is being reprovisioned, you cannot change the second tunnel's configuration.

**To change the shared secret that an IPSec tunnel uses**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **VPN Connections**.
   A list of the IPSec connections in the compartment that you're viewing is displayed. If you don't see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. Click the IPSec connection you're interested in.

3. Click the tunnel you're interested in.

4. Next to the **Shared Secret** field, click **Edit**.

5. Enter your new value. Only numbers, letters, and spaces are allowed.

6. Click **Save Changes**.
Changing from Static Routing to BGP Dynamic Routing

If you want to change an existing IPSec VPN from using static routing to using BGP dynamic routing, follow the process in this section.

**Caution:**

When you change a tunnel's routing type, the tunnel's IPsec status does not change during reprovisioning. However, routing through the tunnel is affected. Traffic is temporarily disrupted until your network engineer configures your CPE device in accordance with the routing type change. **If your existing IPSec VPN is currently configured to use only a single tunnel, this process will disrupt your connection to Oracle.** If your IPSec VPN instead uses multiple tunnels, Oracle recommends reconfiguring one tunnel at a time to avoid disrupting your connection to Oracle.

**To change from static routing to BGP dynamic routing**

**Prerequisites:**
- You've read this section: Routing for the Oracle IPSec VPN on page 2934
- You've gathered the necessary BGP routing information:
  - Your network's ASN. Oracle's BGP ASN for the commercial cloud is 31898. For the Government Cloud, see Oracle's BGP ASN on page 154.
  - For each tunnel: The BGP IP address for each end of the tunnel (the two addresses for a given tunnel must be a pair from a /30 or /31 subnet, and they must be part of the IPSec VPN's encryption domain)

Repeat the following process for each tunnel in the IPSec connection:

1. Reconfigure the tunnel's routing type from static routing to BGP dynamic routing:
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **VPN Connections**.
   b. Click the IPSec connection you're interested in.
      The tunnels are listed, and the status for each tunnel is shown. The **BGP Status** for the tunnel you're interested in should show only a hyphen (no value), which means that the tunnel is currently configured to use static routing.
   c. Click the tunnel to view all of its details.
   d. Click **Edit**.
   e. Do the following:
      - **Routing Type**: Select the radio button for **BGP Dynamic Routing**.
      - **BGP ASN**: Enter your network's BGP ASN.
      - **Inside Tunnel Interface - CPE**: Enter the BGP IP address with subnet mask (either /30 or /31) for the CPE end of the tunnel. For example: 10.0.0.16/31.
      - **Inside Tunnel Interface - Oracle**: Enter the BGP IP address with subnet mask (either /30 or /31) for the Oracle end of the tunnel. For example: 10.0.0.17/31.
   f. Click **Save Changes**.
      The tunnel's **BGP Status** changes to Down.
2. Have your network engineer update your CPE device's tunnel configuration to use BGP.
3. On your side of the connection, confirm that the tunnel's BGP session is in an established state. If it is not, make sure you've configured the correct IP addresses for the tunnel in the Oracle Console and also for your CPE device.
4. In the Oracle Console, confirm that the tunnel's **BGP Status** is now Up.
5. Confirm that your CPE device is learning routes from Oracle, and your CPE device is advertising routes to Oracle.
   If you want to re-advertise the Oracle routes from BGP back to your on-premises network, make sure your CPE device is configured accordingly. Your existing policy to advertise the static routes to your on-premises network may not work for the BGP learned routes.
6. Ping the Oracle BGP IP address from your side of the connection to confirm that traffic is flowing.
After you've confirmed the first tunnel is up and running with BGP, repeat the process for the second tunnel.

**Important:**

As noted in Routing for the Oracle IPSec VPN on page 2934, the static routes that are still configured for the overall IPSec connection do NOT override the BGP routing. Those static routes are ignored when Oracle routes traffic through a tunnel that is configured to use BGP.

Also, you can change a tunnel's routing type back to static routing if necessary. You might do this if the scheduled downtime window for the CPE device is ending soon and you're having trouble establishing the BGP session. When you switch back to static routing, make sure the overall IPSec connection still has your desired static routes configured.

**Monitoring Your IPSec VPN**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring your connection, see VPN Connect Metrics on page 3164.

**Viewing Your VPN Connect Log Messages**

Access the log messages for VPN Connect.

You can view the log messages generated for various operational aspects of VPN Connect such as the negotiations that occur in bringing an IPSec tunnel UP. Enabling and accessing the VPN Connect log messages can be done via VPN Connect or the Logging Service.

- For an overview of the Logging Service in general, refer to Logging Overview on page 2574
- For details on enabling and accessing the VPN Connect log messages via the Logging service, refer to Service Logs on page 2591
- For details on the VPN Connect log message schema, refer to Details for VPN Connect on page 2615

**To enable message logging**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.
2. A list of the IPSec connections in the compartment that you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).
3. For the IPSec connection you're interested in, click the name of the connection.
   The details page for the connection is displayed.
4. On the left side of the screen under Resources, click on Logs.
   If you do not see this option, the connection has the older VPN Connect v1 type. Message logging requires VPN Connect v2.
   Details for the options on the screen are at Enabling Logging for a Resource on page 2591. Logs are handled the same regardless of the resource type generating the log.
6. Click Enable Log.
   The Log detail page is displayed, and the log will be in the process of being created (a "Creating log" message is displayed).

**To view log messages**

You must already have logging enabled to view the message log. To view the message log:

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.
2. A list of the IPSec connections in the compartment that you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

3. On the left side of the screen under Resources, click on Logs.

   If you do not see this option, the connection has the older VPN Connect v1 type. Message logging requires VPN Connect v2.

4. Click on the Log Name of the log you are interested in. This will open a new browser tab showing the requested log.

See To view the contents of logs on page 2581 for details on using the log display screen.

Disabling or Terminating the IPSec VPN

If you want to disable the IPSec VPN between your on-premises network and VCN, you can simply detach the DRG from the VCN instead of deleting the IPSec connection. If you're also using the DRG with FastConnect, detaching the DRG would also interrupt the flow of traffic over FastConnect.

You can delete the IPSec connection. However, if you later want to re-establish it, your network engineer would have to configure your CPE device again with a new set of tunnel configuration information from Oracle.

If you want to permanently delete the entire IPSec VPN, you must first terminate the IPSec connection. Then you can delete the CPE object. If you're not using the DRG for another connection to your on-premises network, you can detach it from the VCN and then delete it.

To delete an IPSec connection

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

   A list of the IPSec connections in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. Click the IPSec connection you're interested in.

3. Click Terminate.

4. Confirm the deletion when prompted.

The IPSec connection will be in the Terminating state for a short period while it's being deleted.

To delete a CPE object

Prerequisite: There must not be an IPSec connection between the CPE object and a DRG.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Customer-Premises Equipment.

   A list of the CPE objects in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. For the CPE object that you want to delete, click the Actions icon (three dots), and then click Delete.

3. Confirm the deletion when prompted.

The object will be in the Terminating state for a short period while it's being deleted.

Managing Tags for an IPSec Connection or CPE Object

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

To manage tags for an IPSec connection

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.

   A list of the IPSec connections in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. Click the IPSec connection you're interested in.

3. Click the Tags tab to view or edit the existing tags. Or click Add tags to add new ones.
To manage tags for a CPE object

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Customer-Premises Equipment.

   A list of the CPE objects in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).
2. Click the CPE object you're interested in.
3. Click the Tags tab to view or edit the existing tags. Or click Apply tag(s) to add new ones.

Moving an IPSec Connection or CPE Object to a Different Compartment

You can move your resources from one compartment to another. After you move the resource to the new compartment, inherent policies apply immediately and affect access to the resource through the Console. Moving the CPE object to a different compartment does not affect the connection between your data center and Oracle Cloud Infrastructure. For more information, see Working with Compartments on page 2432.

To move a CPE object to a different compartment

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Customer-Premises Equipment.
2. Find the CPE object in the list, click the the Actions icon (three dots), and then click Move Resource.
3. Choose the destination compartment from the list.
4. Click Move Resource.

Managing Your DRG

For tasks related to DRGs, see Dynamic Routing Gateways (DRGs) on page 2927.

Using the API for VPN Connect

This topic lists the Networking service API operations for managing VPN Connect components.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage your VCN and subnets, use these operations:

- ListVcns
- CreateVcn
- GetVcn
- UpdateVcn
- DeleteVcn
- ChangeVcnCompartment
- ListSubnets
- CreateSubnet
- GetSubnet
- UpdateSubnet
- DeleteSubnet
- ChangeSubnetCompartment

To manage your DRG, use these operations:

- ListDrgs
- CreateDrg
- GetDrg
- UpdateDrg
- DeleteDrg
- ListDrgAttachments
• **CreateDrgAttachment**: This operation attaches a DRG to a VCN and results in a `DrgAttachment` object with its own OCID.
• **GetDrgAttachment**
• **UpdateDrgAttachment**
• **DeleteDrgAttachment**: This operation detaches a DRG from a VCN by deleting the `DrgAttachment` object.

To manage routing for your VCN, use these operations:
• **ListRouteTables**
• **GetRouteTable**
• **UpdateRouteTable**
• **CreateRouteTable**
• **DeleteRouteTable**

To manage security lists for your VCN, use these operations:
• **ListSecurityLists**
• **GetSecurityList**
• **UpdateSecurityList**
• **CreateSecurityList**
• **DeleteSecurityList**

To manage your CPEs, use these operations:
• **ListCpes**
• **CreateCpe**
• **GetCpe**
• **UpdateCpe**
• **DeleteCpe**
• **ChangeCpeCompartment**

To manage your IPSec connections, use these operations:
• **ListIPSecConnections**
• **CreateIPSecConnection**: Use this operation to get the configuration information for each tunnel, including the IP address of the DRG (the VPN headend) and the shared secret. See [CPE Configuration](#) on page 2967.
• **GetIPSecConnection**
• **UpdateIPSecConnection**
• **DeleteIPSecConnection**
• **ChangeIPSecConnectionCompartment**
• **GetIPSecConnectionDeviceStatus**: Use this operation to determine the status of the IPSec tunnels (up or down).
• **GetIPSecConnectionDeviceConfig**: Use this operation to get the configuration information for each tunnel.

### VPN Connect Metrics

You can monitor the health, capacity, and performance of your **VPN Connect** by using metrics, alarms, and notifications. For more information, see [Monitoring Overview](#) on page 2660 and [Notifications Overview](#) on page 3350.

This topic describes the metrics emitted by the metric namespace `oci_vpn`.

Resources: IPSec connections.

**Overview of Metrics: oci_vpn**

The available metrics help you determine quickly if your **VPN Connect** is up, how much data is flowing over the connection, and if packets are being dropped for unexpected errors.

A VPN Connect includes these resources:
• An IPSec connection, which you can think of as the parent resource (identified by parentResourceId in the following discussion).

• One or more individual tunnels associated with that IPSec connection (each identified by the tunnel's publicIp in the following discussion).

Required IAM Policy

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_vpn

The metrics listed in the following table are automatically available for any VPN Connect that you create. You do not need to enable monitoring on the resource to get these metrics.

You also can use the Monitoring service to create custom queries.

Each metric includes the following dimensions:

PARENTRESOURCEID

The OCID of the IPSec connection (the parent resource). The connection has multiple individual tunnels.

PUBLICIP

Although each tunnel has its own OCID, it can be easier to use the publicIp dimension to identify a specific IPSec tunnel in the connection. The value is the public IP address of the Oracle end of the tunnel (also known as the Oracle VPN headend).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TunnelState</td>
<td>IPSec Tunnel State</td>
<td>Binary (1 or 0)</td>
<td>Whether the tunnel is up (1) or down (0).</td>
<td>parentResourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>publicIp</td>
</tr>
<tr>
<td>PacketsReceived</td>
<td>Packets Received</td>
<td>Packets</td>
<td>Number of packets received at the Oracle end of the connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BytesReceived</td>
<td>Bytes Received</td>
<td>Bytes</td>
<td>Number of bytes received at the Oracle end of the connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PacketsSent</td>
<td>Packets Sent</td>
<td>Packets</td>
<td>Number of packets sent from the Oracle end of the connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BytesSent</td>
<td>Bytes Sent</td>
<td>Bytes</td>
<td>Number of bytes sent from the Oracle end of the connection.</td>
<td></td>
</tr>
</tbody>
</table>
### Networking

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PacketsError</td>
<td>Packets with Errors</td>
<td>Packets</td>
<td>Number of packets dropped at the Oracle end of the connection. Dropped packets indicate a misconfiguration in some part of the overall system. Check if there's been a change to the configuration of your VCN, the IPSec VPN, or your CPE.</td>
<td></td>
</tr>
</tbody>
</table>

#### Using the Console

To view default metrics charts for an individual tunnel in an IPSec connection

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click VPN Connections.
2. Click the IPSec connection to view its details.
3. Click the tunnel you're interested in to view its details and default metrics charts.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for all IPSec connections in a compartment

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that contains the IPSec connection you're interested in.
3. For Metric Namespace, select oci_vpn.

The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

Each IPSec tunnel is a single line in a given chart. The tunnel is identified in the chart by the public IP address of the Oracle end of the tunnel.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

#### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

#### VPN Connect Troubleshooting

Create a service request Ask the community

This topic covers the most common troubleshooting issues for VPN Connect. Some suggestions assume that you are a network engineer with access to your CPE device's configuration.
Log Messages

Viewing log messages generated for various operational aspects of VPN Connect can be a valuable aid in troubleshooting many of the issues presented during operation. Enabling and accessing the VPN Connect log messages can be done via VPN Connect or the Logging Service.

- For an overview of the Logging Service in general, refer to Logging Overview on page 2574
- For details on enabling and accessing the VPN Connect log messages via the logging service, refer to Service Logs on page 2591
- For details on enabling and accessing the VPN Connect log messages via the Networking service, refer to Viewing Your VPN Connect Log Messages on page 3161
- For details on the VPN Connect log message schema, refer to Details for VPN Connect on page 2615

Tunnel Flapping

Interesting traffic at all times: In general, Oracle recommends having interesting traffic running through the IPSec tunnels at all times if your CPE supports it. Certain Cisco ASA versions require the SLA monitor to be configured, which keeps interesting traffic running through the IPSec tunnels. For more information, see the section for "IP SLA Configuration" in the Cisco ASA policy-based configuration template.

Multiple IPSEC Connections: You can use two IPSec connections for redundancy. If both IPSec connections have only a default route (0.0.0.0/0) configured, traffic will route to either of those connections because Oracle uses asymmetric routing. If you want one IPSec connection as primary and another one as backup, configure more-specific routes for the primary connection and less-specific routes (or the default route of 0.0.0.0/0) on the backup connection.

Encryption Domain: The Oracle VPN headend supports only a single encryption domain. If your policy includes multiple entries, the tunnel will flap or there will be connectivity problems in which only a single policy works at any one time.

Local IKE identifier: Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as cpe.example.com. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Maximum Transmission Unit (MTU): The standard internet MTU size is 1500 bytes. For more information on how to determine your MTU please see Overview of MTU on page 3329.

CPE Configuration

Local IKE identifier: Some CPE platforms do not allow you to change the local IKE identifier. If you cannot, you must change the remote IKE ID in the Oracle Console to match your CPE's local IKE ID. You can provide the value either when you set up the IPSec connection, or later, by editing the IPSec connection. Oracle expects the value to be either an IP address or a fully qualified domain name (FQDN) such as cpe.example.com. For instructions, see Changing the CPE IKE Identifier That Oracle Uses on page 3158.

Cisco ASA: Policy Based: Oracle recommends using a route-based configuration to avoid interoperability issues and to achieve tunnel redundancy with a single Cisco ASA device.

The Cisco ASA does not support route-based configuration for software versions older than 9.7.1. For the best results, if your device allows it, Oracle recommends that you upgrade to a software version that supports route-based configuration.

With policy-based configuration, you can configure only a single tunnel between your Cisco ASA and your dynamic routing gateway (DRG).

Multiple Tunnels If you have multiple tunnels up simultaneously, ensure that your CPE is configured to handle traffic coming from your VCN on any of the tunnels. For example, you need to disable ICMP inspection, configure TCP state bypass, and so on. For more details about the appropriate configuration, contact your CPE vendor's support.
**Encryption Domain Issues**

The Oracle VPN headends use route-based tunnels, but can work with policy-based tunnels with some caveats. See Encryption domains for policy-based tunnels on page 2948 for full details.

**Stateful security list rules:** If you're using stateful security list rules (for TCP, UDP, or ICMP traffic), you don't need to ensure that your security list has an explicit rule to allow ICMP type 3 code 4 messages because the Networking service tracks the connections and automatically allows those messages. Stateless rules require an explicit ingress security list rule for ICMP type 3 code 4 messages. Confirm that the instance firewalls are set up correctly.

**General VPN Connect Issues**

**IPSec tunnel is DOWN**

Check these items:

- **Basic configuration:** The IPSec tunnel consists of both phase-1 (ISAKMP) and phase-2 (IPSec) configuration. Confirm that both are configured correctly on your CPE device. See the configuration appropriate for your CPE device:
  
  List of configurations
  
  - Verified CPE Devices on page 2969
  - Using the CPE Configuration Helper on page 2970
  - Checkpoint:
    - Check Point: Route-Based on page 2972
    - Check Point: Policy-Based on page 2997
  - Cisco ASA:
    - Cisco ASA: Route-Based on page 3020
    - Cisco ASA: Policy-Based on page 3032
  - Cisco IOS on page 3046
  - FortiGate on page 3058
  - Furukawa Electric on page 3072
  - Juniper MX on page 3076
  - Juniper SRX on page 3089
  - Libreswan on page 3102
  - NEC IX Series on page 3110
  - Openswan on page 3119
  - Palo Alto on page 3120
  - WatchGuard on page 3153
  - Yamaha RTX Series on page 3153

- **Local and remote proxy IDs:** If you're using a policy-based configuration, check if your CPE is configured with more than one pair of local and remote proxy IDs (subnets). The Oracle VPN router supports only one pair. If your CPE has more than one pair, update the configuration to include only one pair, and choose one of the following two options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Local Proxy ID</th>
<th>Remote Proxy ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANY (or 0.0.0.0/0)</td>
<td>ANY (or 0.0.0.0/0)</td>
</tr>
<tr>
<td>2</td>
<td>On-premises CIDR (an aggregate that covers all the subnets of interest)</td>
<td>VCN's CIDR</td>
</tr>
</tbody>
</table>

- **NAT device:** If the CPE is behind a NAT device, the CPE IKE identifier configured on your CPE might not match the CPE IKE identifier Oracle is using (the public IP address of your CPE). If your CPE does not support setting the CPE IKE identifier on your end, you can provide Oracle with your CPE IKE identifier in the Oracle Console. For more information, see Overview of the IPSec VPN Components on page 2936.
**IPSec tunnel is UP, but no traffic is passing through**

Check these items:

- **Phase 2 (IPSec) configuration:** Confirm that the phase 2 (IPSec) parameters are configured correctly on your CPE device. See the configuration appropriate for your CPE device:
  
  List of configurations
  
  - Verified CPE Devices on page 2969
  - Using the CPE Configuration Helper on page 2970
  - Checkpoint:
    - Check Point: Route-Based on page 2972
    - Check Point: Policy-Based on page 2997
  - Cisco ASA:
    - Cisco ASA: Route-Based on page 3020
    - Cisco ASA: Policy-Based on page 3032
  - Cisco IOS on page 3046
  - FortiGate on page 3058
  - Furukawa Electric on page 3072
  - Juniper MX on page 3076
  - Juniper SRX on page 3089
  - Libreswan on page 3102
  - NEC IX Series on page 3110
  - Openswan on page 3119
  - Palo Alto on page 3120
  - WatchGuard on page 3153
  - Yamaha RTX Series on page 3153
  - **VCN security lists:** Ensure you've set up the VCN security lists to allow the desired traffic (both ingress and egress rules). Note that the VCN's default security list does not allow ping traffic (ICMP type 8 and ICMP type 0). You must add the appropriate ingress and egress rules to allow ping traffic.
  - **Firewall rules:** Ensure that your firewall rules allow both ingress and egress traffic with the Oracle VPN headend IPs and the VCN CIDR block.
  - **Asymmetric routing:** Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec VPN connection. Even if you configure one tunnel as primary and another as backup, traffic from your VCN to your on-premises network can use any tunnel that is "up" on your device. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.
  - **Cisco ASA:** Do not use the originate-only option with an Oracle IPSec VPN tunnel. It causes the tunnel's traffic to be inconsistently blackholed. The command is only for tunnels between two Cisco devices. Here's an example of the command that you should NOT use for the Oracle IPSec VPN tunnels:
    ```
    crypto map <map name> <sequence number> set connection-type originate-only
    ```

**IPSec tunnel is UP, but traffic is passing in only one direction**

Check these items:

- **Asymmetric routing:** Oracle uses asymmetric routing across the multiple tunnels that make up the IPSec VPN connection. Even if you configure one tunnel as primary and another as backup, traffic from your VCN to your on-premises network can use any tunnel that is "up" on your device. Configure your firewalls accordingly. Otherwise, ping tests or application traffic across the connection will not reliably work.
  - **Single tunnel preferred:** If you want to use only one of the tunnels, ensure that you have the proper policy or routing in place on the CPE to prefer that tunnel.
  - **Multiple IPSec connections:** If you have multiple IPSec connections with Oracle, make sure to specify more specific static routes for the preferred IPSec connection.
  - **VCN security lists:** Ensure that your VCN security lists allow traffic in both directions (ingress and egress).
• **Firewall rules:** Ensure that your firewall rules allow traffic in both directions with the Oracle VPN headend IPs and the VCN CIDR block.

**Troubleshooting an IPSec VPN with a Policy-Based Configuration**

**IPSec tunnel is DOWN**

Check these items:

• **Basic configuration:** The IPSec tunnel consists of both phase-1 (ISAKMP) and phase-2 (IPSec) configuration. Confirm that both are configured correctly on your CPE device. See the configuration appropriate for your CPE device:

  List of configurations
  
  • **Verified CPE Devices** on page 2969
  • **Using the CPE Configuration Helper** on page 2970
  • **Checkpoint:**
    • **Check Point: Route-Based** on page 2972
    • **Check Point: Policy-Based** on page 2997
  • **Cisco ASA:**
    • **Cisco ASA: Route-Based** on page 3020
    • **Cisco ASA: Policy-Based** on page 3032
  • **Cisco IOS** on page 3046
  • **FortiGate** on page 3058
  • **Furukawa Electric** on page 3072
  • **Juniper MX** on page 3076
  • **Juniper SRX** on page 3089
  • **Libreswan** on page 3102
  • **NEC IX Series** on page 3110
  • **Openswan** on page 3119
  • **Palo Alto** on page 3120
  • **WatchGuard** on page 3153
  • **Yamaha RTX Series** on page 3153

• **Local and remote proxy IDs:** If you're using a policy-based configuration, check if your CPE is configured with more than one pair of local and remote proxy IDs (subnets). The Oracle VPN router supports only one pair. If your CPE has more than one pair, update the configuration to include only one pair, and choose one of the following two options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Local Proxy ID</th>
<th>Remote Proxy ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANY (or 0.0.0.0/0)</td>
<td>ANY (or 0.0.0.0/0)</td>
</tr>
<tr>
<td>2</td>
<td>On-premises CIDR (an aggregate that covers all the subnets of interest)</td>
<td>VCN's CIDR</td>
</tr>
</tbody>
</table>

• **NAT device:** If the CPE is behind a NAT device, the CPE IKE identifier configured on your CPE might not match the CPE IKE identifier Oracle is using (the public IP address of your CPE). If your CPE does not support setting the CPE IKE identifier on your end, you can provide Oracle with your CPE IKE identifier in the Oracle Console. For more information, see **Overview of the IPSec VPN Components** on page 2936.

• **Cisco ASA:** Do not use the `originate-only` option with an Oracle IPSec VPN tunnel. It causes the tunnel's traffic to be inconsistently blackholed. The command is only for tunnels between two Cisco devices. Here's an example of the command that you should NOT use for the Oracle IPSec VPN tunnels: `crypto map <map name> <sequence number> set connection-type originate-only`
IPSec tunnel is UP but keeps flapping

Check these items:

- **Initiation of connection**: Ensure that your CPE device is initiating the connection.
- **Local and remote proxy IDs**: If you're using a policy-based configuration, check if your CPE is configured with more than one pair of local and remote proxy IDs (subnets). The Oracle VPN router supports only one pair. If your CPE has more than one pair, update the configuration to include only one pair, and choose one of the following two options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Local Proxy ID</th>
<th>Remote Proxy ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANY (or 0.0.0.0/0)</td>
<td>ANY (or 0.0.0.0/0)</td>
</tr>
<tr>
<td>2</td>
<td>On-premises CIDR (an aggregate that covers all the subnets of interest)</td>
<td>VCN's CIDR</td>
</tr>
</tbody>
</table>

- **Interesting traffic at all times**: In general, Oracle recommends having interesting traffic running through the IPSec tunnels at all times if your CPE supports it. Certain Cisco ASA versions require the SLA monitor to be configured, which keeps interesting traffic running through the IPSec tunnels. For more information, see the section for "IP SLA Configuration" in the Cisco ASA policy-based configuration template.

IPSec tunnel is UP but traffic is unsteady

Check these items:

- **Local and remote proxy IDs**: If you're using a policy-based configuration, check if your CPE is configured with more than one pair of local and remote proxy IDs (subnets). The Oracle VPN router supports only one pair. If your CPE has more than one pair, update the configuration to include only one pair, and choose one of the following two options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Local Proxy ID</th>
<th>Remote Proxy ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANY (or 0.0.0.0/0)</td>
<td>ANY (or 0.0.0.0/0)</td>
</tr>
<tr>
<td>2</td>
<td>On-premises CIDR (an aggregate that covers all the subnets of interest)</td>
<td>VCN's CIDR</td>
</tr>
</tbody>
</table>

- **Interesting traffic at all times**: In general, Oracle recommends having interesting traffic running through the IPSec tunnels at all times if your CPE supports it. Certain Cisco ASA versions require the SLA monitor to be configured, which keeps interesting traffic running through the IPSec tunnels. For more information, see the section for "IP SLA Configuration" in the Cisco ASA policy-based configuration template.

BGP Session Troubleshooting for VPN Connect

**BGP status is DOWN**

Check these items:

- **IPSec status**: For the BGP session to be up, the IPSec tunnel itself must be up.
- **BGP address**: Verify that both ends of the tunnel are configured with the correct BGP peering IP address.
- **ASN**: Verify that both ends of the tunnel are configured with the correct BGP local ASN and Oracle BGP ASN. Oracle’s BGP ASN for the commercial cloud is 31898. For the Government Cloud, see Oracle’s BGP ASN on page 154.
- **MD5**: Verify that MD5 authentication is disabled or not configured on your CPE device. The Oracle IPSec VPN does not support MD5 authentication.
• **Firewalls**: Verify that your on-premises firewall or access control lists are not blocking the following ports:
  - TCP port 179 (BGP)
  - UDP port 500 (IKE)
  - IP protocol port 50 (ESP)

If your CPE device's firewall is blocking TCP port 179 (BGP), the BGP neighborship state will always be down. Traffic cannot flow through the tunnel because the CPE device and Oracle router do not have any routes.

### BGP status is flapping

Check these items:

- **IPSec status**: For the BGP session to be up and not flapping, the IPSec tunnel itself must be up and not flapping.
- **Maximum prefixes**: Verify that you are advertising no more than 2000 prefixes. If you're advertising more, BGP won't be established.

### BGP status is UP, but no traffic is passing through

Check these items:

- **VCN security lists**: Ensure you've set up the VCN security lists to allow the desired traffic (both ingress and egress rules). Note that the VCN's default security list does not allow ping traffic (ICMP type 8 and ICMP type 0). You must add the appropriate ingress and egress rules to allow ping traffic.
- **Correct routes on both ends**: Verify that you have received the correct VCN routes from Oracle and the CPE device is using those routes. Likewise, verify that you are advertising the correct on-premises network routes over the IPSec VPN, and the VCN route tables use those routes.

### BGP status is UP, but traffic is passing in only one direction

Check these items:

- **VCN security lists**: Ensure that your VCN security lists allow traffic in both directions (ingress and egress).
- **Firewalls**: Verify that your on-premises firewall or access control lists are not blocking traffic to or from the Oracle end.
- **Asymmetric routing**: Oracle uses asymmetric routing. If you have multiple IPSec connections, ensure that your CPE device is configured for asymmetric route processing.
- **Redundant connections**: If you have redundant IPSec connections, ensure that they're both advertising the same routes.

### Troubleshooting Redundant VPN Connections

Remember these important notes:

- FastConnect uses BGP dynamic routing. IPSec connections can use either static routing or BGP, or a combination.
- For important details about routing and preferred routes when using redundant connections, see [Routing for the Oracle IPSec VPN](#) on page 2934.
- You can use two IPSec connections for redundancy. If both IPSec connections have only a default route (0.0.0.0/0) configured, traffic will route to either of those connections because Oracle uses asymmetric routing. If you want one IPSec connection as primary and another one as backup, configure more-specific routes for the primary connection and less-specific routes (or the default route of 0.0.0.0/0) on the backup connection.

### IPSec and FastConnect are both set up, but traffic is only passing through IPSec

Ensure that you use more specific routes for the connection you want as primary. If you're using the same routes for both IPSec and FastConnect, see the discussion of routing preferences in [Routing for the Oracle IPSec VPN](#) on page 2934.
Two on-premises data centers each have an IPSec connection to Oracle, but only one is passing traffic

Verify that both IPSec connections are up and ensure that you have asymmetric route processing enabled on the CPE.

If both IPSec connections have only a default route (0.0.0.0/0) configured, traffic will route to either of those connections because Oracle uses asymmetric routing. If you want one IPSec connection as primary and another one as backup, configure more-specific routes for the primary connection and less-specific routes (or the default route of 0.0.0.0/0) on the backup connection.

For more information about this type of setup, see Example Layout with Multiple Geographic Areas on page 2965.

FastConnect

The following topics have information about setting up Oracle Cloud Infrastructure FastConnect between your on-premises network and virtual cloud network (VCN):

- FastConnect Overview on page 3173
- FastConnect Requirements on page 3181
- FastConnect Redundancy Best Practices on page 3185
- Routing Details for Connections to Your On-Premises Network on page 2942
- FastConnect: With an Oracle Partner on page 3192
- FastConnect: With a Third-Party Provider on page 3200
- FastConnect: Colocation with Oracle on page 3210
- FastConnect Metrics on page 3236
- FastConnect Troubleshooting on page 3241

FastConnect Overview

Oracle Cloud Infrastructure FastConnect provides an easy way to create a dedicated, private connection between your data center and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections.

Uses for FastConnect

With FastConnect, you can choose to use private peering, public peering, or both.

- **Private peering**: To extend your existing infrastructure into a virtual cloud network (VCN) in Oracle Cloud Infrastructure (for example, to implement a hybrid cloud, or a lift and shift scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918).
- **Public peering**: To access public services in Oracle Cloud Infrastructure without using the internet. For example, Object Storage, the Oracle Cloud Infrastructure Console and APIs, or public load balancers in your VCN. Communication across the connection is with IPv4 public IP addresses. Without FastConnect, the traffic destined for public IP addresses would be routed over the internet. With FastConnect, that traffic goes over your private physical connection. For a list of the services available with public peering, see FastConnect Supported Cloud Services. For a list of the public IP address ranges (routes) that Oracle advertises, see FastConnect Public Peering Advertised Routes on page 3219.

In general it's assumed you'll use private peering, and you might also use public peering. Most of this documentation is relevant to both, with specific details called out for private versus public.

If you choose to have multiple paths from your on-premises network to Oracle, see Routing Details for Connections to Your On-Premises Network on page 2942.

IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.
How and Where to Connect

With FastConnect, there are different connectivity models to choose from.

Oracle Partners

- List of Oracle Cloud Infrastructure FastConnect partners
- Port speeds in 1-Gbps and 10-Gbps increments
- Instructions for integrating: FastConnect: With an Oracle Partner on page 3192

Third-Party Provider

- Port speed of 1 Gbps or 10 Gbps per cross-connect
- Instructions for integrating: FastConnect: With a Third-Party Provider on page 3200

Colocation with Oracle in an Oracle Cloud Infrastructure FastConnect Location

- List of Oracle Cloud Infrastructure FastConnect locations
- Port speed of 1 Gbps or 10 Gbps per cross-connect
- Instructions for integrating: FastConnect: Colocation with Oracle on page 3210

The following table summarizes several important requirements for each connectivity model.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>With Oracle Partner</th>
<th>With Third-Party Provider</th>
<th>Colocation with Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing requirements</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BGP support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Layer 3 support</td>
<td>Recommended</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Obtain a Letter of Authority (LOA) from Oracle</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Network connectivity</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Cross-connect</td>
<td>Yes (from the partner)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Redundant network connectivity</td>
<td>Recommended</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>Cloud connectivity solution architecture support</td>
<td>Recommended</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>FastConnect SKU</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Oracle Cloud Infrastructure Console user login (IAM policy unique setup)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tenancy established (see &quot;Setting Up Your Tenancy&quot; in the Oracle Cloud Infrastructure Getting Started Guide)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Networking**

**Concepts**

Here are some important concepts to understand (also see the following diagrams):

**FastConnect**

The general concept of a connection between your existing network and Oracle Cloud Infrastructure over a private physical network instead of the internet.

**FastConnect location**

A specific Oracle data center where you can connect to Oracle Cloud Infrastructure.

**METRO AREA**

A geographical area (for example, Ashburn) with multiple FastConnect locations. All locations in a metro area connect to the same set of availability domains for resiliency if there is failure in a single location.

**ORACLE PARTNER**

A network service provider that has integrated with Oracle in a FastConnect location. See the list of the Oracle partners in How and Where to Connect on page 3174. If your provider is in the list, see FastConnect: With an Oracle Partner on page 3192.

**THIRD-PARTY PROVIDER**

A network service provider that is NOT on the list of Oracle partners in How and Where to Connect on page 3174. If you have a third-party provider and want to use FastConnect, see FastConnect: With a Third-Party Provider on page 3200.

**COLOCATION**

The situation where your equipment is deployed into a FastConnect location. If your network service provider is not on the list of Oracle partners in How and Where to Connect on page 3174, you must colocate.

**CROSS-CONNECT**

In a colocation or third-party provider scenario, this is the physical cable connecting your existing network to Oracle in the FastConnect location.

**CROSS-CONNECT GROUP**

In a colocation or third-party provider scenario, this is a link aggregation group (LAG) that contains at least one cross-connect. You can add more cross-connects to a cross-connect group as your bandwidth needs increase. This is applicable only for colocation.

**VIRTUAL CLOUD NETWORK (VCN)**

Your virtual network in Oracle Cloud Infrastructure. You can use a VCN to extend your infrastructure into the cloud. For more information, see VCNs and Subnets on page 2821.

**DYNAMIC ROUTING GATEWAY (DRG)**

A virtual edge router attached to your VCN. Necessary for private peering. The DRG is a single point of entry for private traffic coming in to your VCN, whether it's over FastConnect or a VPN Connect link. After creating the DRG, you must attach it to your VCN and add a route for the DRG in the VCN's route table to enable traffic flow. Instructions for everything are included in the sections that follow.

**VIRTUAL CIRCUIT**

An isolated network path that runs over one or more physical network connections to provide a single, logical connection between the edge of your existing network and Oracle Cloud Infrastructure. Private virtual circuits support private peering, and public virtual circuits support public peering (see Uses for FastConnect on page 3173). Each virtual circuit is made up of information shared between you and Oracle (and also a partner if you're connecting through an Oracle partner). You could have multiple private virtual...
circuits, for example, to isolate traffic from different parts of your organization (one virtual circuit for 10.0.1.0/24; another for 172.16.0.0/16), or to provide redundancy.

**Basic Network Diagrams**

The diagrams in this section introduce the basic logical and physical connections involved in FastConnect. Details specific to private versus public peering are called out.

**General Concept of FastConnect**

The following diagram illustrates the two ways to connect to Oracle with FastConnect: either through colocation with Oracle in the FastConnect location, or through an Oracle partner. In both cases, the connection goes between the edge of your existing network and Oracle.

**Physical Connection**

The next two diagrams give more detail about the physical connections. They also show the metro area that contains the FastConnect location, and a VCN within an Oracle Cloud Infrastructure region.
The first diagram shows the colocation scenario, with your physical connection to Oracle within the FastConnect location.

The next diagram shows a scenario with either an Oracle partner or third-party provider. It shows your physical connection to the provider, and the provider's physical connection to Oracle within the FastConnect location.

**Logical Connection: Private Virtual Circuit**

The next two diagrams show a private virtual circuit, which is a single, logical connection between your edge and Oracle Cloud Infrastructure by way of your DRG. Traffic is destined for private IP addresses in your VCN.
The first diagram shows the colocation scenario.

![First Diagram]

The next diagram shows the scenario with either an Oracle partner or third-party provider.

![Second Diagram]

**Logical Connection: Public Virtual Circuit**

A public virtual circuit gives your existing network access to Oracle services in Oracle Cloud Infrastructure. For example, Object Storage, the Oracle Cloud Infrastructure Console and APIs, and public load balancers in your VCN. All communication across a public virtual circuit uses public IP addresses. For a list of services available with FastConnect public peering, see [FastConnect Supported Cloud Services](#). For a list of the public IP address ranges (routes) that Oracle advertises, see [FastConnect Public Peering Advertised Routes](#) on page 3219.
The first diagram shows the colocation scenario with both a private virtual circuit and a public virtual circuit. Notice that the DRG is not involved with the public virtual circuit, only the private virtual circuit.

Here are a few basics to know about public virtual circuits:

- You choose which of your organization's public IP prefixes you want to use with the virtual circuit. All prefix sizes are allowed. Oracle verifies your organization's ownership of each prefix before sending any traffic for it across the connection. Oracle's verification for a given prefix can take up to three business days. You can get the status of the verification of each prefix in the Oracle Console or API. **Oracle begins advertising the Oracle Cloud Infrastructure public IP addresses across the connection only after successfully verifying at least one of your public prefixes.**
- Configure your firewall rules to allow traffic coming from the Oracle public IP addresses.
- Your existing network can receive advertisements for Oracle's public IP addresses through multiple paths (for example: FastConnect and your internet service provider). Make sure to give FastConnect higher preference than your ISP. You must configure your edge appropriately so that traffic uses your desired path to receive the benefits of FastConnect. This is particularly important if you decide to also set up your existing network with private...
access to Oracle services. For important information about path preferences, see Routing Details for Connections to Your On-Premises Network on page 2942.

- You can add or remove public IP prefixes at any time by editing the virtual circuit. If you add a prefix, Oracle first verifies your company's ownership before advertising it across the connection. If you remove a prefix, Oracle stops advertising the prefix within a few minutes of your editing the virtual circuit.

**Oracle Partner Scenario: BGP Session to Either Oracle or the Oracle Partner**

This section is applicable if you're using FastConnect through an Oracle partner. A Border Gateway Protocol (BGP) session is established from your edge, but where it goes depends on which Oracle partner you use.

**Tip:**

For simplicity, the following diagrams show only a private virtual circuit. However, the location of the BGP session is the same for a public virtual circuit.

**To Oracle:** With some of the Oracle partners, the BGP session goes from your edge to Oracle, as shown in the following diagram. When setting up the virtual circuit with Oracle, you are asked to provide basic BGP peering information (see General Requirements on page 3182).

**To the Oracle partner:** With other Oracle partners, your BGP session goes from your edge to the partner's, as shown in the following diagram. When setting up the virtual circuit with Oracle, you are NOT asked for any BGP session information. Instead, you share BGP information with your Oracle partner. Notice that there's a separate BGP session that the partner establishes with Oracle.
To use FastConnect if you do not own a Public ASN or Public IP Address

If you use a Public ASN or Public IP Address loaned or leased from a third-party source, your third-party source must provide a Letter of Authorization (LOA) on your behalf before Oracle can allow the completion of FastConnect configuration.

The following additional steps are required to obtain approval when configuring public peering virtual connections:

1. Obtain an LOA from the third-party source that authorizes the Customer to use the Public ASN and or Public IP address. The LOA must contain:
   - Customer Name approved to the use the Public IP Address and Public ASN
   - The range of the Public IP Addresses and or the Public ASN must be explicitly listed
   - The third-party source who owns the Public IP Addresses and or the Public ASN
   - Third-party source authorization authority signatory
   - Contact email, phone number and address of third-party source
   - Your enterprise's contact email and phone number
   - Date of authorization and validity

2. Using the Console, open a service request on the tenancy and region where you wish to use the third-party provided Public ASN and Public IP Address.

3. Attach the LOA to the service request.

Once the service request is opened and the LOA is approved, Oracle will authorize the use of the Public ASN and or Public IP Address.

FastConnect with Access to Multiple VCNs

You can use a single FastConnect to access multiple VCNs. Different network scenarios are available depending on your needs and which FastConnect connectivity model you use. For more information, see these topics:

- Transit Routing: Access to Multiple VCNs in the Same Region on page 2780: This scenario can be used with either FastConnect or VPN Connect. It involves a single DRG, and multiple VCNs in a hub-and-spoke layout.
- FastConnect with Multiple DRGs and VCNs on page 2816: This scenario can be used only with FastConnect, and only if you're using a third-party provider or colocated with Oracle. It involves multiple DRGs and private virtual circuits.

What's Next?

See these topics to get started:

- FastConnect Requirements on page 3181
- FastConnect Redundancy Best Practices on page 3185
- Routing Details for Connections to Your On-Premises Network on page 2942
- FastConnect: With an Oracle Partner on page 3192
- FastConnect: With a Third-Party Provider on page 3200
- FastConnect: Colocation with Oracle on page 3210

FastConnect Requirements

This topic covers the requirements for implementing FastConnect.

For general information about FastConnect, see the articles listed for FastConnect on page 3173.

Before Getting Started: Learn and Plan

Here are basic things you need to do before getting started with FastConnect:

- **FastConnect concepts:** Be familiar with the basic concepts covered in FastConnect Concepts.
- **Limits increase:** If you are colocated with Oracle, you must ask Oracle to increase your account limits for cross-connects. By default, these limits are initially set to 0, and a request to create a cross-connect will fail. For instructions, see Requesting a Service Limit Increase on page 217. In your request, indicate the region where you need the resources. It can take a couple of business days for the limit increase to take effect.
Networking

- **Hardware and routing requirements**: Review the hardware and routing requirements.
- **Tenancy setup and compartment design**: If you haven't yet, set up your tenancy. Think about who needs access to Oracle Cloud Infrastructure and how. For more information, see “Setting Up Your Tenancy” in the Oracle Cloud Infrastructure Getting Started Guide. Specifically for FastConnect, see Required IAM Policy on page 3184 to understand the policy required to work with FastConnect components.
- **Cloud network design**: Design your virtual cloud network (VCN), including how you want to allocate your VCN's subnets, define security list rules, define route tables, set up load balancers, and so on. For more information, see Networking on page 2746.
- **Redundancy**: Think through your overall redundancy model to ensure your network can handle planned maintenance by Oracle or your organization, and unexpected failures of the various components. For best practices, see FastConnect Redundancy Best Practices on page 3185.
- **Public IP prefixes**: If you plan to set up a public virtual circuit, get the list of the public IP prefixes that you want to use with the connection. Oracle must validate your organization's ownership of each of the prefixes before advertising each one over the connection.
- **Cloud network setup**: Set up your VCN, subnets, DRG, security lists, IAM policies, and so on, according to your design.

**General Requirements**

Before getting started with FastConnect, ensure that you meet the following requirements:

- Oracle Cloud Infrastructure account, with at least one user with appropriate Oracle Cloud Infrastructure Identity and Access Management (IAM) permissions (for example, a user in the Administrators group).
- Network equipment that supports Layer 3 routing using BGP.
- For colocation with Oracle: Ability to connect using single mode fiber in your selected FastConnect location. Also see Hardware and Routing Requirements on page 3182.
- For connection to an Oracle partner: At least one physical network connection with the partner. Also see Hardware and Routing Requirements on page 3182.
- For connection to a third-party provider: At least one physical connection with the provider. Also see Hardware and Routing Requirements on page 3182.
- For private peering only: At least one existing DRG set up for your VCN.
- For public peering only: The list of public IP address prefixes that you want to use with the connection. Oracle will validate your ownership of each prefix.

**Important:**

If you intend to colocate with Oracle, you must ask Oracle to increase your account limits for cross-connects. These default limits are initially set to 0, and a without a specific request for a limit increase you won’t be able to create a valid cross-connect. For instructions on placing this request, see Requesting a Service Limit Increase on page 217. In your request, indicate the region where you need the resources. It can take a couple of business days for the limit increase to take effect.

**Hardware and Routing Requirements**

*If you're using an Oracle partner*

Here are general routing requirements for FastConnect. These are particularly relevant if your BGP session is between your edge and Oracle.

- **IP addressing supported**: IPv4. IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.
- **P2P IP addresses**:
  - For public virtual circuits, Oracle specifies the IP addresses.
  - For private virtual circuits where your BGP session is between your edge and Oracle, you specify these addresses (/30 or /31, and one pair per virtual circuit). If you set up multiple private virtual circuits that go to the same DRG, you must use a different address on your edge router for each virtual circuit.
• **Maximum IP MTU:** 9000
• **Routing protocol:** BGPv4
• **BGP prefix limit:** For public virtual circuits: 200 prefixes. For private virtual circuits: 2000 prefixes.
• **BGP ASN:** 2-byte or 4-byte ASNs are supported, except for those listed in *Special-Purpose Autonomous System (AS) Numbers*. Public virtual circuits require a public ASN. Oracle's BGP ASN for the commercial cloud is 31898. For the US Government Cloud, see Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171. BGP ASN 65534 is not available for you to use with FastConnect and VPN. All other private ASNs in the 64512 - 65533 (inclusive) range defined in RFC-6996 can be used normally.
• **BGP MD5 authentication:** Optional to use with your virtual circuit. Oracle supports up to 128-bit MD5 authentication
• **BGP keep-alive interval:** 60s
• **BGP hold-time interval:** 180s

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>By default, Oracle uses the default BGP timers of 60 seconds for keep-alive and 180 seconds for hold-time. If you need fast BGP convergence, you can use any value in these supported ranges: 6-60 seconds for keep-alive, and 18-180 seconds for hold-time.</td>
</tr>
</tbody>
</table>

*If you’re colocating in a FastConnect location or using a third-party provider*

For the cross-connect group and cross-connects:

• **Bandwidth (three choices):**
  • 1 Gbps:
    • 1000Base-LX, 10-km range, 1310 nm
    • **You must configure your edge device so that auto-negotiation is OFF**
    • Minimum Rx level > -15 dBm
  • 10 Gbps:
    • 10 GbE, LR (10-km range), 1310 nm
    • Minimum Rx level > -12 dBm
  • 100 Gbps:
    • 100GBASE, LR4 QSFP28 (10-km range), WDM optics
    • CrossConnect Groups (LAG/LACP) are not currently supported
    • Minimum Rx level > -12 dBm on each of four lanes

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Gbps speeds are available to select customers only. Please work with your account representative to gain access to these ports.</td>
</tr>
</tbody>
</table>

• **General:**
  • Single Mode Fiber
  • Duplex LC connectors

• **Redundancy:**
  • Device redundancy highly recommended
  • In some regions, location redundancy is available and recommended

• **Capacity:**
  • 1 GbE: Minimum 1, Maximum 8
  • 10 GbE: Minimum 1, Maximum 8
  • 100 GbE: 1 only

• **LAG protocol:** LACP with short timers (3 @ 1s). If your router doesn't support LAG, you can set up a single non-LAG cross-connect.
• **VLAN tagging**: 802.1q (single tag)
• **VLAN range**: 100-4094 (you assign the VLANs)
• **Maximum interface MTU**: 9196 (include 4-byte FCS trailer)

For routing:

• **IP addressing supported**: IPv4. IPv6 addressing is currently supported only in the US Government Cloud. For more information, see IPv6 Addresses on page 2889.

• **P2P IP addresses**:
  • For public virtual circuits, Oracle specifies the IP addresses.
  • For private virtual circuits, you specify the addresses (a /30 or /31). You need one pair of IP addresses per private virtual circuit. If you set up multiple private virtual circuits that go to the same DRG, you must use a different address on your edge router for each virtual circuit.

• **Maximum IP MTU**: 9000
• **Routing protocol**: BGPv4
• **BGP prefix limit**: For public virtual circuits: 200 prefixes. For private virtual circuits: 2000 prefixes.
• **BGP ASN**: 2-byte or 4-byte ASNs are supported, except for those listed in Special-Purpose Autonomous System (AS) Numbers. Public virtual circuits require a public ASN. Oracle's BGP ASN is 31898. For the US Government Cloud, see Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171. BGP ASN 65534 is not available for you to use with FastConnect and VPN. All other private ASNs in the 64512 - 65533 (inclusive) range defined in RFC-6996 can be used normally.

• **BGP MD5 authentication**: Optional to use with your virtual circuit. Oracle supports up to 128-bit MD5 authentication
• **BGP keep-alive interval**: 60s
• **BGP hold-time interval**: 180s

**Tip:**
By default, Oracle uses the default BGP timers of 60 seconds for keep-alive and 180 seconds for hold-time. If you need fast BGP convergence, you can use any value in these supported ranges: 6-60 seconds for keep-alive, and 18-180 seconds for hold-time.

**Required IAM Policy**

*If you're using an Oracle partner*

To work with Networking resources such as dynamic routing gateways (DRGs), VCNs, and virtual circuits, you need to have a user login to the Console, and your user needs sufficient authority (by way of an IAM policy) to perform all the instructions below. If your user is in the Administrators group, you have the required authority.

If your user is not, then a policy like this would generally cover all the Networking resources:

```bash
Allow group NetworkAdmins to manage virtual-network-family in tenancy
```

To only create and manage a virtual circuit, you would need a policy like this:

```bash
Allow group VirtualCircuitAdmins to manage drgs in tenancy
Allow group VirtualCircuitAdmins to manage virtual-circuits in tenancy
```

The first statement (to manage DRGs) is necessary only for private virtual circuits.

For more information, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

*If you're colocating in a FastConnect location or using a third-party provider*

To work with Networking resources such as dynamic routing gateways (DRGs), VCNs, virtual circuits, and cross-connects, you need to have a user login to the Console, and your user needs sufficient authority (by way of an IAM policy) to perform all the instructions below. If your user is in the Administrators group, you have the required authority.

If your user is not, then a policy like this would generally cover all the Networking resources:

```bash
Allow group NetworkAdmins to manage virtual-network-family in tenancy
```

To only create and manage a virtual circuit, you would need a policy like this:

```bash
Allow group VirtualCircuitAdmins to manage drgs in tenancy
Allow group VirtualCircuitAdmins to manage virtual-circuits in tenancy
```

The first statement (to manage DRGs) is necessary only for private virtual circuits.

For more information, see Getting Started with Policies on page 2135 and Common Policies on page 2142.
policy) to perform all the instructions that follow. If your user is in the Administrators group, you have the required authority.

If your user is not, then a policy like this would generally cover all the Networking resources:

```
Allow group NetworkAdmins to manage virtual-network-family in tenancy
```

To only create and manage cross-connects, cross-connect groups, and virtual circuits, you would need a policy like this:

```
Allow group FastConnectAdmins to manage drgs in tenancy
Allow group FastConnectAdmins to manage cross-connects in tenancy
Allow group FastConnectAdmins to manage cross-connect-groups in tenancy
Allow group FastConnectAdmins to manage virtual-circuits in tenancy
```

The first statement (to manage DRGs) is necessary only for private virtual circuits.

For more information, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Identifiers for Your FastConnect Resources**

Your resources have several identifiers:

- **Name for the overall connection:** When you create a new FastConnect connection, you can give it a descriptive name of your choice. If you don't specify one, Oracle automatically assigns a name to the connection.

- **Reference name for each cross-connect:** Each cross-connect has an optional reference name. If you set up a cross-connect, Oracle recommends that you fill in the reference name with the identifier for the cross-connect's physical fiber cable. That makes it easier for Oracle to help if future troubleshooting is required for the connection. After cabling is done and you have the identifier from the data center, you can add it to the cross-connect's information in the Oracle Console.

- **OCID for each resource:** Each cross-connect group, cross-connect, and virtual circuit has its own unique Oracle-assigned identifier called an OCID.

**What's Next?**

Choose the topic that suits your situation:

- FastConnect: With an Oracle Partner on page 3192
- FastConnect: With a Third-Party Provider on page 3200
- FastConnect: Colocation with Oracle on page 3210

**FastConnect Redundancy Best Practices**

This topic covers best practices for redundancy when implementing FastConnect.

For general information about FastConnect, see FastConnect on page 3173.

**Overview**

In general, you should design your network to achieve high availability (HA). In addition, you should be prepared for these types of disruptions:

- Regularly scheduled maintenance by your organization, your provider (if you're using one), or Oracle.
- Unexpected failures on the part of your networking components, your provider, or Oracle. Failures are rare, but you should plan for them.

For redundancy, Oracle provides:

- Multiple providers for each region
• Two **FastConnect locations** for each of the following regions (all other regions have a single FastConnect location)
  - Germany Central (Frankfurt)
  - UK South (London)
  - US East (Ashburn)
  - US West (Phoenix)
• Two routers in each FastConnect location
• Multiple physical connections between each Oracle partner and Oracle (for a given region)

The redundancy best practices depend on which connectivity model you use. Also see How and Where to Connect on page 3174.

**If You Use an Oracle Partner**

Connectivity model:
• **FastConnect: With an Oracle Partner** on page 3192

Oracle handles redundancy of the physical connections between the partner and Oracle, and the redundancy of routers in the FastConnect locations. You should handle redundancy of the physical connection between your existing network and the Oracle partner.

The remaining best practices depend on the partner you're using, and details of the BGP session from your edge:
• For some partners, the BGP session from your edge goes to Oracle. For redundancy best practices, see the next section.
• For other partners, the BGP session from your edge goes to the Oracle partner. For redundancy best practices, see Oracle Partner Scenario: Your BGP Session Is to the Oracle Partner on page 3187.

For information about the two scenarios, see Basic Network Diagrams on page 3176.

**Oracle Partner Scenario: Your BGP Session Is to Oracle**

At a minimum, each Oracle partner has two separate physical connections to Oracle. Set up one virtual circuit on one physical connection (as primary), and the other virtual circuit on another physical connection (as secondary). The following diagram illustrates two virtual circuits, each going to a different router in a single FastConnect location. If the region has a second location, your partner's second physical connection might instead go to that location.

If you're working in a region that has only a single FastConnect location, you might also want location diversity. To achieve that, repeat the preceding setup of two virtual circuits with the same Oracle partner, but in a second FastConnect location in a nearby region. Notice that you must have a duplicate setup of your Oracle cloud resources in that second region, as shown in the following diagram.
If you also want provider diversity, repeat your entire setup with another provider in each region that you're using.

**Oracle Partner Scenario: Your BGP Session Is to the Oracle Partner**

In this scenario, the BGP session *from your edge* goes to the Oracle partner (as shown in the following diagram). Separate from your BGP session, the Oracle partner has *its own* BGP sessions with Oracle (between the partner's edge and Oracle's edge). The virtual circuit is a logical connection that goes from your edge to the Oracle edge.

The partner has two separate physical connections to Oracle. You create one virtual circuit with the partner. In this scenario, the virtual circuit is automatically designed to be redundant and diverse. The virtual circuit has two separate BGP sessions between the partner and Oracle, each on a different physical connection. The following diagram shows the two separate BGP sessions for the single virtual circuit as dotted lines.
Separately, you must ensure that the connection between your edge and the partner is redundant and diverse.

If you're working in a region that has only a single FastConnect location, you might also want location diversity. To achieve that, repeat the preceding setup of a virtual circuit with the same Oracle partner, but in a second FastConnect location in a nearby region. Notice that you must also have a duplicate setup of your Oracle cloud resources in that second region, as shown in the following diagram.
If You Use a Third-Party Provider or Colocate with Oracle

Connectivity models:

- FastConnect: With a Third-Party Provider on page 3200
- FastConnect: Colocation with Oracle on page 3210

Oracle handles redundancy of the Oracle routers in the FastConnect locations. You should handle redundancy of the physical connection between your existing network and Oracle.

To do this, create two physical connections to Oracle, one for each FastConnect location that serves the region. This means that in the Oracle Console, you set up two separate FastConnect connections. You then create two virtual circuits. Set up the first one on the first physical connection (the first FastConnect connection), and the second one on the second physical connection. The following diagram shows the general setup.
Networking

You might prefer to connect to only a single FastConnect location because of cost concerns, or if the region has only a single FastConnect location. In that case, create two physical connections and ensure each goes to a different Oracle router in that FastConnect location. You can do this in the Oracle Console when you set up the second physical connection. You can specify the proximity of that connection to other FastConnect connections in that location. For example, the following image shows how to request that your second physical connection (which is a cross-connect group) is created on a different router than your first connection in that FastConnect location (called MyConnection-1).

You must scale the bandwidth of both physical connections evenly, and by using a cross-connect group (LAG) for each connection. Imagine that you have two individual 10 Gbps cross-connects in a single FastConnect location (each to a different Oracle router for redundancy and diversity). If you need to have 20-Gbps bandwidth at a given time, you must ensure that each of your physical connections consists of a cross-connect group (LAG) to contain the cross-connect. Then you need to add another 10 Gbps cross-connect to each LAG, so that each redundant physical connection has two 10 Gbps cross-connects. FastConnect currently does not support equal-cost multi-path routing (ECMP).

If you're working in a region that has only a single FastConnect location, you might also want location diversity. To achieve that, repeat your setup in a second FastConnect location in a nearby region. Notice that you must also have a duplicate setup of your Oracle cloud resources in that second region, as shown in the following diagram.
VPN Connect as Backup for FastConnect

Oracle recommends using VPN Connect as a backup for your FastConnect connection. If you do, ensure that the VPN Connect tunnels are configured to use BGP routing with a route-based VPN. Within your existing on-premises network, manipulate the routing to prefer routes learned through FastConnect over routes learned through VPN Connect. For example, use AS_Path Prepend to influence egress traffic from Oracle, and use local preference to influence egress traffic from your network.

If you are using VPN backup, review Oracle's BGP routing behavior in the table shown in Routing Preferences for Traffic from Oracle to Your On-Premises Network on page 2943.

The following diagram shows a setup with redundant FastConnect virtual circuits and redundant VPN Connect tunnels.
Related Resources

- Routing Details for Connections to Your On-Premises Network on page 2942
- Connectivity Redundancy Guide (PDF)

What’s Next?

Choose the topic that suits your situation:

- FastConnect: With an Oracle Partner on page 3192
- FastConnect: With a Third-Party Provider on page 3200
- FastConnect: Colocation with Oracle on page 3210

FastConnect: With an Oracle Partner

This topic is for customers who want to use Oracle Cloud Infrastructure FastConnect by connecting to an Oracle partner. For a summary of the different ways to connect, see the connectivity models.

If you instead want to use a network provider that is not on the list of Oracle partners, see FastConnect: With a Third-Party Provider on page 3200. Or if you want to use FastConnect by collocating with Oracle, see FastConnect: Colocation with Oracle on page 3210.

For general information about FastConnect, see FastConnect on page 3173.
Getting Started with FastConnect

The following flow chart shows the overall process of setting up FastConnect.

Also see the sequence diagram in To get the status of your virtual circuit on page 3197.

Task 1: Learn and plan

If you haven't yet, walk through the planning in Before Getting Started: Learn and Plan on page 3181. Also see FastConnect Redundancy Best Practices on page 3185.

Task 2: Set up connection to the Oracle partner

If you haven't already, start the process of ordering the connection from the Oracle partner, setting it up, and then testing it with the partner. It can take some time, depending on the partner.

Task 3: Set up a DRG (private peering only)

Summary: If you plan to use a private virtual circuit (private peering), you need a DRG. If you haven't already, use the Oracle Cloud Infrastructure Console to set up a DRG, attach it to your VCN, and update routing in your VCN to include a route rule to send traffic to the DRG. It's easy to forget to update the route table. Without the route rule, no traffic will flow.

Instructions:

- To create a DRG on page 2929
- To attach a DRG to a VCN on page 2930
• To update rules in an existing route table on page 2925

Task 4: Set up your virtual circuit

Summary: Create one or more virtual circuits for your connection in the Oracle Console. If your network design includes more than one virtual circuit, complete the following steps for each one.

Instructions:
Repeat the following steps for each virtual circuit you want to create.

1. In the Console, confirm you're viewing the compartment that you want to work in. If you're not sure which one, use the compartment that contains the DRG that you'll connect to (for a private virtual circuit). The choice of compartment, along with a corresponding IAM policy, controls who has access to the virtual circuit you're about to create.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
   The resulting FastConnect page is where you'll create a new connection and later return to when you need to manage the connection.
3. Click Create FastConnect.
4. Select FastConnect Partner and choose the partner from the list.
5. Click Next.
6. Enter the following for your virtual circuit:
   - Name: A friendly name that helps you track your virtual circuits. The value does not need to be unique across your virtual circuits, and you can change it later. Avoid entering confidential information.
   - Create in Compartment: Leave as is (the compartment you're currently working in).
7. Choose the virtual circuit type (private or public). A private virtual circuit is for private peering (where your existing network receives routes for your VCN's private IP addresses). A public virtual circuit is for public peering.
Networking

(where your existing network receives routes for the Oracle Cloud Infrastructure public IP addresses). Also see Uses for FastConnect on page 3173.

- For a private virtual circuit, enter the following:
  - **Dynamic Routing Gateway:** Select the DRG to route the FastConnect traffic to.
  - **Provisioned Bandwidth:** Choose a value. If your bandwidth needs increase later, you can update the virtual circuit to use a different value (see To edit a virtual circuit on page 3198).

If your BGP session goes to Oracle (see Basic Network Diagrams on page 3176), the dialog box includes other fields for the BGP session:

- **Customer BGP IP Address:** The BGP peering IP address for your edge (your CPE), with either a /30 or /31 subnet mask.
- **Oracle BGP IP Address:** The BGP peering IP address you want to use for the Oracle edge (the DRG), with either a /30 or /31 subnet mask.
- **Enable IPv6 Address Assignment:** Available only in the Government Cloud. For more information, see FastConnect and IPv6 on page 2897.
- **Customer BGP ASN:** The public or private ASN for your network.
- **Use a BGP MD5 Authentication Key (optional):** Select this check box and provide a key if your system requires MD5 authentication. Oracle supports up to 128-bit MD5 authentication.

- For a public virtual circuit, enter the following:
  - **Provisioned Bandwidth:** Choose a value. If your bandwidth needs increase later, you can update the virtual circuit to use a different value (see To edit a virtual circuit on page 3198).
  - **Public IP Prefixes:** The public IP prefixes that you want Oracle to receive over the connection. All prefix sizes are allowed. You can enter a comma-separated list of prefixes, or one per line.
  - **Customer BGP ASN:** The public ASN for your network. Present only if your BGP session goes to Oracle (see Basic Network Diagrams on page 3176). Oracle specifies the BGP IP addresses for a public virtual circuit.
  - **Use a BGP MD5 Authentication Key (optional):** Select this check box and provide a key if your system requires MD5 authentication. Oracle supports up to 128-bit MD5 authentication.

8. **Click Create.**

The virtual circuit is created. Its OCID and a link to the partner's portal are displayed in the resulting confirmation box at the top of the page. The OCID is also available with the other virtual circuit details.

9. **Copy and paste the OCID to another location. You give it to your partner in the next task.**

The virtual circuit is listed on the FastConnect page.

Until you complete the next task and the partner does their provisioning work, the virtual circuit's Lifecycle State is PENDING PROVIDER and the BGP state is DOWN. After the partner does their work, the Lifecycle State switches to PROVISIONED. When the BGP session is established and working, the BGP state changes to UP.

**Tip:**

For a virtual circuit where your BGP session goes to the Oracle partner, the BGP state for the virtual circuit reflects the status of the separate BGP session between the Oracle partner and Oracle. For reference, see Basic Network Diagrams on page 3176.

Also see the diagram in To get the status of your virtual circuit on page 3197.

**Task 5: Give the partner information about the virtual circuit**

Contact the partner and give the OCID of each virtual circuit that you created, along with any other information the partner requests. Depending on the partner, you might do this in the partner's portal, or over the phone. The partner then configures each virtual circuit on their end to complete the connectivity.

If your partner is AT&T: After AT&T gives you the service key for your virtual circuit, create a ticket at My Oracle Support to request provisioning, and give Oracle the service key.
Task 6: Configure your edge

If your BGP session goes to Oracle: (see Basic Network Diagrams on page 3176), configure your edge (your CPE) to use the BGP peering information (see General Requirements on page 3182). Oracle's BGP ASN for the commercial cloud is 31898. For the Government Cloud, see Oracle's BGP ASN on page 154. By default, Oracle uses the default BGP timers of 60 seconds for keep-alive and 180 seconds for hold-time. If you need fast BGP convergence, you can use any value in these supported ranges: 6-60 seconds for keep-alive, and 18-180 seconds for hold-time. Also configure the router for redundancy according to the network design you decided on earlier (see FastConnect Redundancy Best Practices on page 3185). After you successfully configure the BGP session, the virtual circuit's BGP session state changes to UP.

If your BGP session instead goes to the Oracle partner: You still need to configure your router if you haven't already. You may need to contact your partner to get the required BGP peering information. This BGP session must be up and running for FastConnect to work. Also configure your edge router for redundancy according to the network design you decided on earlier (see FastConnect Redundancy Best Practices on page 3185).

Important:

For a public virtual circuit: Your existing network can receive advertisements for Oracle's public IP addresses through multiple paths (for example: FastConnect and your internet service provider). Make sure to give FastConnect higher preference than your ISP. You must configure your edge appropriately so that traffic uses your desired path to receive the benefits of FastConnect. This is particularly important if you decide to also set up your existing network with private access to Oracle services. For important information about path preferences, see Routing Details for Connections to Your On-Premises Network on page 2942.

Task 7: Check light levels

Confirm that the light levels are good for each of your physical network connections to the partner. Don't proceed until they are.

Task 8: Confirm your interfaces are up

Confirm your side of the interfaces for the connections to the partner are up. Don't proceed until they are.

BGP Session Goes to Oracle

Task 9a: Ping the Oracle BGP IP address

For each virtual circuit, ping the Oracle BGP IP address assigned to the virtual circuit. Check the error counters and look for any dropped packets. Don't proceed until you can successfully ping this IP address without errors.

Task 9b: Confirm that the BGP session is established

For each virtual circuit, confirm that the BGP session is in an established state. When it is, the connection is ready to test (see Task 11: Test the connection on page 3197).

BGP Session Goes to the Partner

Task 10a: Ping the partner's edge

For each virtual circuit, ping the partner's edge. Check the error counters and look for any dropped packets. Don't proceed until you can successfully ping the partner's edge without errors.

Task 10b: Confirm the BGP session is established

Confirm the BGP session you have with the partner is in an established state. Don't proceed until it is.

Task 10c: Ping the Oracle BGP IP address

For each virtual circuit, ping the Oracle BGP IP address (which you can get from the partner). Check the error counters and look for any dropped packets. When you can successfully ping this IP address without errors, the connection is ready to test.
Networking

Task 11: Test the connection

For a private virtual circuit: You should be able to launch an instance in your VCN and access it (for example, with SSH) from a host in your existing private network. See Creating an Instance on page 695. If you can, your FastConnect private virtual circuit is ready to use.

For a public virtual circuit:

1. Make sure that Oracle has successfully verified at least one of the public prefixes you've submitted. You can see the status of each prefix by viewing the virtual circuit's details in the Console. When one of the prefixes has been validated, Oracle starts advertising the regional Oracle Cloud Infrastructure public addresses over the connection.
2. Launch an instance with a public IP address.
3. Ping the public IP address from a host in your existing private network. You should see the packet on the FastConnect interface on the virtual circuit. If you do, your FastConnect public virtual circuit is ready to use. However, remember that only the public prefixes that Oracle has successfully verified so far are advertised on the connection.

Managing Your Virtual Circuit

To get the status of your virtual circuit

1. In the Console, go to Networking, and then click FastConnect to view your list of connections.
2. Click the virtual circuit you're interested in to view its details.

The following diagram shows the different states of the virtual circuit when you're setting it up.
To edit a virtual circuit

You can change these items for a virtual circuit:

- The name
- The bandwidth
- Which DRG it uses (for a private virtual circuit)
- The public IP prefixes (for a public virtual circuit)
- Depending on the situation, you might also have access to the BGP session information for the virtual circuit and thus can change it.
Important:

If your virtual circuit is working and in the PROVISIONED state before you edit it, be aware that changing any of the properties besides the name, bandwidth, and public prefixes (for a public virtual circuit) causes the virtual circuit's state to switch to PROVISIONING and may cause the related BGP session to go down. After Oracle re-provisions the virtual circuit, its state returns to PROVISIONED. Make sure you confirm that the associated BGP session is back up.

If you change the public IP prefixes for a public virtual circuit, the BGP status is unaffected. Oracle begins advertising a new IP prefix over the connection only after verifying your ownership of it. The virtual circuit's state changes to PROVISIONING while Oracle implements any prefix changes.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Edit and make your changes. Avoid entering confidential information.
4. Click Save Changes.

To terminate a virtual circuit

Important:

Also terminate the connection with the partner, or else the partner may continue to bill you.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Delete.
4. Confirm when prompted.

The virtual circuit's Lifecycle State changes to TERMINATING and then to TERMINATED.

To manage public IP prefixes for a public virtual circuit

For general information about the prefixes, see Basic Network Diagrams on page 3176.

You can specify your public IP prefixes when you create the virtual circuit. See Task 4: Set up your virtual circuit on page 3194.

You can add or remove public IP prefixes later after creating the virtual circuit. See To edit a virtual circuit on page 3198. If you add a new prefix, Oracle first verifies your company's ownership before advertising it across the connection. If you remove a prefix, Oracle stops advertising the prefix within a few minutes of your editing the virtual circuit.

You can view the state of Oracle's verification of a given public prefix by viewing the virtual circuit's details in the Console. Here are the possible values:

- **In progress**: Oracle is in the process of verifying your organization's ownership of the prefix.
- **Failed**: Oracle could not verify your organization's ownership. Oracle will not advertise the prefix over the virtual circuit.
- **Completed**: Oracle successfully verified your organization's ownership. Oracle is advertising the prefix over the virtual circuit.

To move a connection to a different compartment

You can move a connection from one compartment to another. After you move the connection to the new compartment, inherent policies apply immediately and affect access to the connection through the Console. Moving the connection to a different compartment does not affect the connection between your data center and Oracle Cloud Infrastructure. For more information, see Moving a Compartment to a Different Parent Compartment on page 2435.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Find the connection in the list, click the Actions icon (three dots), and then click **Move Resource**.
3. Choose the destination compartment from the list.
4. Click **Move Resource**.
5. If there are alarms monitoring the connection, update the alarms to reference the new compartment. See To update an alarm after moving a resource on page 2737 for more information.

**Monitoring Your Connection**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring your connection, see FastConnect Metrics on page 3236.

**Troubleshooting**

See FastConnect Troubleshooting on page 3241.

**FastConnect: With a Third-Party Provider**

This topic is for customers who want to use Oracle Cloud Infrastructure FastConnect by connecting to a third-party network provider of their choice, and not an Oracle partner. For a summary of the different ways to connect, see the connectivity models.

If you are using an Oracle partner, see FastConnect: With an Oracle Partner on page 3192. Or, if you want to use FastConnect by colocating with Oracle, see FastConnect: Colocation with Oracle on page 3210.

For general information about FastConnect, see FastConnect on page 3173.

**Important Points and Responsibilities**

- You can use FastConnect by working with a third-party network service provider or carrier of your choice. The network provider must be capable of connecting to the Oracle routers in one of the FastConnect data center locations over single-mode fiber. For more detailed technical requirements, see Hardware and Routing Requirements on page 3182.

- Your overall connection with the third-party provider includes two parts, as illustrated in the following diagram:
  - **Part 1**: Your physical connection to the third-party provider. The rest of this topic assumes you’ve already set up this part of the overall connection.
  - **Part 2**: The physical fiber connection (cross-connect) that the third-party provider sets up in the FastConnect location data center on your behalf.

  ![Diagram](https://example.com/diagram.png)

- To obtain the Letter of Authorization (LOA) for the cross-connect, you must use the Oracle Console to **set up a cross-connect or cross-connect group**. The resulting LOA from Oracle covers part 2 of the connection in the preceding diagram.
- You must forward the LOA to your third-party provider, who is responsible for working with the data center to set up the physical cross-connect on your behalf.
• The third-party provider issues a cross-connect order with the data center facility to run fiber optics to complete the connection from the third-party provider's cage to Oracle's patch panel as described in the LOA. Typically the data center colocation staff are the ones who run the fiber optics to complete the connection.

• Each LOA is valid for only a limited time. If the physical cross-connect is not set up before the LOA's expiration, the LOA is revoked.

• **The third-party provider is responsible for charging you for the entire connection (both parts 1 and 2).** Oracle does not set up this cross-connect in the data center, does not pay for it, and does not include it in your FastConnect charges.

• The LOA specifies an Oracle demarcation point. If your network provider is located at a different demarcation point in the data center cage, they must set up the cross-connect from their demarcation point to the Oracle demarcation point.

**Getting Started with FastConnect**

The following flow chart shows the overall process of setting up FastConnect.

**Note:**

In general, this topic assumes that your router supports link aggregation (LAG) and you will set up a cross-connect group (a LAG) with at least one cross-connect in it. The following procedures and screenshots reflect that. However, if your router doesn't support link aggregation, you can instead set up a single non-LAG cross-connect (with no cross-connect group). The procedures in this topic are still generally applicable. Instead you work only with a single cross-connect and not one or more in a cross-connect group.
Task 1: Learn and plan

If you haven’t yet, walk through the planning in Before Getting Started: Learn and Plan on page 3181. Also see FastConnect Redundancy Best Practices on page 3185.

Task 2: Set up a DRG (private peering only)

Summary: If you plan to use a private virtual circuit (private peering), you need a DRG. If you haven’t already, use the Oracle Cloud Infrastructure Console to set up a DRG, attach it to your VCN, and update routing in your VCN to include a route rule to send traffic to the DRG. It’s easy to forget to update the route table. Without the route rule, no traffic will flow.

Instructions:
- To create a DRG on page 2929
- To attach a DRG to a VCN on page 2930
- To update rules in an existing route table on page 2925

Task 3: Set up your cross-connect group and cross-connect

Summary: Create a connection in the Console, which consists of a cross-connect group (for link aggregation, or LAG) that contains at least one cross-connect. If you need more cross-connects in the group, you can add them later. You can have a maximum of eight cross-connects in a group.

You have the option to set up a single non-LAG cross-connect (with no cross-connect group) if your router does not support link aggregation (LAG).
Instructions:

1. In the Console, confirm you're viewing the compartment that you want to work in. If you're not sure which one, use the compartment that contains the DRG that you'll connect to (for a private virtual circuit). This choice of compartment, in conjunction with a corresponding IAM policy, controls who has access to the cross-connect group and each cross-connect you're about to create.

2. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.

   The resulting FastConnect page is where you'll create a new connection and later return to when you need to manage the connection and its components.

3. Click Create FastConnect.

4. Select Colocate with Oracle and click Next. Select this option even though a third-party provider will set up the physical connection to Oracle in the FastConnect location.

5. Enter the following items:
   - **Name:** A descriptive name that helps you keep track of this connection. You can't change the name later. Avoid entering confidential information. If you're creating a cross-connect group (LAG), the cross-connect group will use this name. Each cross-connect in this group will also use it, but with a hyphen and number appended (for example, MyName-1, MyName-2, and so on).
   - **Compartment:** Leave as is (the compartment you're currently working in).
   - **Cross-Connect Type:**
     - If your router supports LAG, select Cross-Connect Group. You will create a cross-connect group (a LAG) with at least one cross-connect.
     - If your router does not support link aggregation (LAG), select Single Cross-Connect. You will create a single non-LAG cross-connect with no cross-connect group.
   - **Reference Name:** The ID for the physical LAG for the cross-connect group. This makes future connection troubleshooting easier. You might need to get this value from your third-party provider. If you don't have it, you can add it later. If you're creating a single non-LAG cross-connect, enter the ID for the physical fiber cable for the cross-connect.
   - **Number of cross-connects:** Available only if you're creating a cross-connect group. This is the number of individual cross-connects to create in the cross-connect group. In the Console, you can create three. If you need more, you can add more cross-connects later (total eight in a cross-connect group).
   - **Port speed:** 1 Gbps, 10 Gbps, or 100 Gbps.

   **Note:**

   100 Gbps speeds are available to select customers only. Please work with your account representative to gain access to these ports.

   - **Physical location:** The FastConnect location for this connection.
   - **Specify Router Proximity:** Optionally specify whether you want the new connection to be on the same or different router than one of your other connections.

6. Click Create.

   The new connection is created and listed on the FastConnect page.

7. Click the new connection to see its details.

8. **Print the LOA for each cross-connect:** Each cross-connect you just created has a Letter of Authorization (LOA). View each cross-connect's details, and then view and print the cross-connect's LOA. In the next task, you forward
Networking

it to your third-party provider so they can request cabling at the FastConnect location. The cross-connect's status is PENDING CUSTOMER until you complete the next few tasks.

Task 4: Forward the LOA to your third-party provider

Forward the LOA or LOAs from the preceding task to your third-party network provider so they can request cabling at the FastConnect location. Each LOA is valid for a limited time. The details are printed on the LOA.

Task 5: Check light levels

After the third-party provider completes setup of the physical cross-connect in the FastConnect location, confirm from your side that the light levels for each physical connection (cross-connect) are good (> -15 dBm). Don’t proceed until they are.

In the Console, you can see the light levels that Oracle detects by viewing the details of the cross-connect, as shown in the following screenshot:

If they are not good, contact your third-party network provider.

Task 6: Confirm that your interfaces are up

For each cross-connect’s physical fiber cable, confirm your side of the interfaces are up. Don’t proceed until they are.

In the Console, you can see the status of Oracle’s side of the interfaces (up or down) by viewing the details of the cross-connect (see the preceding screenshot).

If the interfaces are not up, contact your third-party network provider.
**Task 7: Activate each cross-connect**

**Summary:** When your physical fiber cables in the FastConnect location are set up and ready to use, return to the Oracle Console and activate each cross-connect that you set up earlier. The process of activating a cross-connect informs Oracle that the corresponding physical fiber cable is ready. Oracle will then complete the router configuration for each cross-connect.

**Instructions:**
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click through to view the cross-connect's details, and then click Activate.
4. Confirm when prompted.
5. While still viewing the cross-connect's details, click Edit and enter the ID for the physical fiber cable for this cross-connect. Adding this value can help with any connection troubleshooting in the future. If you don't have the value available now, you can add it later.

If you have other cross-connects that are ready to use, wait for the first to be provisioned, and then activate the next one. Only one cross-connect in a group can be activated and then provisioned at a time. After you complete this task, each cross-connect's status changes to PROVISIONING and then to PROVISIONED (typically within one minute).

**Task 8: Set up your virtual circuit**

**Summary:** Create one or more virtual circuits for your connection in the Oracle Console. The cross-connect group (or your single non-LAG cross-connect) must first be in the PROVISIONED state.

**Important:**

If you want to use a single FastConnect to connect your existing network to multiple DRGs and VCNs, you must set up a different private virtual circuit for each VCN. Each virtual circuit must have a different VLAN and a different set of BGP IP addresses. For more information, see FastConnect with Multiple DRGs and VCNs on page 2816.

**Instructions:**
1. In the Console, return to the connection you created earlier. Under Resources, click Virtual Circuits.
2. Click Add Virtual Circuit.
3. Enter the following for your virtual circuit:
   - **Name:** A descriptive name that helps you keep track of your virtual circuits. The value does not need to be unique across your virtual circuits, and you can change it later. Avoid entering confidential information.
   - **Compartment:** Select the compartment where you want to create the virtual circuit. If you're not sure, use the current compartment. This choice of compartment, in conjunction with a corresponding IAM policy, controls who has access to the virtual circuit.
4. Choose the virtual circuit type (private or public). A private virtual circuit is for private peering (where your existing network receives routes for your VCN's private IP addresses). A public virtual circuit is for public peering.
Networking

(where your existing network receives routes for the Oracle Cloud Infrastructure public IP addresses). Also see Uses for FastConnect on page 3173.

• For a private virtual circuit, enter the following:

  - **Dynamic Routing Gateway**: Select the DRG to route the FastConnect traffic to.
  - **Provisioned Bandwidth**: Choose your desired value. If your bandwidth needs increase later, you can update the virtual circuit to use a different value (see To edit a virtual circuit on page 3217).
  - **VLAN**: The number of the VLAN to use for this virtual circuit. It must be a VLAN that is not already assigned to another virtual circuit.
  - **Customer BGP IP Address**: The BGP peering IP address for your edge (your CPE), with either a /30 or /31 subnet mask.
  - **Oracle BGP IP Address**: The BGP peering IP address you want to use for the Oracle edge (the DRG), with either a /30 or /31 subnet mask.
  - **Enable IPv6 Address Assignment**: Available only in the US Government Cloud. For more information, see FastConnect and IPv6 on page 2897.
  - **Customer BGP ASN**: The public or private ASN for your network.
  - **Use a BGP MD5 Authentication Key (optional)**: Select this check box and provide a key if your system requires MD5 authentication. Oracle supports up to 128-bit MD5 authentication.

• For a public virtual circuit, enter the following:

  - **Provisioned Bandwidth**: Choose your desired value. If your bandwidth needs increase later, you can update the virtual circuit to use a different value (see To edit a virtual circuit on page 3217).
  - **Public IP Prefixes**: The public IP prefixes that you want Oracle to receive over the connection. All prefix sizes are allowed. You can enter a comma-separated list of prefixes, or one per line.
  - **VLAN**: The number of the VLAN to use for this virtual circuit. It must be a VLAN that is not already assigned to another virtual circuit.
  - **Customer BGP ASN**: The public ASN for your network. Note that Oracle specifies the BGP IP addresses for a public virtual circuit.
  - **Use a BGP MD5 Authentication Key (optional)**: Select this check box and provide a key if your system requires MD5 authentication. Oracle supports up to 128-bit MD5 authentication.

5. Click **Create**.

The virtual circuit is created.

The virtual circuit's status is PROVISIONING briefly while Oracle's system provisions the virtual circuit. The status then switches to DOWN if the BGP session between your edge and Oracle's edge is not yet correctly configured, if the VLAN isn't configured correctly, or if there any other problems. Otherwise the status switches to UP.

**Task 9: Configure your edge**

Configure each of your edge routers to use the BGP information and VLAN for the virtual circuit. Oracle's BGP ASN for the commercial cloud is 31898. For the Government Cloud, see Oracle's BGP ASN on page 154. By default, Oracle uses the default BGP timers of 60 seconds for keep-alive and 180 seconds for hold-time. If you need fast BGP convergence, you can use any value in these supported ranges: 6-60 seconds for keep-alive, and 18-180 seconds for hold-time.

**Important:**

For a public virtual circuit: Your existing network can receive advertisements for Oracle's public IP addresses through multiple paths (for example: FastConnect and your internet service provider). Make sure to give FastConnect higher preference than your ISP. You must configure your edge appropriately so that traffic uses your desired path to receive the benefits of FastConnect. This is particularly important if you decide to also set up your existing network with private access to Oracle services. For important information about path preferences, see Routing Details for Connections to Your On-Premises Network on page 2942.
If you have a cross-connect group (a LAG) with one or more cross-connects in it, here are details to know about LACP:

- LACP is required on the network interface that is directly plugged in to Oracle's router.
- LACP is required even if you have only a single cross-connect in the cross-connect group.
- If the third-party provider is performing any media conversion, LACP must be configured on the provider's device instead of your device.

Also configure the router for redundancy according to the network design you decided on earlier. After you successfully configure BGP and the VLAN, the virtual circuit's status will switch to UP.

**Task 10: Ping the Oracle BGP IP address**

Ping the Oracle BGP IP address assigned to the virtual circuit. Check the error counters and look for any dropped packets. Don't proceed until you can successfully ping this IP address without errors.

If you've set up a cross-connect group: if the ping is not successful, and you're NOT learning MAC addresses, verify that you configured LACP as mentioned in Task 9.

**Task 11: Confirm that the BGP session is established**

For each virtual circuit you set up, confirm the BGP session is in an established state on your side of the connection.

**Task 12: Test the connection**

**For a private virtual circuit:** You should be able to launch an instance in your VCN and access it (for example, with SSH) from a host in your existing private network. See [Creating an Instance](page-695) on page 695. If you can, your FastConnect private virtual circuit is ready to use.

**For a public virtual circuit:**

1. Make sure that Oracle has successfully verified *at least one* of the public prefixes you've submitted. You can see the status of each prefix by viewing the virtual circuit's details in the Console. When one of the prefixes has been validated, Oracle starts advertising the regional Oracle Cloud Infrastructure public addresses over the connection.
2. Launch an instance with a public IP address.
3. Ping the public IP address from a host in your existing private network. You should see the packet on the FastConnect interface on the virtual circuit. If you do, your FastConnect public virtual circuit is ready to use. However, remember that *only the public prefixes that Oracle has successfully verified so far* are advertised on the connection.

**Managing Your Connection**

**To get the status of your connection**

Look at the icon for the particular part of the connection that you're interested in (cross-connect group, cross-connect, or virtual circuit).

Here are reasons for particular status values:

**Cross-Connect: PENDING CUSTOMER**

- You need to forward the LOA to your third-party provider so they can request cabling at the FastConnect location. See [Task 4: Forward the LOA to your third-party provider](page-3204) on page 3204.
- Or, you need to activate a cross-connect after confirming it's ready to use. See [Task 7: Activate each cross-connect](page-3205) on page 3205, but make sure you've performed tasks 5 and 6 first.

**Virtual circuit: DOWN**

In general this means you've created a virtual circuit, but configuration is incomplete or incorrect:

- You need to configure your edge. See [Task 9: Configure your edge](page-3206) on page 3206.
- Or, you've configured BGP or the VLAN incorrectly on your edge (make sure to configure the router to use the BGP and VLAN values assigned to the virtual circuit).
The following table summarizes the different states of each component involved in the connection at different points during setup:

<table>
<thead>
<tr>
<th>Task in Setup Process</th>
<th>CCG Icon</th>
<th>CC Icon</th>
<th>VC Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 3: Set up your cross-connect group and cross-connect</td>
<td>PENDING</td>
<td>PENDING CUSTOMER</td>
<td>N/A</td>
</tr>
<tr>
<td>on page 3202</td>
<td>PROVISIONING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 7: Activate each cross-connect on page 3205</td>
<td>PROVISIONED</td>
<td>PROVISIONED</td>
<td>N/A</td>
</tr>
<tr>
<td>Task 8: Set up your virtual circuit on page 3205</td>
<td>PROVISIONED</td>
<td>PROVISIONED</td>
<td>PROVISIONING &gt; DOWN</td>
</tr>
<tr>
<td>Task 9: Configure your edge on page 3206</td>
<td>PROVISIONED</td>
<td>PROVISIONED</td>
<td>DOWN &gt; UP</td>
</tr>
</tbody>
</table>

To add a new cross-connect to an existing cross-connect group

When you first create a cross-connect group in the Console, you're allowed to create three cross-connects in the group. You can later add more to increase the bandwidth and resiliency of the group. The total allowed number is eight.

1. Create the new cross-connect in the existing cross-connect group:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
   b. Select the compartment where the connection resides, and then click the connection to view its details.
   c. Click Add Cross-Connect.
   d. Enter the following items:
      • **Name:** A descriptive name that helps you keep track of this cross-connect. The value does not need to be unique across your cross-connects. You can't change the name later. Avoid entering confidential information.
      • **Reference Name:** Your ID for the physical fiber cable for the cross-connect. This makes future connection troubleshooting easier. If you don't have it, you can add it later.
   e. Click Add.
      The cross-connect is created. The status of the cross-connect is PENDING CUSTOMER to indicate that you have more work to do.
   f. Print the new cross-connect's LOA. You forward it to your third-party provider in the next step.
2. Perform tasks 4-7 in Getting Started with FastConnect on page 3201. In summary, you need to have the cabling set up for the new cross-connect, validate the light levels and interfaces are good, and then activate the cross-connect.

To edit a virtual circuit

You can change these items for a virtual circuit:

• The name
• The bandwidth
• Which DRG it uses (for a private virtual circuit)
• Which VLAN it uses
• The BGP session information
• The public IP prefixes (for a public virtual circuit)

**Important:**

Notes About Editing a Virtual Circuit
If your virtual circuit is working and in the PROVISIONED state before you edit it, be aware that changing any of the properties besides the name, bandwidth, and public prefixes (for a public virtual circuit) causes the virtual circuit's state to switch to PROVISIONING and may cause the related BGP session to go down. After Oracle re-provisions the virtual circuit, its state returns to PROVISIONED. Make sure you confirm that the associated BGP session is back up.

If you change the public IP prefixes for a public virtual circuit, the BGP status is unaffected. Oracle begins advertising a new IP prefix over the connection only after verifying your ownership of it. The virtual circuit's state changes to PROVISIONING while Oracle implements any prefix changes.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Virtual Circuits, and then click the virtual circuit to view its details.
4. Click Edit and make your changes. Avoid entering confidential information.
5. Click Save Changes.

To terminate a connection, or part of it

To stop being billed for a connection, you must terminate the virtual circuit, each cross-connect, and the cross-connect group associated with the connection (in that order).

Important:
Also terminate the connection with the data center or third-party provider, or else they may continue to bill you.

To terminate a virtual circuit

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Virtual Circuits, and then click the virtual circuit to view its details.
4. Click Delete.
5. Confirm when prompted.

The virtual circuit's status changes to TERMINATING and then to TERMINATED.

To terminate a cross-connect

If you have multiple cross-connects to delete in a cross-connect group, wait until the state of the first one changes to TERMINATED before deleting the next one. Also, you can't delete a cross-connect if it's the last provisioned cross-connect in a cross-connect group that's being used by a provisioned virtual circuit.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Cross-Connects, and then click the cross-connect to view its details.
4. Click Delete.
5. Confirm when prompted.

The cross-connect's status changes to TERMINATING and then to TERMINATED.

To terminate a cross-connect group

Prerequisite: The cross-connect group must have no virtual circuits running on it and contain no cross-connects.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Delete.
4. Confirm when prompted.
The cross-connect group's status changes to TERMINATING and then to TERMINATED.

To manage public IP prefixes for a public virtual circuit

For general information about the prefixes, see Basic Network Diagrams on page 3176.

You can specify your public IP prefixes when you create the virtual circuit. See Task 8: Set up your virtual circuit on page 3214.

You can add or remove public IP prefixes later after creating the virtual circuit. See To edit a virtual circuit on page 3217. If you add a new prefix, Oracle first verifies your company's ownership before advertising it across the connection. If you remove a prefix, Oracle stops advertising the prefix within a few minutes of your editing the virtual circuit.

You can view the state of Oracle's verification of a given public prefix by viewing the virtual circuit's details in the Console. Here are the possible values:

- **In progress**: Oracle is in the process of verifying your organization's ownership of the prefix.
- **Failed**: Oracle could not verify your organization's ownership. Oracle will not advertise the prefix over the virtual circuit.
- **Completed**: Oracle successfully verified your organization's ownership. Oracle is advertising the prefix over the virtual circuit.

To move a connection to a different compartment

You can move a connection from one compartment to another. After you move the connection to the new compartment, inherent policies apply immediately and affect access to the connection through the Console. Moving the connection to a different compartment does not affect the connection between your data center and Oracle Cloud Infrastructure. For more information, see To move a resource to a different compartment on page 2444.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Find the connection in the list, click the the Actions icon (three dots), and then click Move Resource.
3. Choose the destination compartment from the list.
4. Click Move Resource.
5. If there are alarms monitoring the connection, update the alarms to reference the new compartment. See To update an alarm after moving a resource on page 2737 for more information.

Monitoring Your Connection

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring your connection, see FastConnect Metrics on page 3236.

Troubleshooting

See FastConnect Troubleshooting on page 3241.

FastConnect: Colocation with Oracle

This topic is for customers who are colocated with Oracle in a FastConnect location. For a summary of the different ways to connect, see the connectivity models.

If you instead have a relationship with an Oracle partner, see FastConnect: With an Oracle Partner on page 3192. Or if you have a relationship with a third-party provider, see FastConnect: With a Third-Party Provider on page 3200.

For general information about FastConnect, see FastConnect on page 3173.
Getting Started with FastConnect

The following flow chart shows the overall process of setting up FastConnect.

Note:

In general, this topic assumes that your router supports link aggregation (LAG) and you will set up a cross-connect group (a LAG) with at least one cross-connect in it. The following procedures and screenshots reflect that. However, if your router doesn't support link aggregation, you can instead set up a single non-LAG cross-connect (with no cross-connect group). The procedures in this topic are still generally applicable. Instead you work only with a single cross-connect and not one or more in a cross-connect group.

Task 1: Learn and plan

If you haven't yet, walk through the planning in Before Getting Started: Learn and Plan on page 3181. Also see FastConnect Redundancy Best Practices on page 3185.

Task 2: Set up a DRG (private peering only)

Summary: If you plan to use a private virtual circuit (private peering), you need a DRG. If you haven't already, use the Oracle Cloud Infrastructure Console to set up a DRG, attach it to your VCN, and update routing in your VCN to include a route rule to send traffic to the DRG. It's easy to forget to update the route table. Without the route rule, no traffic will flow.
Instructions:

- To create a DRG on page 2929
- To attach a DRG to a VCN on page 2930
- To update rules in an existing route table on page 2925

Task 3: Set up your cross-connect group and cross-connect

Summary: Create a connection in the Console, which consists of a cross-connect group (for link aggregation, or LAG) that contains at least one cross-connect. If you need more cross-connects in the group, you can add them later. You can have a maximum of eight cross-connects in a group.

You have the option to set up a single non-LAG cross-connect (with no cross-connect group) if your router does not support link aggregation (LAG).

Instructions:

1. In the Console, confirm you're viewing the compartment that you want to work in. If you're not sure which one, use the compartment that contains the DRG that you'll connect to (for a private virtual circuit). This choice of compartment, in conjunction with a corresponding IAM policy, controls who has access to the cross-connect group and each cross-connect you're about to create.

2. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.

   The resulting FastConnect page is where you'll create a new connection and later return to when you need to manage the connection and its components.

3. Click Create FastConnect.

4. Select Colocate with Oracle and click Next.

5. Enter the following items:

   - Name: A descriptive name that helps you keep track of this connection. You can't change the name later. Avoid entering confidential information. If you're creating a cross-connect group (LAG), the cross-connect group will use this name. Each cross-connect in this group will also use it, but with a hyphen and number appended (for example, MyName-1, MyName-2, and so on).
   - Compartment: Leave as is (the compartment you're currently working in).
   - Cross-Connect Type:
     - If your router supports LAG, select Cross-Connect Group. You will create a cross-connect group (a LAG) with at least one cross-connect.
     - If your router does not support link aggregation (LAG), select Single Cross-Connect. You will create a single non-LAG cross-connect with no cross-connect group.
   - Reference Name: The ID for the physical LAG for the cross-connect group. This makes future connection troubleshooting easier. If you don't have it, you can add it later. If you're creating a single non-LAG cross-connect, enter the ID for the physical fiber cable for the cross-connect.
   - Number of cross-connects: Available only if you're creating a cross-connect group. This is the number of individual cross-connects to create in the cross-connect group. In the Console, you can create three. If you need more, you can add more cross-connects later (total eight in a cross-connect group).
   - Port speed: 1 Gbps, 10 Gbps, or 100 Gbps.

   **Note:**

   100 Gbps speeds are available to select customers only. Please work with your account representative to gain access to these ports.

   - Physical location: The FastConnect location for this connection.
   - Specify Router Proximity: Optionally specify whether you want the new connection to be on the same or different router than one of your other connections.
6. Click **Create**.

   The new connection is created and listed on the FastConnect page.

7. Click the new connection to see its details.

8. **Print the LOA for each cross-connect**: Each cross-connect you just created has a Letter of Authorization (LOA). View each cross-connect’s details, and then view and print the cross-connect’s LOA. In the next task, you submit it with your cabling request at the FastConnect location. The cross-connect’s status is PENDING CUSTOMER until you complete the next few tasks.

![MyConnection](image)

**Task 4: Submit LOA and request cabling in the FastConnect location**

At the FastConnect location, submit each LOA from the preceding task and request cabling for each cross-connect. Each LOA is valid for a limited time. The details are printed on the LOA.

**Task 5: Check light levels**

For each cross-connect’s physical fiber cable, confirm from your side that the light levels are good (> -15 dBm). Don’t proceed until they are.

In the Console, you can see the light levels that Oracle detects by viewing the details of the cross-connect, as shown in the following screenshot:

![MyConnection](image)

**Task 6: Confirm that your interfaces are up**

For each cross-connect’s physical fiber cable, confirm your side of the interfaces are up. Don’t proceed until they are.

In the Console, you can see the status of Oracle’s side of the interfaces (up or down) by viewing the details of the cross-connect (see the preceding screenshot).
Task 7: Activate each cross-connect

Summary: When your physical fiber cables in the FastConnect location are set up and ready to use, return to the Oracle Console and activate each cross-connect that you set up earlier. The process of activating a cross-connect informs Oracle that the corresponding physical fiber cable is ready. Oracle will then complete the router configuration for each cross-connect.

Instructions:
1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click through to view the cross-connect's details, and then click Activate.
4. Confirm when prompted.
5. While still viewing the cross-connect's details, click Edit and enter the ID for the physical fiber cable for this cross-connect. Adding this value can help with any connection troubleshooting in the future. If you don't have the value available now, you can add it later.

If you have other cross-connects that are ready to use, wait for the first to be provisioned, and then activate the next one. Only one cross-connect in a group can be activated and then provisioned at a time. After you complete this task, each cross-connect's status changes to PROVISIONING and then to PROVISIONED (typically within one minute).

Task 8: Set up your virtual circuit

Summary: Create one or more virtual circuits for your connection in the Oracle Console. The cross-connect group (or your single non-LAG cross-connect) must first be in the PROVISIONED state.

Instructions:
1. In the Console, return to the connection you created earlier. Under Resources, click Virtual Circuits.
2. Click Add Virtual Circuit.
3. Enter the following for your virtual circuit:
   - **Name**: A descriptive name that helps you keep track of your virtual circuits. The value does not need to be unique across your virtual circuits, and you can change it later. Avoid entering confidential information.
   - **Compartment**: Select the compartment where you want to create the virtual circuit. If you're not sure, use the current compartment. This choice of compartment, in conjunction with a corresponding IAM policy, controls who has access to the virtual circuit.
4. Choose the virtual circuit type (private or public). A private virtual circuit is for private peering (where your existing network receives routes for your VCN's private IP addresses). A public virtual circuit is for public peering.
Networking

(where your existing network receives routes for the Oracle Cloud Infrastructure public IP addresses). Also see Uses for FastConnect on page 3173.

- For a private virtual circuit, enter the following:
  - **Dynamic Routing Gateway**: Select the DRG to route the FastConnect traffic to.
  - **Provisioned Bandwidth**: Choose your desired value. If your bandwidth needs increase later, you can update the virtual circuit to use a different value (see To edit a virtual circuit on page 3217).
  - **VLAN**: The number of the VLAN to use for this virtual circuit. It must be a VLAN that is not already assigned to another virtual circuit.
  - **Customer BGP IP Address**: The BGP peering IP address for your edge (your CPE), with either a /30 or /31 subnet mask.
  - **Oracle BGP IP Address**: The BGP peering IP address you want to use for the Oracle edge (the DRG), with either a /30 or /31 subnet mask.
  - **Enable IPv6 Address Assignment**: Available only in the US Government Cloud. For more information, see FastConnect and IPv6 on page 2897.
  - **Customer BGP ASN**: The public or private ASN for your network.
  - **Use a BGP MD5 Authentication Key (optional)**: Select this check box and provide a key if your system requires MD5 authentication. Oracle supports up to 128-bit MD5 authentication.

- For a public virtual circuit, enter the following:
  - **Provisioned Bandwidth**: Choose your desired value. If your bandwidth needs increase later, you can update the virtual circuit to use a different value (see To edit a virtual circuit on page 3217).
  - **Public IP Prefixes**: The public IP prefixes that you want Oracle to receive over the connection. All prefix sizes are allowed. You can enter a comma-separated list of prefixes, or one per line.
  - **VLAN**: The number of the VLAN to use for this virtual circuit. It must be a VLAN that is not already assigned to another virtual circuit.
  - **Customer BGP ASN**: The public ASN for your network. Note that Oracle specifies the BGP IP addresses for a public virtual circuit.
  - **Use a BGP MD5 Authentication Key (optional)**: Select this check box and provide a key if your system requires MD5 authentication. Oracle supports up to 128-bit MD5 authentication.

5. Click Create.

The virtual circuit is created.

The virtual circuit's status is PROVISIONING briefly while Oracle's system provisions the virtual circuit. The status then switches to DOWN if the BGP session between your edge and Oracle's edge is not yet correctly configured, if the VLAN isn't configured correctly, or if there any other problems. Otherwise the status switches to UP.

**Task 9: Configure your edge**

Configure each of your edge routers to use the BGP information and VLAN for the virtual circuit. Oracle's BGP ASN for the commercial cloud is 31898. For the Government Cloud, see Oracle's BGP ASN on page 154. By default, Oracle uses the default BGP timers of 60 seconds for keep-alive and 180 seconds for hold-time. If you need fast BGP convergence, you can use any value in these supported ranges: 6-60 seconds for keep-alive, and 18-180 seconds for hold-time.

**Important:**

For a public virtual circuit: Your existing network can receive advertisements for Oracle’s public IP addresses through multiple paths (for example: FastConnect and your internet service provider). Make sure to give FastConnect higher preference than your ISP. You must configure your edge appropriately so that traffic uses your desired path to receive the benefits of FastConnect. This is particularly important if you decide to also set up your existing network with private access to Oracle services. For important information about path preferences, see Routing Details for Connections to Your On-Premises Network on page 2942.
If you have a cross-connect group (a LAG) with one or more cross-connects in it, here are details to know about LACP:

- LACP is required on the network interface that is directly plugged in to Oracle's router.
- LACP is required even if you have only a single cross-connect in the cross-connect group.
- If the third-party provider is performing any media conversion, LACP must be configured on the provider's device instead of your device.

Also configure the router for redundancy according to the network design you decided on earlier. After you successfully configure BGP and the VLAN, the virtual circuit's status will switch to UP.

**Task 10: Ping the Oracle BGP IP address**

Ping the Oracle BGP IP address assigned to the virtual circuit. Check the error counters and look for any dropped packets. Don't proceed until you can successfully ping this IP address without errors.

If you've set up a cross-connect group: if the ping is not successful, and you're NOT learning MAC addresses, verify that you configured LACP as mentioned in Task 9.

**Task 11: Confirm that the BGP session is established**

For each virtual circuit you set up, confirm the BGP session is in an established state on your side of the connection.

**Task 12: Test the connection**

**For a private virtual circuit:** You should be able to launch an instance in your VCN and access it (for example, with SSH) from a host in your existing private network. See Creating an Instance on page 695. If you can, your FastConnect private virtual circuit is ready to use.

**For a public virtual circuit:**

1. Make sure that Oracle has successfully verified at least one of the public prefixes you've submitted. You can see the status of each prefix by viewing the virtual circuit's details in the Console. When one of the prefixes has been validated, Oracle starts advertising the regional Oracle Cloud Infrastructure public addresses over the connection.
2. Launch an instance with a public IP address.
3. Ping the public IP address from a host in your existing private network. You should see the packet on the FastConnect interface on the virtual circuit. If you do, your FastConnect public virtual circuit is ready to use. However, remember that only the public prefixes that Oracle has successfully verified so far are advertised on the connection.

**Managing Your Connection**

**To get the status of your connection**

Look at the icon for the particular part of the connection that you're interested in (cross-connect group, cross-connect, or virtual circuit).

Here are reasons for particular status values:

**Cross-Connect: PENDING CUSTOMER**

- You need to submit the LOA and request cabling at the FastConnect location. See Task 4: Submit LOA and request cabling in the FastConnect location on page 3213.
- Or, you need to activate a cross-connect after confirming it's ready to use. See Task 7: Activate each cross-connect on page 3214, but make sure you've performed tasks 5 and 6 first.

**Virtual circuit: DOWN**

In general this means you've created a virtual circuit, but configuration is incomplete or incorrect:

- You need to configure your edge. See Task 9: Configure your edge on page 3215.
- Or, you've configured BGP or the VLAN incorrectly on your edge (make sure to configure the router to use the BGP and VLAN values assigned to the virtual circuit).
The following table summarizes the different states of each component involved in the connection at different points during setup:

<table>
<thead>
<tr>
<th>Task in Setup Process</th>
<th>CCG Icon</th>
<th>CC Icon</th>
<th>VC Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 3: Set up your cross-connect group and cross-connect</td>
<td>PENDING</td>
<td>PENDING CUSTOMER</td>
<td>N/A</td>
</tr>
<tr>
<td>on page 3212</td>
<td>PROVISIONING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 7: Activate each cross-connect on page 3214</td>
<td>PROVISIONED</td>
<td>PROVISIONED</td>
<td>N/A</td>
</tr>
<tr>
<td>Task 8: Set up your virtual circuit on page 3214</td>
<td>PROVISIONED</td>
<td>PROVISIONED</td>
<td>PROVISIONING &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>Task 9: Configure your edge on page 3215</td>
<td>PROVISIONED</td>
<td>PROVISIONED</td>
<td>DOWN &gt; UP</td>
</tr>
</tbody>
</table>

To add a new cross-connect to an existing cross-connect group

When you first create a cross-connect group in the Console, you're allowed to create three cross-connects in the group. You can later add more to increase the bandwidth and resiliency of the group. The total allowed number is eight.

1. Create the new cross-connect in the existing cross-connect group:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
   b. Select the compartment where the connection resides, and then click the connection to view its details.
   c. Click Add Cross-Connect.
   d. Enter the following items:
      • **Name**: A descriptive name that helps you keep track of this cross-connect. The value does not need to be unique across your cross-connects. You can't change the name later. Avoid entering confidential information.
      • **Reference Name**: Your ID for the physical fiber cable for the cross-connect. This makes future connection troubleshooting easier. If you don't have it, you can add it later.
   e. Click Add.
      The cross-connect is created. The status of the cross-connect is PENDING CUSTOMER to indicate that you have more work to do.
   f. Print the new cross-connect's LOA. You submit it with your cabling order in the next step.
2. Perform tasks 4-7 in Getting Started with FastConnect on page 3211. In summary, you need to have the cabling set up for the new cross-connect, validate the light levels and interfaces are good, and then activate the cross-connect.

To edit a virtual circuit

You can change these items for a virtual circuit:
- The name
- The bandwidth
- Which DRG it uses (for a private virtual circuit)
- Which VLAN it uses
- The BGP session information
- The public IP prefixes (for a public virtual circuit)

**Important:**

Notes About Editing a Virtual Circuit
If your virtual circuit is working and in the PROVISIONED state before you edit it, be aware that changing any of the properties besides the name, bandwidth, and public prefixes (for a public virtual circuit) causes the virtual circuit's state to switch to PROVISIONING and may cause the related BGP session to go down. After Oracle re-provisions the virtual circuit, its state returns to PROVISIONED. Make sure you confirm that the associated BGP session is back up.

If you change the public IP prefixes for a public virtual circuit, the BGP status is unaffected. Oracle begins advertising a new IP prefix over the connection only after verifying your ownership of it. The virtual circuit's state changes to PROVISIONING while Oracle implements any prefix changes.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Virtual Circuits, and then click the virtual circuit to view its details.
4. Click Edit and make your changes. Avoid entering confidential information.
5. Click Save Changes.

To terminate a connection, or part of it

To stop being billed for a connection, you must terminate the virtual circuit, each cross-connect, and the cross-connect group associated with the connection (in that order).

Important:

Also terminate the connection with the data center or third-party provider, or else they may continue to bill you.

To terminate a virtual circuit

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Virtual Circuits, and then click the virtual circuit to view its details.
4. Click Delete.
5. Confirm when prompted.

The virtual circuit's status changes to TERMINATING and then to TERMINATED.

To terminate a cross-connect

If you have multiple cross-connects to delete in a cross-connect group, wait until the state of the first one changes to TERMINATED before deleting the next one. Also, you can't delete a cross-connect if it's the last provisioned cross-connect in a cross-connect group that's being used by a provisioned virtual circuit.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Cross-Connects, and then click the cross-connect to view its details.
4. Click Delete.
5. Confirm when prompted.

The cross-connect's status changes to TERMINATING and then to TERMINATED.

To terminate a cross-connect group

Prerequisite: The cross-connect group must have no virtual circuits running on it and contain no cross-connects.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection to view its details.
3. Click Delete.
4. Confirm when prompted.
The cross-connect group's status changes to TERMINATING and then to TERMINATED.

To manage public IP prefixes for a public virtual circuit

For general information about the prefixes, see Basic Network Diagrams on page 3176.

You can specify your public IP prefixes when you create the virtual circuit. See Task 8: Set up your virtual circuit on page 3214.

You can add or remove public IP prefixes later after creating the virtual circuit. See To edit a virtual circuit on page 3217. If you add a new prefix, Oracle first verifies your company's ownership before advertising it across the connection. If you remove a prefix, Oracle stops advertising the prefix within a few minutes of your editing the virtual circuit.

You can view the state of Oracle's verification of a given public prefix by viewing the virtual circuit's details in the Console. Here are the possible values:

- **In progress**: Oracle is in the process of verifying your organization's ownership of the prefix.
- **Failed**: Oracle could not verify your organization's ownership. Oracle will not advertise the prefix over the virtual circuit.
- **Completed**: Oracle successfully verified your organization's ownership. Oracle is advertising the prefix over the virtual circuit.

To move a connection to a different compartment

You can move a connection from one compartment to another. After you move the connection to the new compartment, inherent policies apply immediately and affect access to the connection through the Console. Moving the connection to a different compartment does not affect the connection between your data center and Oracle Cloud Infrastructure. For more information, see To move a resource to a different compartment on page 2444.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Find the connection in the list, click the the Actions icon (three dots), and then click Move Resource.
3. Choose the destination compartment from the list.
4. Click Move Resource.
5. If there are alarms monitoring the connection, update the alarms to reference the new compartment. See To update an alarm after moving a resource on page 2737 for more information.

Monitoring Your Connection

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring your connection, see FastConnect Metrics on page 3236.

Troubleshooting

See FastConnect Troubleshooting on page 3241.

FastConnect Public Peering Advertised Routes

This topic lists the public IP address ranges (routes) that are advertised to your on-premises network by way of FastConnect public peering (a public virtual circuit).

When you connect with FastConnect to Oracle Cloud Infrastructure in a particular region, the routes advertised over the public virtual circuit may include routes for other Oracle Cloud Infrastructure regions, and for specific Oracle Cloud Infrastructure Classic regions. If you do not own a Public ASN or Public IP Address, you may need to review To use FastConnect if you do not own a Public ASN or Public IP Address on page 3181. The following sections list the regional routes that are advertised over the public virtual circuit.
<table>
<thead>
<tr>
<th>Americas</th>
<th>These Oracle Cloud Infrastructure regional routes are advertised over the public virtual circuit</th>
<th>These Oracle Cloud Infrastructure Classic regional routes are advertised over the public virtual circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use FastConnect public peering to connect to this Oracle Cloud Infrastructure region...</td>
<td>Brazil East (Sao Paulo) Chile (Santiago)</td>
<td>Sao Paulo-Classic</td>
</tr>
<tr>
<td></td>
<td>Brazil East (Sao Paulo) Chile (Santiago)</td>
<td></td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>Brazil East (Sao Paulo) Chile (Santiago)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Brazil East (Sao Paulo) Chile (Santiago)</td>
<td></td>
</tr>
<tr>
<td>Chile (Santiago)</td>
<td>Brazil East (Sao Paulo) Chile (Santiago)</td>
<td></td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td>Ashburn-Classic Chicago-Classic</td>
</tr>
<tr>
<td></td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td></td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td>Ashburn-Classic Chicago-Classic</td>
</tr>
<tr>
<td></td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td></td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td>Ashburn-Classic Chicago-Classic</td>
</tr>
<tr>
<td></td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td></td>
</tr>
<tr>
<td>US West (Phoenix)</td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td>Ashburn-Classic Chicago-Classic</td>
</tr>
<tr>
<td></td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td></td>
</tr>
<tr>
<td>US West (San Jose)</td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td>Ashburn-Classic Chicago-Classic</td>
</tr>
<tr>
<td></td>
<td>Canada Southeast (Toronto) Canada Southeast (Montreal) US East (Ashburn) US West (Phoenix) US West (San Jose)</td>
<td></td>
</tr>
</tbody>
</table>
## Asia-Pacific (APAC)

<table>
<thead>
<tr>
<th>If you use FastConnect public peering to connect to this Oracle Cloud Infrastructure region...</th>
<th>These Oracle Cloud Infrastructure regional routes are advertised over the public virtual circuit</th>
<th>These Oracle Cloud Infrastructure Classic regional routes are advertised over the public virtual circuit</th>
</tr>
</thead>
</table>
| **Australia East (Sydney)** | Australia East (Sydney)  
Australia Southeast (Melbourne)  
India West (Mumbai)  
India South (Hyderabad)  
Japan East (Tokyo)  
Japan Central (Osaka)  
South Korea Central (Seoul)  
South Korea North (Chuncheon) | Sydney-Classic |
| **Australia Southeast (Melbourne)** | Australia East (Sydney)  
Australia Southeast (Melbourne)  
India West (Mumbai)  
India South (Hyderabad)  
Japan East (Tokyo)  
Japan Central (Osaka)  
South Korea Central (Seoul)  
South Korea North (Chuncheon) | Sydney-Classic |
| **India West (Mumbai)** | Australia East (Sydney)  
Australia Southeast (Melbourne)  
India West (Mumbai)  
India South (Hyderabad)  
Japan East (Tokyo)  
Japan Central (Osaka)  
South Korea Central (Seoul)  
South Korea North (Chuncheon) | Sydney-Classic |
<table>
<thead>
<tr>
<th>Location</th>
<th>Regional Routes</th>
<th>Classic Regional Routes</th>
</tr>
</thead>
</table>
| India South (Hyderabad)   | Australia East (Sydney)  
                          Australia Southeast (Melbourne)  
                          India West (Mumbai)  
                          India South (Hyderabad)  
                          Japan East (Tokyo)  
                          Japan Central (Osaka)  
                          South Korea Central (Seoul)  
                          South Korea North (Chuncheon) | Sydney-Classic |
| Japan East (Tokyo)        | Australia East (Sydney)  
                          Australia Southeast (Melbourne)  
                          India West (Mumbai)  
                          India South (Hyderabad)  
                          Japan East (Tokyo)  
                          Japan Central (Osaka)  
                          South Korea Central (Seoul)  
                          South Korea North (Chuncheon) | Sydney-Classic |
| Japan Central (Osaka)     | Australia East (Sydney)  
                          Australia Southeast (Melbourne)  
                          India West (Mumbai)  
                          India South (Hyderabad)  
                          Japan East (Tokyo)  
                          Japan Central (Osaka)  
                          South Korea Central (Seoul)  
                          South Korea North (Chuncheon) | Sydney-Classic |
| South Korea Central (Seoul)| Australia East (Sydney)  
                          Australia Southeast (Melbourne)  
                          India West (Mumbai)  
                          India South (Hyderabad)  
                          Japan East (Tokyo)  
                          Japan Central (Osaka)  
                          South Korea Central (Seoul)  
                          South Korea North (Chuncheon) | Sydney-Classic |
### Networking

If you use FastConnect public peering to connect to this Oracle Cloud Infrastructure region...

<table>
<thead>
<tr>
<th>Region</th>
<th>Oracle Cloud Infrastructure regional routes advertised over the public virtual circuit</th>
<th>Oracle Cloud Infrastructure Classic regional routes advertised over the public virtual circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>South Korea North (Chuncheon)</strong></td>
<td>Australia East (Sydney) &lt;br&gt;Australia Southeast (Melbourne) &lt;br&gt;India West (Mumbai) &lt;br&gt;India South (Hyderabad) &lt;br&gt;Japan East (Tokyo) &lt;br&gt;Japan Central (Osaka) &lt;br&gt;South Korea Central (Seoul) &lt;br&gt;South Korea North (Chuncheon)</td>
<td>Sydney-Classic</td>
</tr>
<tr>
<td><strong>Europe, Middle East, Africa (EMEA)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Germany Central (Frankfurt)</strong></td>
<td>Netherlands Northwest (Amsterdam) &lt;br&gt;Germany Central (Frankfurt) &lt;br&gt;Switzerland North (Zurich) &lt;br&gt;UK South (London) &lt;br&gt;Saudi Arabia West (Jeddah)</td>
<td>Amsterdam-Classic  Slough-Classic</td>
</tr>
<tr>
<td><strong>Switzerland North (Zurich)</strong></td>
<td>Netherlands Northwest (Amsterdam) &lt;br&gt;Germany Central (Frankfurt) &lt;br&gt;Switzerland North (Zurich) &lt;br&gt;UK South (London) &lt;br&gt;Saudi Arabia West (Jeddah)</td>
<td>Amsterdam-Classic  Slough-Classic</td>
</tr>
<tr>
<td><strong>UK South (London)</strong></td>
<td>Netherlands Northwest (Amsterdam) &lt;br&gt;Germany Central (Frankfurt) &lt;br&gt;Switzerland North (Zurich) &lt;br&gt;UK South (London) &lt;br&gt;Saudi Arabia West (Jeddah)</td>
<td>Amsterdam-Classic  Slough-Classic</td>
</tr>
</tbody>
</table>
If you use FastConnect public peering to connect to this Oracle Cloud Infrastructure region...
The Oracle Cloud Infrastructure regional routes are advertised over the public virtual circuit.
The Oracle Cloud Infrastructure Classic regional routes are advertised over the public virtual circuit.

<table>
<thead>
<tr>
<th>Saudi Arabia West (Jeddah)</th>
<th>Netherlands Northwest (Amsterdam)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Germany Central (Frankfurt)</td>
</tr>
<tr>
<td></td>
<td>Switzerland North (Zurich)</td>
</tr>
<tr>
<td></td>
<td>UK South (London)</td>
</tr>
<tr>
<td></td>
<td>Saudi Arabia West (Jeddah)</td>
</tr>
</tbody>
</table>

**Oracle Cloud Infrastructure Regional Routes**

*Australia East (Sydney)*

- 134.70.92.0/23
- 134.70.94.0/23
- 140.91.38.0/23
- 140.91.212.0/23
- 140.204.20.0/23
- 140.204.22.0/23
- 140.238.192.0/20
- 140.238.192.0/21
- 152.67.96.0/20
- 192.29.144.0/21

*Australia Southeast (Melbourne)*

- 134.70.108.0/23
- 134.70.110.0/23
- 140.91.46.0/23
- 140.91.224.0/23
- 140.204.42.0/23
- 140.204.44.0/23
- 168.138.0.0/19
- 192.29.208.0/20
- 192.29.208.0/21

*Brazil East (Sao Paulo)*

- 134.70.84.0/23
- 134.70.86.0/23
- 140.91.34.0/23
- 140.91.208.0/23
- 140.204.12.0/23
- 140.204.14.0/23
- 140.238.176.0/20
- 140.238.176.0/21
- 192.29.128.0/21

*Canada Southeast (Toronto)*

- 132.145.96.0/21
- 132.145.104.0/22
<table>
<thead>
<tr>
<th>Region</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>132.145.108.0/22</td>
</tr>
<tr>
<td></td>
<td>134.70.72.0/23</td>
</tr>
<tr>
<td></td>
<td>134.70.74.0/23</td>
</tr>
<tr>
<td></td>
<td>140.91.28.0/23</td>
</tr>
<tr>
<td></td>
<td>140.91.202.0/23</td>
</tr>
<tr>
<td></td>
<td>140.204.0.0/23</td>
</tr>
<tr>
<td></td>
<td>140.204.2.0/23</td>
</tr>
<tr>
<td></td>
<td>140.238.128.0/20</td>
</tr>
<tr>
<td></td>
<td>192.29.0.0/21</td>
</tr>
<tr>
<td></td>
<td>192.29.8.0/22</td>
</tr>
<tr>
<td></td>
<td>192.29.12.0/22</td>
</tr>
<tr>
<td></td>
<td>192.29.64.0/20</td>
</tr>
<tr>
<td><strong>Canada Southeast (Montreal)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>134.70.116.0/23</td>
</tr>
<tr>
<td></td>
<td>134.70.118.0/23</td>
</tr>
<tr>
<td></td>
<td>140.91.50.0/23</td>
</tr>
<tr>
<td></td>
<td>140.91.226.0/23</td>
</tr>
<tr>
<td></td>
<td>140.204.46.0/23</td>
</tr>
<tr>
<td></td>
<td>140.204.48.0/23</td>
</tr>
<tr>
<td></td>
<td>168.138.64.0/19</td>
</tr>
<tr>
<td></td>
<td>192.29.80.0/20</td>
</tr>
<tr>
<td></td>
<td>192.29.80.0/21</td>
</tr>
<tr>
<td><strong>Chile (Santiago)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>129.149.32.0/21</td>
</tr>
<tr>
<td></td>
<td>129.151.96.0/19</td>
</tr>
<tr>
<td></td>
<td>134.70.152.0/23</td>
</tr>
<tr>
<td></td>
<td>134.70.154.0/23</td>
</tr>
<tr>
<td></td>
<td>140.91.66.0/23</td>
</tr>
<tr>
<td></td>
<td>140.91.244.0/23</td>
</tr>
<tr>
<td></td>
<td>140.204.86.0/23</td>
</tr>
<tr>
<td></td>
<td>140.204.88.0/23</td>
</tr>
<tr>
<td><strong>Germany Central (Frankfurt)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>130.61.0.0/23</td>
</tr>
<tr>
<td></td>
<td>130.61.2.0/23</td>
</tr>
<tr>
<td></td>
<td>130.61.4.0/23</td>
</tr>
<tr>
<td></td>
<td>130.61.6.0/24</td>
</tr>
<tr>
<td></td>
<td>130.61.7.0/24</td>
</tr>
<tr>
<td></td>
<td>130.61.8.0/21</td>
</tr>
<tr>
<td></td>
<td>130.61.16.0/20</td>
</tr>
<tr>
<td></td>
<td>130.61.32.0/20</td>
</tr>
<tr>
<td></td>
<td>130.61.48.0/20</td>
</tr>
<tr>
<td></td>
<td>130.61.64.0/21</td>
</tr>
<tr>
<td></td>
<td>130.61.72.0/21</td>
</tr>
<tr>
<td></td>
<td>130.61.80.0/21</td>
</tr>
<tr>
<td></td>
<td>130.61.88.0/21</td>
</tr>
<tr>
<td></td>
<td>130.61.96.0/23</td>
</tr>
<tr>
<td></td>
<td>130.61.98.0/23</td>
</tr>
<tr>
<td></td>
<td>130.61.100.0/22</td>
</tr>
</tbody>
</table>
• 130.61.104.0/21
• 130.61.112.0/21
• 130.61.120.0/21
• 130.61.128.0/17
• 132.145.224.0/21
• 132.145.232.0/21
• 132.145.240.0/21
• 132.145.248.0/21
• 134.70.40.0/23
• 134.70.42.0/23
• 134.70.44.0/23
• 134.70.46.0/23
• 134.70.48.0/23
• 134.70.50.0/23
• 138.1.0.0/22
• 138.1.4.0/22
• 138.1.8.0/22
• 138.1.12.0/22
• 138.1.40.0/21
• 138.1.64.0/22
• 138.1.68.0/22
• 138.1.72.0/22
• 138.1.76.0/22
• 138.1.96.0/22
• 138.1.100.0/22
• 138.1.104.0/22
• 138.1.160.0/20
• 138.1.176.0/20
• 138.1.192.0/20
• 140.91.16.0/23
• 140.91.18.0/23
• 140.91.20.0/23
• 140.91.198.0/23
• 144.25.48.0/22
• 144.25.52.0/22
• 144.25.56.0/22
• 144.25.60.0/22
• 147.154.128.0/20
• 147.154.144.0/20
• 147.154.160.0/20
• 147.154.176.0/20
• 147.154.192.0/21
• 147.154.200.0/21
• 147.154.208.0/21

India West (Mumbai)

• 134.70.76.0/23
• 134.70.78.0/23
• 140.91.30.0/23
• 140.91.204.0/23
• 140.204.4.0/23
• 140.204.6.0/23
• 140.238.160.0/21
• 140.238.224.0/21
• 192.29.48.0/21

**India South (Hyderabad)**
• 129.148.128.0/21
• 134.70.120.0/23
• 134.70.122.0/23
• 140.91.52.0/23
• 140.91.228.0/23
• 140.204.50.0/23
• 140.204.62.0/23
• 152.67.160.0/19
• 207.135.18.0/23

**Japan East (Tokyo)**
• 132.145.112.0/22
• 132.145.116.0/22
• 132.145.120.0/21
• 134.70.80.0/23
• 134.70.82.0/23
• 140.91.32.0/23
• 140.91.206.0/23
• 140.204.8.0/23
• 140.204.10.0/23
• 140.238.32.0/20
• 140.238.48.0/20
• 158.101.128.0/19
• 158.101.128.0/20
• 192.29.32.0/20
• 192.29.32.0/22
• 192.29.36.0/22
• 140.238.192.0/20
• 140.238.160.0/21
• 140.238.224.0/21
• 140.238.240.0/20
• 132.145.80.0/20
• 140.238.0.0/20
• 134.70.92.0/22
• 140.91.38.0/23
• 140.204.20.0/23
• 192.29.144.0/23
• 140.204.4.0/23
• 192.29.48.0/22
• 192.29.160.0/21
• 134.70.96.0/22
• 140.91.40.0/23
• 140.204.24.0/23
• 192.29.20.0/22
• 134.70.76.0/23
• 134.70.78.0/23
• 140.204.4.0/23
• 140.204.6.0/23
• 132.145.84.0/22
• 132.145.88.0/21
• 134.70.98.0/23
• 140.204.24.0/23
• 140.204.26.0/23
• 140.238.0.0/20
• 192.29.16.0/22
• 134.70.94.0/23
• 140.204.20.0/23
• 140.204.22.0/23
• 152.67.0.0/20
• 140.238.192.0/21
• 152.67.96.0/20
• 129.91.16.0/21
• 129.91.176.0/20
• 129.154.0.0/16
• 129.154.0.0/24
• 129.154.2.0/24
• 160.34.48.0/20
• 160.34.74.0/23
• 160.34.83.0/24
• 160.34.112.0/24
• 160.34.113.0/24
• 205.223.86.0/23
• 205.223.86.0/24
• 205.223.87.0/24

Japan Central (Osaka)
• 134.70.112.0/23
• 134.70.114.0/23
• 140.91.48.0/23
• 140.91.218.0/23
• 140.204.30.0/23
• 140.204.32.0/23
• 168.138.32.0/19
• 192.29.240.0/20
• 192.29.240.0/21

Netherlands Northwest (Amsterdam)
• 134.70.104.0/23
• 134.70.106.0/23
• 140.91.44.0/23
• 140.91.222.0/23
• 140.204.36.0/23
• 140.204.38.0/23
• 140.204.40.0/23
• 158.101.192.0/19
• 192.29.192.0/20
• 192.29.192.0/21
• 193.123.32.0/20

South Korea Central (Seoul)
• 132.145.80.0/22
• 132.145.84.0/22
• 132.145.88.0/21
• 134.70.96.0/23
• 134.70.98.0/23
• 140.91.40.0/23
• 140.91.214.0/23
• 140.204.24.0/23
• 140.204.26.0/23
• 140.238.0.0/20
• 192.29.16.0/22
• 192.29.20.0/22

South Korea North (Chuncheon)
• 132.145.80.0/22
• 132.145.84.0/22
• 132.145.88.0/21
• 134.70.96.0/23
• 134.70.98.0/23
• 140.91.40.0/23
• 140.91.214.0/23
• 140.204.24.0/23
• 140.204.26.0/23
• 140.238.0.0/20
• 192.29.16.0/22
• 192.29.20.0/22

Switzerland North (Zurich)
• 134.70.88.0/23
• 134.70.90.0/23
• 140.91.36.0/23
• 140.91.210.0/23
• 140.204.16.0/23
• 140.204.18.0/23
• 140.238.168.0/21
• 140.238.208.0/21
• 192.29.56.0/21

Saudi Arabia West (Jeddah)
• 134.70.100.0/23
• 134.70.102.0/23
• 140.91.42.0/23
• 140.91.220.0/23
• 140.204.34.0/23
• 158.101.224.0/19
• 192.29.224.0/20
• 192.29.224.0/21
• 193.122.64.0/20

**UK South (London)**
• 130.35.112.0/22
• 132.145.0.0/23
• 132.145.2.0/23
• 132.145.4.0/23
• 132.145.6.0/24
• 132.145.7.0/24
• 132.145.8.0/21
• 132.145.16.0/20
• 132.145.32.0/20
• 132.145.48.0/20
• 132.145.64.0/23
• 132.145.66.0/23
• 132.145.68.0/22
• 132.145.72.0/21
• 134.70.56.0/23
• 134.70.58.0/23
• 134.70.60.0/23
• 134.70.62.0/23
• 134.70.64.0/23
• 134.70.66.0/23
• 138.1.16.0/22
• 138.1.20.0/22
• 138.1.24.0/22
• 138.1.28.0/22
• 138.1.80.0/22
• 138.1.84.0/22
• 138.1.88.0/22
• 138.1.92.0/22
• 138.1.208.0/20
• 138.1.224.0/20
• 138.1.240.0/20
• 140.91.22.0/23
• 140.91.24.0/23
• 140.91.26.0/23
• 140.91.200.0/23
• 140.238.64.0/19
• 144.25.64.0/22
• 144.25.68.0/22
• 144.25.72.0/22
• 144.25.76.0/22
• 147.154.224.0/20
• 147.154.240.0/20

**US East (Ashburn)**
• 129.213.0.0/23
• 129.213.2.0/23
• 129.213.4.0/23
• 129.213.6.0/24
• 129.213.7.0/24
• 129.213.8.0/21
• 129.213.16.0/20
• 129.213.32.0/20
• 129.213.48.0/20
• 129.213.64.0/20
• 129.213.80.0/20
• 129.213.96.0/20
• 129.213.112.0/20
• 129.213.128.0/22
• 129.213.132.0/22
• 129.213.136.0/22
• 129.213.140.0/22
• 129.213.144.0/21
• 129.213.152.0/21
• 129.213.160.0/21
• 129.213.168.0/21
• 129.213.176.0/20
• 129.213.192.0/21
• 129.213.200.0/21
• 129.213.208.0/21
• 130.35.16.0/22
• 130.35.20.0/22
• 130.35.24.0/22
• 130.35.28.0/22
• 130.35.48.0/20
• 130.35.64.0/20
• 130.35.80.0/20
• 130.35.96.0/21
• 130.35.104.0/21
• 130.35.120.0/21
• 130.35.144.0/22
• 130.35.148.0/22
• 130.35.152.0/22
• 130.35.156.0/22
• 130.35.176.0/22
• 130.35.180.0/22
• 130.35.184.0/22
• 130.35.188.0/22
• 130.35.192.0/22
• 130.35.196.0/22
• 130.35.200.0/22
• 130.35.204.0/22
• 130.35.208.0/22
• 130.35.212.0/22
• 130.35.216.0/22
• 130.35.220.0/22
• 130.35.224.0/22
• 130.35.232.0/21
• 132.145.128.0/20
• 132.145.144.0/20
• 132.145.160.0/20
• 132.145.176.0/20
• 132.145.192.0/21
• 132.145.200.0/21
• 132.145.208.0/21
• 132.145.216.0/21
• 134.70.24.0/23
• 134.70.26.0/23
• 134.70.28.0/23
• 134.70.30.0/23
• 134.70.32.0/23
• 134.70.34.0/23
• 138.1.48.0/21
• 140.91.10.0/23
• 140.91.12.0/23
• 140.91.14.0/23
• 140.91.196.0/23
• 144.25.32.0/22
• 144.25.36.0/22
• 144.25.40.0/22
• 144.25.44.0/22
• 144.25.80.0/20
• 147.154.0.0/20
• 147.154.16.0/20
• 147.154.32.0/20
• 147.154.48.0/20
• 147.154.64.0/21
• 147.154.72.0/21
• 147.154.80.0/21
• 150.136.0.0/16

US West (Phoenix)
• 129.146.0.0/22
• 129.146.4.0/22
• 129.146.8.0/23
• 129.146.10.0/23
• 129.146.12.0/24
• 129.146.13.0/24
• 129.146.14.0/24
• 129.146.16.0/23
• 129.146.18.0/23
• 129.146.20.0/22
• 129.146.24.0/22
• 129.146.28.0/22
• 129.146.32.0/22
• 129.146.36.0/22
• 129.146.40.0/22
• 129.146.44.0/22
Networking

- 129.146.48.0/21
- 129.146.56.0/21
- 129.146.64.0/21
- 129.146.72.0/21
- 129.146.80.0/21
- 129.146.88.0/21

US West (San Jose)

- 129.148.160.0/21
- 134.70.124.0/23
- 134.70.126.0/23
- 140.91.54.0/23
- 140.91.234.0/23
- 140.204.58.0/23
- 140.204.60.0/23
- 152.67.224.0/19

Oracle Cloud Infrastructure Classic Regional Routes

Amsterdam-Classic

- 130.162.0.0/16
- 132.226.0.0/16
- 140.86.0.0/16
- 141.145.0.0/19
- 160.34.16.0/20
- 160.34.120.0/24
- 160.34.121.0/24
- 205.223.82.0/24
- 205.223.83.0/24

Ashburn-Classic

- 68.233.64.0/21
- 68.233.72.0/21
- 74.117.200.0/23
- 74.117.203.0/24
- 74.117.206.0/24
- 129.144.0.0/16
- 129.145.16.0/21
- 129.145.24.0/23
- 129.145.28.0/23
- 129.145.39.0/24
- 129.145.40.0/22
- 129.149.0.0/17
- 129.149.128.0/17
- 129.150.0.0/15
- 129.152.32.0/20
- 129.152.60.0/22
- 129.152.80.0/20
- 129.152.128.0/17
- 129.156.64.0/18
- 129.157.0.0/22
- 129.157.4.0/22
• 129.157.8.0/21
• 129.157.112.0/20
• 129.157.128.0/17
• 129.158.0.0/15
• 129.191.0.0/16
• 142.0.160.0/21
• 142.0.170.0/24
• 144.25.128.0/17
• 160.34.0.0/20
• 160.34.72.0/23
• 160.34.82.0/24
• 160.34.86.0/24
• 160.34.88.0/23
• 160.34.100.0/22
• 160.34.104.0/24
• 160.34.105.0/24
• 160.34.107.0/24
• 160.34.108.0/23
• 160.34.110.0/23
• 160.34.124.0/23
• 192.18.192.0/23
• 199.167.172.0/24
• 208.72.89.0/24
• 208.72.91.0/24
• 208.72.92.0/23
• 208.72.94.0/24

**Chicago-Classic**
• 68.233.72.0/21
• 74.117.200.0/23
• 74.117.203.0/24
• 74.117.206.0/24
• 129.145.24.0/23
• 129.145.28.0/23
• 129.145.39.0/24
• 129.145.40.0/22
• 129.149.0.0/17
• 129.149.128.0/17
• 129.150.0.0/15
• 129.152.80.0/20
• 129.152.128.0/17
• 129.191.0.0/16
• 160.34.0.0/20
• 160.34.72.0/23
• 160.34.82.0/24
• 160.34.86.0/24
• 160.34.88.0/23
• 160.34.104.0/24
• 160.34.108.0/23
• 160.34.110.0/23
• 160.34.110.0/23
• 199.167.172.0/24
• 208.72.89.0/24
• 208.72.91.0/24
• 208.72.92.0/23
• 208.72.94.0/24

_Sao Paulo-Classic_
• 129.91.0.0/20
• 144.22.0.0/17

_Slough-Classic_
• 74.117.207.0/24
• 129.152.64.0/22
• 129.156.0.0/18
• 141.144.0.0/16
• 141.144.32.0/19
• 141.145.32.0/20
• 141.145.48.0/20
• 141.145.82.0/23
• 141.145.85.0/24
• 141.145.96.0/20
• 141.145.112.0/20
• 144.21.0.0/16
• 144.24.0.0/16
• 160.34.64.0/23
• 160.34.66.0/23
• 160.34.78.0/24
• 160.34.79.0/24
• 160.34.87.0/24
• 160.34.122.0/24
• 160.34.126.0/23
• 199.167.173.0/24
• 199.167.174.0/24
• 199.167.175.0/24
• 208.72.90.0/24

_Sydney-Classic_
• 140.238.160.0/21
• 140.238.224.0/21
• 140.238.240.0/20
• 132.145.112.0/20
• 140.238.32.0/20
• 140.238.48.0/20
• 132.145.80.0/20
• 140.238.0.0/20
• 140.204.4.0/23
• 192.29.48.0/22
• 192.29.160.0/21
• 134.70.80.0/22
• 140.91.32.0/23
• 140.204.8.0/23
FastConnect Metrics

You can monitor the health, capacity, and performance of your FastConnect connection by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

This topic describes the metrics emitted by the metric namespace oci_fastconnect.

Resources: cross-connect groups, virtual circuits
Overview of Metrics: **oci_fastconnect**

Metrics are available for multiple resources in the FastConnect connection. The metrics help you determine quickly whether your FastConnect connection is up, how much data is flowing over the connection, and whether packets are being dropped for unexpected errors.

FastConnect offers different **connectivity models:**

- **Connect with an Oracle partner:** Metrics are available for virtual circuits in the connection.
- **Connect with a third-party provider:** Metrics are available for the cross-connect group (LAG) and virtual circuits in the connection. Metrics for cross-connects will be available in a future release.
- **Colocate with Oracle:** Metrics are available for the cross-connect group (LAG) and virtual circuits in the connection. Metrics for cross-connects will be available in a future release.

A cross-connect group (LAG) contains one or more cross-connects. If there are multiple and one goes down, the cross-connect group stays up, but the group might experience a lower overall bandwidth.

**Required IAM Policy**

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

**Available Metrics: oci_fastconnect**

The metrics listed in the following table are automatically available for each virtual circuit or cross-connect group that you create. You do not need to enable monitoring to get these metrics.

You also can use the Monitoring service to create custom queries.

Each metric includes the following dimensions:

**COMPONENT**

Possible values are crossconnectgroup and virtualcircuit. If you connect through an Oracle partner, only the virtualcircuit component is available.

**RESOURCEID**

The OCID of the resource (either a cross-connect group or virtual circuit).
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionState</td>
<td>Connection State</td>
<td>Binary (1 or 0)</td>
<td>The values are up (1) or down (0). For a virtual circuit, the operational state of the virtual circuit's interface. For a cross-connect group, this reflects the overall operational state of the cross-connects that make up the cross-connect group (LAG). If at least one of the cross-connects is up, this value is up (1). If all the cross-connects in the group are down, this value is down (0).</td>
<td>component resourceId</td>
</tr>
<tr>
<td>PacketsReceived</td>
<td>Packets Received</td>
<td>Packets</td>
<td>Number of packets received on the FastConnect interface at the Oracle end of the connection. For a cross-connect group (LAG), the value is the sum across all cross-connects in the group.</td>
<td></td>
</tr>
<tr>
<td>BytesReceived</td>
<td>Bytes Received</td>
<td>Bytes</td>
<td>Number of bytes received on the FastConnect interface at the Oracle end of the connection. For a cross-connect group (LAG), the value is the sum across all cross-connects in the group.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>PacketsSent</td>
<td>Packets Sent</td>
<td>Packets</td>
<td>Number of packets sent from the FastConnect interface at the Oracle end of the connection. For a cross-connect group (LAG), the value is the sum across all cross-connects in the group.</td>
<td></td>
</tr>
<tr>
<td>BytesSent</td>
<td>Bytes Sent</td>
<td>Bytes</td>
<td>Number of bytes sent from the FastConnect interface at the Oracle end of the connection. For a cross-connect group (LAG), the value is the sum across all cross-connects in the group.</td>
<td></td>
</tr>
<tr>
<td>PacketsError</td>
<td>Packets with Errors</td>
<td>Packets</td>
<td>Number of packets dropped at the Oracle end of the connection. Dropped packets indicate a misconfiguration in some part of the overall system. Check if there's been a change to the configuration of your VCN, the virtual circuit, or your CPE. For a cross-connect group (LAG), the value is the sum across all cross-connects in the group.</td>
<td></td>
</tr>
</tbody>
</table>

**Using the Console**

The instructions depend on which FastConnect connectivity model you use.

**If You Use an Oracle Partner**

*To view default metric charts for a single FastConnect connection*

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **FastConnect**.
2. Click the connection you're interested in.
3. The default metrics charts for the connection's virtual circuit are displayed on the resulting page.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**To view default metric charts for all FastConnect connections in a compartment**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that you're interested in.
3. For Metric Namespace, select oci_fastconnect.

   The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

If there are multiple FastConnect connections in the compartment, by default the charts show a separate line for each one (each virtual circuit).

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**If You Use a Third-Party Provider or Colocate with Oracle**

In this situation, you manage both the physical connection (cross-connects) and logical connection (virtual circuit).

For the physical connection, metrics are available for the cross-connect group (LAG), but not the individual cross-connects. If you are using only a single cross-connect with no cross-connect group, then no metrics are available for the physical connection.

For the logical connection, metrics are available for each virtual circuit.

**To view default metric charts for a single FastConnect connection**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Click the connection you're interested in.
3. View the metrics for the resource you're interested in:
   - For a cross-connect group: Under Resources, click Metrics. The default metrics charts are displayed on the resulting page.
   - For a virtual circuit:
      a. Under Resources, click Virtual Circuits.
      b. Click the virtual circuit you're interested in. If it's a private virtual circuit, the default metrics charts are displayed on the resulting page. If it's a public virtual circuit, click Metrics to view the charts.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**To view default metric charts for all FastConnect connections in a compartment**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that you're interested in.
3. For Metric Namespace, select oci_fastconnect.

   The Service Metrics page dynamically updates the page to show charts for each metric emitted by the selected metric namespace.

By default the charts show a separate line for each resource in the compartment (each cross-connect group and virtual circuit).

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

FastConnect Troubleshooting

This topic covers troubleshooting techniques for a FastConnect connection that has issues.

Some of the troubleshooting techniques assume that you are a network engineer with access to your CPE's configuration.

Microsoft Azure Connection Issues

Problems terminating the Azure connection

The connection components must be terminated in a specific order. If you don't follow this order, the FastConnect virtual circuit switches to a "Failed" state and cannot be deleted.

To fix a virtual circuit in the "Failed" state, go to the Azure portal and confirm the following items:

- The ExpressRoute circuit is not in the "Failed" state. If it is, click the ExpressRoute circuit's Refresh button. The circuit should return to its normal state.
- The ExpressRoute circuit has no connections. Delete all its connections and then retry terminating the connection.

After you've confirmed the preceding items, you can continue with the termination process in the following steps:

1. In the Oracle Console, delete your FastConnect virtual circuit. Ensure that it is deleted before proceeding.
2. In the Azure portal, confirm that the private peering for the ExpressRoute circuit has been deleted. Also confirm that the ExpressRoute circuit's status has changed to "Not Provisioned".
3. In the Azure portal, delete the ExpressRoute circuit.

General Issues

Cross-connect and physical connection (layer 1)

Check these items:

- **Port allocation**: Verify that your connection is using the correct port, and the port is UP and activated.
- **Optical signal**: Verify that your connection is using the correct optics and transceiver, and the port is sending and receiving an optimal signal. For more information, see FastConnect Requirements on page 3181.
- **Fiber strands**: Try rolling or flipping the Tx/Rx fiber strands.
- **End-to-end physical connectivity**: Verify the end-to-end physical connectivity. Also verify the Tx/Rx optic signal between your CPE, the provider's network device (if you're working with a provider), and the Oracle FastConnect router.

Data-link (layer 2)

Check the following items on your CPE. If you're working with a provider, also have them check the items on their network device:

- **BGP address**: Verify that the router is configured with the correct BGP peering IP address under the correct VLAN on the interface.

Important:

If you're working with an Oracle partner or a third-party provider, contact both the provider and Oracle to help troubleshoot the issue. If you're colocated with Oracle, contact Oracle.
• **MAC address:** Verify that the router is receiving the MAC address from the Oracle FastConnect router, and that the MAC address has an entry in the router’s address resolution protocol (ARP) table.

• **LAG and LACP:** Verify that the router has LAG configured and LACP is enabled on the interface (the Oracle FastConnect router requires both). For more information, see FastConnect Requirements on page 3181.

Network and transport (layers 3 and 4)

Check the following items on your CPE. If you're working with a provider, also have them check the items on their network device:

• **BGP address:** Verify that the router is configured with the correct BGP peering IP address.

• **ASN:** Verify that the router is configured with the correct BGP local ASN and Oracle BGP ASN. Oracle's BGP ASN for the commercial cloud is 31898. For the Government Cloud, see Oracle's BGP ASN on page 154.

• **MD5:** If you're using MD5 authentication, verify that the authentication string (the password) is correct.

• **Maximum prefixes:** Verify that you are advertising less than the maximum allowed number of prefixes for virtual circuits. If you're advertising more prefixes than allowed, BGP establishment fails. Here are the limits:
  - Public virtual circuits: maximum 200 prefixes
  - Private virtual circuits: maximum 2000 prefixes

• **Firewalls:** Verify that your on-premises firewall or access control lists are not blocking TCP port 179 (BGP) or any high-numbered TCP ports.

*FastConnect virtual circuit is UP, but BGP session is DOWN*

The Oracle Console displays an alert if the virtual circuit is in the PROVISIONED state, but the BGP session is DOWN.

Typically, the alert indicates one of the following issues:

• You have not yet configured your CPE with the required information for the FastConnect connection. After you configure the CPE, the alert should no longer appear.

• You have configured your CPE with incorrect information. Verify that your CPE is configured with the correct information.

The CPE configuration information includes these items:

• BGP address for each side of the connection

• ASN for your network and for Oracle's network

• MD5 authentication string (if you're using MD5 authentication)

• Maximum number of allowed prefixes

For more details, see the preceding information shown for network and transport (layers 3 and 4) in FastConnect is DOWN on page 3241.

**Exception:** The preceding information is not relevant if you're using an Oracle partner, and the BGP session from your CPE goes to that partner and not Oracle. In that case, contact your provider to confirm that the BGP session they have with Oracle is configured correctly.

*FastConnect virtual circuit is UP, but no traffic is passing through*

Check these items:

• **VCN security lists:** Ensure you've set up the VCN security lists to allow the desired traffic (both ingress and egress rules). Note that the VCN's default security list does not allow ping traffic (ICMP type 8 and ICMP type 0). You must add the appropriate ingress and egress rules to allow ping traffic.

• **Correct routes on both ends:** Verify that you have received the correct VCN routes from FastConnect and the CPE is using those routes. Likewise, verify that you are advertising the correct on-premises network routes to FastConnect and the VCN route tables use those routes.

*FastConnect virtual circuit is UP, but traffic is passing in only one direction*

Check these items:

• **VCN security lists:** Ensure that your VCN security lists allow traffic in both directions (ingress and egress).
Networking

- **Firewalls:** Verify that your on-premises firewall or access control lists are not blocking traffic to or from the Oracle end.
- **Asymmetric routing:** Oracle uses asymmetric routing. If you have multiple virtual circuits, ensure that your CPE is configured for asymmetric route processing.
- **Redundant connections:** If you have redundant FastConnect virtual circuits, ensure that they're both advertising the same routes.

**Redundant Connections**
Remember that FastConnect uses BGP dynamic routing, and IPSec connections can use either static routing or BGP, or a combination.

*IPSec and FastConnect are both set up, but traffic is only passing through IPSec*

Verify that the route tables use more specific routes for the connection you want as primary. If you're using the same routes for both IPSec and FastConnect, see the discussion of routing preferences in Routing for the Oracle IPSec VPN on page 2934.

**Access to the Internet**
See these topics for how to give your virtual cloud network (VCN) access to the internet:
- **Internet Gateway** on page 3243: For public resources that need to be reached from the internet
- **NAT Gateway** on page 3247: For resources that need to reach the internet but are not reachable from the internet

**Internet Gateway**
This topic describes how to set up and manage an internet gateway to give your VCN internet access.

| Tip: |
| Oracle also offers a **NAT gateway**, which is recommended for subnets in your VCN that do not require ingress connections from the internet. |

**Highlights**
- An internet gateway is an optional virtual router you can add to your VCN to enable direct connectivity to the internet.
- The gateway supports connections initiated from within the VCN (egress) and connections initiated from the internet (ingress).
- Resources that need to use the gateway for internet access must be in a public subnet and have public IP addresses. Resources that have private IP addresses can instead use a NAT gateway to initiate connections to the internet.
- Each public subnet that needs to use the internet gateway must have a route table rule that specifies the gateway as the target.
- You use security rules to control the types of traffic allowed in and out of resources in that subnet. Make sure to allow only the desired types of internet traffic.
- The internet gateway can be used only by resources in the gateway's VCN. Hosts in the connected on-premises network or in a peered VCN cannot use that internet gateway.
- You can't add or move an internet gateway to a VCN within a security zone. Security zones do not permit public subnets.

**Overview of Internet Gateways**
Before continuing, make sure you've read **Access to the Internet** on page 2752 and also understand how to set up security rules for the resources in a subnet.

An internet gateway as an optional virtual router that connects the edge of the VCN with the internet. To use the gateway, the hosts on both ends of the connection must have public IP addresses for routing. Connections that originate in your VCN and are destined for a public IP address (either inside or outside the VCN) go through the
internet gateway. Connections that originate outside the VCN and are destined for a public IP address inside the VCN go through the internet gateway.

A given VCN can have only one internet gateway. You control which public subnets in the VCN can use the gateway by configuring the subnet’s associated route table. You use security rules to control the types of traffic allowed in and out of resources in those public subnets.

The following diagram illustrates a simple VCN setup with two public subnets. The VCN has an internet gateway, and the two public subnets are both configured to use the VCN’s default route table. The table has a route rule that sends all egress traffic from the subnets to the internet gateway. The gateway allows any ingress connections from the internet with a destination IP address equal to the public IP address of a resource in the VCN. However, the public subnet’s security list rules ultimately determine the specific types of traffic that are allowed in and out of the resources in the subnet. Those specific security rules are not shown in the diagram.

Tip:
Traffic through an internet gateway between a VCN and a public IP address that is part of Oracle Cloud Infrastructure (such as Object Storage) is routed without being sent over the internet.

Working with Internet Gateways
You create an internet gateway in the context of a specific VCN. In other words, the internet gateway is automatically attached to a VCN. However, you can disable and re-enable the internet gateway at any time. Compare this with a dynamic routing gateway (DRG), which you create as a standalone object that you then attach to a particular VCN. DRGs use a different model because they’re intended to be modular building blocks for privately connecting VCNs to your on-premises network.
For traffic to flow between a subnet and an internet gateway, you must create a route rule accordingly in the subnet's route table (for example, destination CIDR = 0.0.0.0/0 and target = internet gateway). If the internet gateway is disabled, that means no traffic will flow to or from the internet even if there's a route rule that enables that traffic. For more information, see Route Tables on page 2921.

For the purposes of access control, you must specify the compartment where you want the internet gateway to reside. If you're not sure which compartment to use, put the internet gateway in the same compartment as the cloud network. For more information, see Access Control on page 2831.

You may optionally assign a friendly name to the internet gateway. It doesn't have to be unique, and you can change it later. Oracle automatically assigns the internet gateway a unique identifier called an Oracle Cloud ID (OCID). For more information, see Resource Identifiers.

To delete an internet gateway, it does not have to be disabled, but there must not be a route table that lists it as a target.

Using the Console

To set up an internet gateway

Prerequisites:

• You've determined which subnets in the VCN need access to the internet, and you've created those public subnets.
• You've determined the types of ingress and egress internet traffic that you want to enable for the resources in each public subnet (examples: ingress HTTPS connections, ingress ICMP ping connections).
• The required IAM policy is in place to allow you to work with Networking service resources. For administrators: see IAM Policies for Networking on page 2832.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you've configured the public subnet to use the default security list, remember that the list includes several helpful default rules that enable basic required access (examples: ingress SSH, egress access to all destinations). Oracle recommends that you become familiar with the basic access that these default rules provide. If you choose not to use the default security list, make sure to provide this basic access by implementing these security rules either in network security groups (NSGs) or custom security lists.</td>
</tr>
<tr>
<td>The following procedure uses security lists, but you could instead implement the security rules in a network security group and then create all of the subnet's resources in that NSG.</td>
</tr>
</tbody>
</table>
1. For each public subnet that needs to use the internet gateway, set up the subnet's security list rules to allow the desired internet traffic.
   a. In the Console, while viewing the VCN you're interested in, click Security Lists.
   b. Click the security list you're interested in (a security list associated with the public subnet).
   c. Under Resources, click either Ingress Rules or Egress Rules depending on the type of rule you want to work with.
   d. If you want to add a new rule, click Add Ingress Rule (or Add Egress Rule).
      
      Example
      
      Imagine you have web servers in the public subnet. This example shows how to add an ingress rule for HTTPS connections (TCP port 443) coming from the internet to the web server. Without this rule, inbound HTTPS connections are not allowed.
      
      1. Leave the Stateless check box unselected.
      2. Source Type: CIDR
      3. Source CIDR: 0.0.0.0/0
      4. IP Protocol: Leave as TCP.
      5. Source Port Range: Leave as All.
      6. Destination Port Range: Enter 443.
      7. Description: An optional description of the rule.
   e. If you want to delete an existing rule, click the Actions icon (three dots), and then click Remove.
   f. If you wanted to edit an existing rule, click the Actions icon (three dots), and then click Edit.

2. Create the VCN's internet gateway:
   a. In the Console, while viewing the VCN you're interested in, click Internet Gateways.
   b. Click Create Internet Gateway.
   c. Enter the following:
      
      • Name: A friendly name for the internet gateway. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
      • Create in Compartment: The compartment where you want to create the internet gateway, if different from the compartment you're currently working in.
      • Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
   d. Click Create Internet Gateway.
      
      Your internet gateway is created and displayed on the Internet Gateways page of the compartment you chose. It's already enabled, but you still need to add a route rule that allows traffic to flow to the gateway.

3. For each public subnet that needs to use the internet gateway, update the subnet's route table:
   a. While viewing the VCN's details, click Route Tables.
   b. Click the public subnet's route table to view its details.
   c. Click Add Route Rule.
   d. Enter the following:
      
      • Target Type: Internet Gateway
      • Destination CIDR block: 0.0.0.0/0 (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table will go to the target specified in this rule)
      • Compartment: The compartment where the internet gateway is located.
      • Target: The internet gateway you just created.
      • Description: An optional description of the rule.
   e. Click Save.
      
      An internet gateway is now enabled and working for your cloud network.
To disable/enable an internet gateway

This is available only through the API. If you don't have access to the API and need to disable or enable an internet gateway, contact Oracle Support. You can also easily delete and recreate the internet gateway if needed. Just make sure to update any route tables that refer to the internet gateway.

To delete an internet gateway

Prerequisite: The internet gateway does not have to be disabled, but there must not be a route table that lists it as a target.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Internet Gateways.
4. Click the Actions icon (three dots) for the internet gateway, and then click Terminate.
5. Confirm when prompted.

To manage tags for an internet gateway

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Internet Gateways.
4. Click the Actions icon (three dots) for the internet gateway, and then click View Tags. From there you can view the existing tags, edit them, and apply new ones.

For more information, see Resource Tags on page 211.

To move an internet gateway to a different compartment

You can move an internet gateway from one compartment to another. When you move an internet gateway to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Under Resources, click Internet Gateways.
4. Click the the Actions icon (three dots) for the internet gateway, and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

For more information about using compartments and policies to control access to your cloud network, see Access Control on page 2831. For general information about compartments, see Managing Compartments on page 2431.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage your internet gateways, use these operations:

- ListInternetGateways
- CreateInternetGateway
- GetInternetGateway
- UpdateInternetGateway
- DeleteInternetGateway
- ChangeInternetGatewayCompartment

NAT Gateway

This topic describes how to set up and manage a Network Address Translation (NAT) gateway. A NAT gateway gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.
Networking

Highlights

- You can add a NAT gateway to your VCN to give instances in a private subnet access to the internet.
- Instances in a private subnet don't have public IP addresses. With the NAT gateway, they can initiate connections to the internet and receive responses, but not receive inbound connections initiated from the internet.
- NAT gateways are highly available and support TCP, UDP, and ICMP ping traffic.

Overview of NAT

NAT is a networking technique commonly used to give an entire private network access to the internet without assigning each host a public IPv4 address. The hosts can initiate connections to the internet and receive responses, but not receive inbound connections initiated from the internet.

When a host in the private network initiates an internet-bound connection, the NAT device's public IP address becomes the source IP address for the outbound traffic. The response traffic from the internet therefore uses that public IP address as the destination IP address. The NAT device then routes the response to the host in the private network that initiated the connection.

Overview of NAT Gateways

The Networking service offers a reliable and highly available NAT solution for your VCN in the form of a NAT gateway.

Example scenario: Imagine you have resources that need to receive inbound traffic from the internet (for example, web servers). You also have private resources that need to be protected from inbound traffic from the internet. All of these resources need to initiate connections to the internet to request software updates from sites on the internet.

You set up a VCN and add a public subnet to hold the web servers. When launching the instances, you assign public IP addresses to them so they can receive inbound internet traffic. You also add a private subnet to hold the private instances. They cannot have public IP addresses because they are in a private subnet.

You add an internet gateway to the VCN. You also add a route rule in the public subnet's route table that directs internet-bound traffic to the internet gateway. The public subnet's instances can now initiate connections to the internet and also receive inbound connections initiated from the internet. Remember that you can use security rules to control the types of traffic that are allowed in and out of the instances at the packet level.

You add a NAT gateway to the VCN. You also add a route rule in the private subnet's route table that directs internet-bound traffic to the NAT gateway. The private subnet's instances can now initiate connections to the internet. The NAT gateway allows responses, but it does not allow connections that are initiated from the internet. Without that NAT gateway, the private instances would instead need to be in the public subnet and have public IP addresses to get their software updates.

The following diagram illustrates the basic network layout for the example. The arrows indicate whether connections can be initiated in only one direction or both.
A NAT gateway can be used only by resources in the gateway's own VCN. If the VCN is **peered with another**, resources in the other VCN cannot access the NAT gateway.

Also, resources in an on-premises network connected to the NAT gateway's VCN with **FastConnect** or an **IPSec VPN** cannot use the NAT gateway.

**Here are a few basics about NAT gateways:**

- The NAT gateway supports TCP, UDP, and ICMP ping traffic.
- The gateway supports a maximum of approximately 20,000 concurrent connections to a single destination address and port.
- The Networking service automatically assigns a public IP address to the NAT gateway. You can't choose the public IP address or use one of your **reserved public IP addresses**.
- There's a limit on the number of NAT gateways per VCN. You can request an increase to that limit. See **Service Limits** on page 215.

**Routing for a NAT Gateway**

You control routing in your VCN at the subnet level, so you can specify which subnets in your VCN use a NAT gateway. You can have more than one NAT gateway on a VCN (although you must **request an increase in your limits**). For example, if you want an external application to distinguish traffic from the VCN's different subnets, you could set up a different NAT gateway (and thus a different public IP address) for each subnet. A given subnet can route traffic to only a single NAT gateway.

**Blocking Traffic Through a NAT Gateway**

You create a NAT gateway in the context of a specific VCN. In other words, the NAT gateway is automatically always attached to only one VCN of your choice. However, you can block or allow traffic through the NAT gateway at any time. By default, the gateway allows traffic upon creation. Blocking the NAT gateway prevents all traffic from flowing, regardless of any existing route rules or security rules in your VCN. For instructions on how to block traffic, see **To block/allow traffic for a NAT gateway** on page 3251.
**Transitioning to a NAT Gateway**

If you're switching from using a **NAT instance in your VCN** to a NAT gateway, consider that the public IP address for your NAT device will change.

If you're switching from using an internet gateway to a NAT gateway, the instances with access to the NAT gateway no longer need public IP addresses to reach the internet. Also, the instances no longer need to be in a public subnet. You can't switch a subnet from **public to private**. However, you can delete the **ephemeral public IPs** from your instances if you like.

**Deleting a NAT Gateway**

To delete a NAT gateway, its traffic does not have to be blocked, but there must not be a route table that lists it as a target. For instructions, see **To delete a NAT gateway** on page 3251.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators: see **IAM Policies for Networking** on page 2832.

**Setting Up a NAT Gateway**

**Task 1: Create the NAT gateway**

1. In the Console, confirm you're viewing the compartment that contains the VCN that you want to add the NAT gateway to. For information about compartments and access control, see **Access Control** on page 2831.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
3. Click the VCN you're interested in.
4. Under **Resources**, click **NAT Gateways**.
5. Click **Create NAT Gateway**.
6. Enter the following values:
   - **Name**: A friendly name for the NAT gateway. It doesn't have to be unique. Avoid entering confidential information.
   - **Create in compartment**: The compartment where you want to create the NAT gateway, if different from the compartment you're currently working in.
   - **Choose IP Address Type**: Specify whether the public IP address is reserved or ephemeral.
     - **Ephemeral IP Address**: Choose this option to let Oracle specify an **ephemeral IP address** for you from the Oracle IP pool. This is the default.
     - **Reserved IP Address**: Choose this option to specify an existing **reserved IP address** by name, or to create a new reserved IP address by assigning a name and selecting a source **IP pool** for the address. If you don't select a pool you've created, the default Oracle IP pool is used.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click **Create NAT Gateway**.

The NAT gateway is then created and displayed on the **NAT Gateways** page in the compartment you chose. The gateway allows traffic by default. At any time, you can **block or allow traffic** through it.

**Task 2: Update routing for the subnet**

When you create a NAT gateway, you must also create a route rule that directs the desired traffic from the subnet to the NAT gateway. You do this for each subnet that needs to access the gateway.

1. Determine which subnets in your VCN need access to the NAT gateway.
2. For each of those subnets, update the subnet's route table to include a new rule:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click the VCN you're interested in.
   c. Under Resources, click Route Tables.
   d. Click the route table you're interested in.
   e. Click Add Route Rule and enter the following values:
      • Target Type: NAT Gateway.
      • Destination CIDR Block: 0.0.0.0/0
      • Compartment: The compartment where the NAT gateway is located.
      • Target NAT Gateway: The NAT gateway.
      • Description: An optional description of the rule.
   f. Click Add Route Rule.

Any subnet traffic with a destination that matches the rule is routed to the NAT gateway. For more information about setting up route rules, see Route Tables on page 2921.

Later, if you no longer need the NAT gateway and want to delete it, you must first delete all the route rules in your VCN that specify the NAT gateway as the target.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without the required routing, traffic doesn't flow over the NAT gateway. If a situation occurs where you need to temporarily stop the traffic flow over the gateway, you can simply remove the route rule that enables traffic. Or you can block traffic through the gateway entirely. You do not need to delete it.</td>
</tr>
</tbody>
</table>

Using the Console

**To create a NAT gateway**

See the instructions in To create a NAT gateway on page 3251.

**To block/allow traffic for a NAT gateway**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the NAT gateway you're interested in, click the Actions icon (three dots) and then click Block Traffic (or Allow Traffic if you're enabling traffic for the NAT gateway).
5. Confirm when prompted.

When the traffic is blocked, the NAT gateway’s icon turns gray, and the label changes to BLOCKED. When the traffic is allowed, the NAT gateway’s icon turns green, and the label changes to AVAILABLE.

**To update a NAT gateway**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the NAT gateway you're interested in, click the Actions icon (three dots), and then click Edit.
5. Make your changes and click Save Changes.

**To delete a NAT gateway**

Prerequisite: There must not be a route table that lists the NAT gateway as a target.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the NAT gateway you want to delete, click the Actions icon (three dots), and then click **Terminate**.
5. Confirm when prompted.

**To manage tags for a NAT gateway**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Under **Resources**, click **NAT Gateways**.
4. Click the Actions icon (three dots) for the NAT gateway, and then click **View Tags**. From there you can view the existing tags, edit them, and apply new ones.

For more information, see **Resource Tags** on page 211.

**To move a NAT gateway to a different compartment**

You can move a NAT gateway from one compartment to another. When you move a NAT gateway to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. In **Resources**, click **NAT Gateways**.
4. Find the NAT gateway in the list, click the the Actions icon (three dots), and then click **Move Resource**.
5. Choose the destination compartment from the list.
6. Click **Move Resource**.

The NAT gateway moves to the new compartment immediately. Depending on your permissions, you can select the compartment in the left side menu to view the NAT gateway.

For more information about using compartments and policies to control access to your cloud network, see **Access Control** on page 2831. For general information about compartments, see **Managing Compartments** on page 2431.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage your NAT gateways, use these operations:

- **ListNatGateways**
- **CreateNatGateway**
- **GetNatGateway**
- **UpdateNatGateway**
- **DeleteNatGateway**
- **ChangeNatGatewayCompartment**

To manage route tables, see Route Tables on page 2921.

**Access to Your On-Premises Network**

The following topics have information about ways to privately connect your cloud network to your existing on-premises network. Regardless of which method you use, you need a dynamic routing gateway (DRG) attached to your cloud network.

- **Dynamic Routing Gateways (DRGs)** on page 2927
- **Routing Details for Connections to Your On-Premises Network** on page 2942
Networking

- VPN Connect:
  - VPN Connect Overview on page 2933
  - VPN Connect Quickstart on page 2939
  - Routing Details for Connections to Your On-Premises Network on page 2942
  - Supported IPSec Parameters on page 2945
  - Supported Encryption Domain or Proxy ID on page 2948
  - Setting Up VPN Connect on page 2949
  - Working with VPN Connect on page 3156
  - CPE Configuration on page 2967
  - Verified CPE Devices on page 2969
  - Using the CPE Configuration Helper on page 2970
  - VPN Connect FAQ
  - Using the API for VPN Connect on page 3163
  - VPN Connect Metrics on page 3164
  - VPN Connect Troubleshooting on page 3166

- FastConnect:
  - FastConnect Overview on page 3173
  - FastConnect Requirements on page 3181
  - FastConnect Redundancy Best Practices on page 3185
  - Routing Details for Connections to Your On-Premises Network on page 2942
  - FastConnect: With an Oracle Partner on page 3192
  - FastConnect: With a Third-Party Provider on page 3200
  - FastConnect: Colocation with Oracle on page 3210
  - FastConnect Metrics on page 3236
  - FastConnect Troubleshooting on page 3241

Private Access

This topic gives an overview of the options for enabling private access to services within Oracle Cloud Infrastructure. Private access means that traffic does not go over the internet. Access can be from hosts within your virtual cloud network (VCN) or your on-premises network.

**Tip:**

This topic does not discuss access to services through an internet gateway. However, remember that traffic through an internet gateway between a VCN and a public IP address that is part of Oracle Cloud Infrastructure is routed without being sent over the internet.

**Highlights**

- You can enable private access to certain services within Oracle Cloud Infrastructure from your VCN or on-premises network by using either a private endpoint or a service gateway. See the sections that follow.
• For each private access option, these services or resource types are available:
  
  • **With a private endpoint:**
    
    • Autonomous Database (shared Exadata infrastructure)
    • Streaming
    • Data Safe
    • Data Catalog
    • Oracle Analytics Cloud
    • Data Flow
  
  • **With a service gateway:** Available services
  
  • With either private access option, the traffic stays within the Oracle Cloud Infrastructure network and does not traverse the internet. However, if you use a service gateway, requests to the service use a public endpoint for the service.
  
  • If you do not want to access a given Oracle service through a public endpoint, Oracle recommends using a private endpoint in your VCN (assuming the service supports private endpoints). A private endpoint is represented as a private IP address within a subnet in your VCN.

**About Private Endpoints**

A private endpoint is a private IP address within your VCN that you can use to access a given service within Oracle Cloud Infrastructure. The service sets up the private endpoint in a subnet of your choice within the VCN. You can think of the private endpoint as just another *VNIC* in your VCN. You can control access to it like you would for any other VNIC: by using *security rules*. However, the service sets up this VNIC and maintains its availability on your behalf. You only need to maintain the subnet and the security rules.

The following diagram illustrates the concept.

The private endpoint gives hosts within your VCN and your on-premises network access to a *single resource* within the Oracle service of interest (for example, one Autonomous Database with shared Exadata infrastructure). Compare that private access model with a service gateway (see the next section): If you created five Autonomous Databases for a given VCN, all five would be accessible through a single service gateway by sending requests to a public endpoint for the service. However, with the private endpoint model, there would be five separate private endpoints: one for each Autonomous Database, and each with its own private IP address.
The service that sets up the private endpoint in your VCN might provide you a DNS name (fully qualified domain name, or FQDN) for the private endpoint, and not the private IP address itself. If you've configured your network setup for DNS, your hosts can access the private endpoint by using the FQDN. If the service supports the use of network security groups (NSGs) with its resources, you can request that the service set up the private endpoint in an NSG of your choice within your VCN. NSGs let you write security rules to control access to the private endpoint without knowing the private IP address assigned to the private endpoint.

If you have a private endpoint for a resource, hosts within the VCN can use the private endpoint's FQDN or private IP address to access the resource. You set up security rules to control access between hosts in the VCN and the private endpoint. For an example of how to do this with Autonomous Data Warehouse, see Autonomous Database with Private Endpoint on page 1163.

You can also set up transit routing with your VCN so that hosts in the on-premises network can use the private endpoint. To enable on-premises hosts to use the private endpoint's FQDN instead of its private IP address, you have two options:

- Set up an instance in the VCN to be a custom DNS server. For an example of an implementation of this scenario with the Oracle Terraform provider, see Hybrid DNS Configuration.
- Manage hostname resolution yourself manually.

You might have multiple VCNs with hosts that need access to the specific resource of interest. You can peer the VCNs so that hosts in the other VCNs can also use the private endpoint (the preceding diagram does not show any peered VCNs).

### About Service Gateways

A service gateway gives resources in your VCN and on-premises network private access to multiple services within Oracle Cloud Infrastructure, without the traffic going over the internet.

The following diagram illustrates the concept. The diagram refers to the Oracle Services Network, which is a conceptual network in Oracle Cloud Infrastructure that is reserved for Oracle services.

To use a service gateway from a particular subnet within your VCN, you set up a route rule in the subnet's route table, and specify the service gateway as the target of the rule. You also set up security rules to control access between hosts in the VCN and the services available through the service gateway.

If you have more than one VCN in your tenancy, you can configure each with its own service gateway.
You can also set up transit routing for the Oracle Services Network so that hosts in your on-premises network can use a VCN's service gateway.

Access to Oracle Services: Service Gateway

This topic describes how to set up and manage a service gateway. A service gateway enables cloud resources without public IP addresses to privately access Oracle services.

Access to Oracle Services

The Oracle Services Network is a conceptual network in Oracle Cloud Infrastructure that is reserved for Oracle services. These services have public IP addresses that you typically reach over the internet. However, you can access the Oracle Services Network without the traffic going over the internet. There are different ways, depending on which of your hosts need the access:

- **Hosts in your on-premises network:**
  - Private access through a VCN with FastConnect private peering or VPN Connect: The on-premises hosts use private IP addresses and reach the Oracle Services Network by way of the VCN and the VCN's service gateway.
  - Public access with FastConnect public peering: The on-premises hosts use public IP addresses.

- **Hosts in your VCN:**
  - Private access through a service gateway: This is the scenario covered in this topic. The VCN's hosts use private IP addresses.

Highlights

- A service gateway lets your virtual cloud network (VCN) privately access specific Oracle services without exposing the data to the public internet. No internet gateway or NAT is required to reach those specific services. The resources in the VCN can be in a private subnet and use only private IP addresses. The traffic from the VCN to the Oracle service travels over the Oracle network fabric and never traverses the internet.
- The service gateway is regional and enables access only to supported Oracle services in the same region as the VCN.
- The service gateway allows access to supported Oracle services within the region to protect your data from the internet. Your workloads may require access to public endpoints or services not supported by the service gateway (for example, to download updates or patches). Ensure you have a NAT gateway or other access to the internet if necessary.
- The supported Oracle services are Oracle Cloud Infrastructure Object Storage and others in the Oracle Services Network. For a list, see Service Gateway: Supported Cloud Services in Oracle Services Network.
- The service gateway uses the concept of a service CIDR label, which is a string that represents all the regional public IP address ranges for the service or group of services of interest (for example, OCI PHX Object Storage is the string for Object Storage in US West (Phoenix)). You use that service CIDR label when you configure the service gateway and related route rules to control traffic to the service. You can optionally use it when configuring security rules. If the service's public IP addresses change in the future, you don't have to adjust those rules.
- You can set up a VCN so that your on-premises network has private access to Oracle services by way of the VCN and the VCN's service gateway. The hosts in your on-premises network communicate with their private IP addresses and the traffic does not go over the internet. For more information, see Transit Routing: Private Access to Oracle Services on page 2803

Overview of Service Gateways

A service gateway lets resources in your VCN privately access specific Oracle services, without exposing the data to an internet gateway or NAT. The resources in the VCN can be in a private subnet and use only private IP addresses. The traffic from the VCN to the service of interest travels over the Oracle network fabric and never traverses the internet.

The following simple diagram illustrates a VCN that has both a public subnet and a private subnet. Resources in the private subnet have only private IP addresses.

The VCN has three gateways:
Networking

- **Internet gateway**: To provide the public subnet direct access to public endpoints on the internet. Connections can be initiated from the subnet or from the internet. The resources in the public subnet must have public IP addresses. For more information, see *Internet Gateway* on page 3243.
- **Service gateway**: To provide the private subnet with private access to supported Oracle services within the region. Connections can be initiated only from the subnet.
- **NAT gateway**: To provide the private subnet with private access to public endpoints on the internet. Connections can be initiated only from the subnet. For more information, see *NAT Gateway* on page 3247.

You control routing in your VCN at the subnet level, so you can specify which subnets in your VCN use each gateway. In the diagram, the route table for the public subnet sends non-local traffic through the internet gateway. The route table for the private subnet sends traffic destined for the Oracle services through the service gateway. It sends all remaining traffic to the NAT gateway.

**Important:**

See this known issue for information about configuring route rules with service gateway as the target on route tables associated with public subnets.

A service gateway can be used by resources in the gateway's own VCN. However, if the VCN is peered with another, resources in the other VCN cannot access the service gateway unless a service gateway is configured in both VCNs. You could configure traffic destined for Oracle Services Network that originates on a spoke to travel through a network virtual appliance (NVA) in the hub and then through the hub's service gateway. See Using a Private IP as a Route Target on page 2924 and Transit Routing: Private Access to Oracle Services on page 2803 for more information.

Resources in your on-premises network that is connected to the service gateway's VCN with FastConnect or VPN Connect can also use the service gateway. For more information, see Transit Routing: Private Access to Oracle Services on page 2803.

Notice that your on-premises network can also use FastConnect public peering for private access to public Oracle services. That means that your on-premises network could have multiple paths to access Oracle services public IP address ranges. If that is the case, your edge device receives route advertisement of the Oracle services public IP address ranges over multiple paths. For important information about configuring your edge device correctly, see Routing Details for Connections to Your On-Premises Network on page 2942.

A VCN can have only one service gateway. For more information about limits, see Service Limits on page 215.
For instructions on setting up a service gateway, see Setting Up a Service Gateway in the Console on page 3260.

About Service CIDR Labels

Each Oracle service has a regional public endpoint that uses public IP addresses for access. When you set up a service gateway with access to an Oracle service, you also set up Networking service route rules and optionally security rules that control traffic with the service. That means you need to know the service's public IP addresses to set up those rules. To make it easier for you, the Networking service uses service CIDR labels to represent all the public CIDRs for a given Oracle service or a group of Oracle services. If a service's CIDRs change in the future, you don't have to adjust your route rules or security rules.

Examples:

- **OCI PHX Object Storage** is a service CIDR label that represents all the Object Storage CIDRs in the US West (Phoenix) region.
- **All PHX Services in Oracle Services Network** is a service CIDR label that represents all the CIDRs for the supported services in the Oracle Services Network in the US West (Phoenix) region. For a list of the services, see Service Gateway: Supported Cloud Services in Oracle Services Network.

As you can see, a service CIDR label can be associated with either a single Oracle service (example: Object Storage), or multiple Oracle services.

The term service is often used in this topic in place of the more accurate term service CIDR label. The important thing to remember is that when you set up a service gateway (and related route rules), you specify the service CIDR label you're interested in. In the Console, you're presented with the available service CIDR labels. If you use the REST API, the ListServices operation returns the available Service objects. The Service object's cidrBlock attribute contains the service CIDR label (example: all-phx-services-in-oracle-services-network).

Available Service CIDR Labels

Here are the available service CIDR labels:

- **OCI <region> Object Storage**: For information about the service, see Overview of Object Storage on page 3392
- **All <region> Services in Oracle Services Network**: For a list of supported services, see Service Gateway: Supported Cloud Services in Oracle Services Network.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>See this known issue for information about accessing Oracle YUM services through the service gateway.</td>
</tr>
</tbody>
</table>

Enabling a Service CIDR Label for a Service Gateway

To give your VCN access to a given service CIDR label, you must **enable** that service CIDR label for the VCN's service gateway. You can do that when you create the service gateway, or later after it's created. You can also disable a service CIDR label for the service gateway at any time.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Because Object Storage is covered by both OCI &lt;region&gt; Object Storage and All &lt;region&gt; Services in Oracle Services Network, a service gateway can use only one of those service CIDR labels. Likewise, a route table can have a single rule for one of the service CIDR labels. It cannot have two separate rules, one for each label.</td>
</tr>
<tr>
<td>If the service gateway is configured to use All &lt;region&gt; Services in Oracle Services Network, the route rule can use either CIDR label. However, if the service gateway is configured to use OCI &lt;region&gt; Object Storage and the route rule uses All &lt;region&gt; Services in Oracle Services Network, traffic to services in the Oracle Services Network except Object Storage will be</td>
</tr>
</tbody>
</table>
Networking

blackholed. The Console prohibits you from configuring the service gateway and corresponding route table in that manner.

If you want to switch the service gateway to use a different service CIDR label, see To switch to a different service CIDR label on page 3263.

Blocking Traffic Through a Service Gateway

You create a service gateway in the context of a specific VCN. In other words, the service gateway is always attached to that one VCN. However, you can block or allow traffic through the service gateway at any time. By default, the gateway allows traffic flow upon creation. Blocking the service gateway traffic prevents all traffic from flowing, regardless of what service CIDR labels are enabled, or any existing route rules or security rules in your VCN. For instructions on how to block traffic, see To block or allow traffic for a service gateway on page 3263.

Route Rules and Security Rules for a Service Gateway

For traffic to be routed from a subnet in your VCN to a service gateway, you must add a rule accordingly to the subnet's route table. The rule must use the service gateway as the target. For the destination, you must use the service CIDR label that is enabled for the service gateway. This means that you don't have to know the specific public CIDRs, which could change over time.

Any traffic leaving the subnet and destined for the service's public CIDRs is then routed to the service gateway. If the service gateway traffic is blocked, no traffic flows through it even if there's a route rule that matches the traffic. For instructions on setting up route rules for a service gateway, see Task 2: Update routing for the subnet on page 3260.

The VCN's security rules must also allow the desired traffic. If you like, you can use a service CIDR label instead of a CIDR for the source or destination of the desired traffic. Again, this means that you don't have to know the specific public CIDRs for the service. For convenience, you can use a service CIDR label in security rules even if your VCN doesn't have a service gateway, and the traffic to the services uses an internet gateway.

You can use stateful or stateless security rules that use a service CIDR label:

- **For stateful rules**: Create an egress rule with the destination service = the service CIDR label of interest. As with any security rule, you can specify other items such as the IP protocol and source and destination ports.
- **For stateless rules**: You must have both egress and ingress rules. Create an egress rule with the destination service = the service CIDR label of interest. Also create an ingress rule with the source service = the service CIDR label of interest. As with any security rule, you can specify other items such as the IP protocol and source and destination ports.

For instructions on setting up security rules that use a service CIDR label, see Task 3: (Optional) Update security rules on page 3261.

Object Storage: Allowing Bucket Access from Only a Particular VCN or CIDR Range

If you use a service gateway to access Object Storage, you can write an IAM policy that allows access to a particular Object Storage bucket only if these requirements are met:

- The request goes through a service gateway.
- The request originates from the particular VCN that is specified in the policy.

For examples of this particular type of IAM policy, and important caveats about its use, see Task 4: (Optional) Update IAM Policies to Restrict Object Storage Bucket Access on page 3262.

Alternatively, you can use IAM IP-based filtering to restrict access to an IP address or ranges of addresses. For more information, see Managing Network Sources on page 2427.

Deleting a Service Gateway

To delete a service gateway, its traffic does not have to be blocked, but there must not be a route table that lists it as a target. See To delete a service gateway on page 3264.
Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: see IAM Policies for Networking on page 2832.

Setting Up a Service Gateway in the Console

Following is the process for setting up a service gateway. It assumes that you already have a VCN with a subnet (either private or public).

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The service gateway allows access to supported Oracle services within the region to protect your data from the internet. Your applications may require access to public endpoints or services not supported by the service gateway (for example, to download updates or patches). Ensure you have a NAT gateway or other access to the internet if necessary.</td>
</tr>
</tbody>
</table>

Task 1: Create the service gateway

1. In the Console, confirm you're viewing the compartment that contains the VCN that you want to add the service gateway to. For information about compartments and access control, see Access Control on page 2831.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
3. Click the VCN you're interested in.
4. On the left side of the page, click Service Gateways.
5. Click Create Service Gateway.
6. Enter the following values:
   - **Name**: A descriptive name for the service gateway. It doesn't have to be unique. Avoid entering confidential information.
   - **Create in compartment**: The compartment where you want to create the service gateway, if different from the compartment you're currently working in.
   - **Services**: Optionally select the service CIDR label you're interested in. If you don't select one now, you can later update the service gateway and add a service CIDR label then. Without at least one service CIDR label enabled for the gateway, no traffic flows through it.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click Create Service Gateway.

The service gateway is then created and displayed on the Service Gateways page in the compartment you chose. The gateway allows traffic through it by default. At any time, you can block or allow the traffic through it.

Task 2: Update routing for the subnet

When you configure a service gateway for a particular service CIDR label, you must also create a route rule that specifies that label as the destination and the target as the service gateway. You do this for each subnet that needs to access the gateway.

1. Determine which subnets in your VCN need access to the service gateway.
2. For each of those subnets, update the subnet's route table to include a new rule:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click the VCN you're interested in.
   c. Under Resources, click Route Tables.
   d. Click the route table you're interested in.
   e. Click Edit Route Rules.
   f. Click Add Route Rule and enter the following values:
      • Target Type: Service Gateway.
      • Destination Service: The service CIDR label that is enabled for the gateway.
      • Compartment: The compartment where the service gateway is located.
      • Target: The service gateway.
      • Description: An optional description of the rule.
   g. Click Save.

Any subnet traffic with a destination that matches the rule is routed to the service gateway. For more information about setting up route rules, see Route Tables on page 2921.

Later, if you no longer need the service gateway and want to delete it, you must first delete all the route rules in your VCN that specify the service gateway as the target.

**Tip:**
Without the required routing, traffic doesn't flow over the service gateway.
If a situation occurs where you want to temporarily stop the traffic flow over the gateway to a particular service, you can simply remove the route rule that enables traffic. You can also disable that particular service CIDR label for the gateway. Or you can block all traffic through the service gateway entirely.
You do not have to delete the gateway.

**Task 3: (Optional) Update security rules**

When you configure a service gateway to access a service CIDR label, you must also ensure that the security rules are configured to allow the desired traffic. Your security rules might already allow this traffic, which is why this task is optional. The following procedure assumes you are using security lists to implement your security rules. The procedure describes how to set up a rule that uses the service CIDR label. You do this for each subnet that needs to access the gateway.

**Tip:**
Security lists are one way to control traffic in and out of the VCN's resources.
You can also use network security groups, which let you apply a set of security rules to a set of resources that all have the same security posture.

1. Determine which subnets in your VCN need to connect to the services you're interested in.
2. Update the security list for each of those subnets to include rules to allow the desired egress or ingress traffic with the particular service:
   
a. In the Console, while viewing the VCN you're interested in, click Security Lists.
   
b. Click the security list you're interested in.
   
c. Click Edit All Rules and create one or more rules, each for the specific type of traffic you want to allow. See the following example for more details.
   
   Example
   
   Let's say you want to add a stateful rule that enables egress HTTPS (TCP port 443) traffic from the subnet to both Object Storage and Oracle YUM repos. Here are the basic steps you take when adding a rule:
   
   1. In the Allow Rules for Egress section, click +Add Rule.
   
   2. Leave the Stateless check box unselected.
   
   3. Destination Type: Service.
   
   4. Destination Service: The service CIDR label that you're interested in. To access both Object Storage and Oracle YUM repos, it's All <region> Services in Oracle Services Network.
   
   5. IP Protocol: Leave as TCP.
   
   6. Source Port Range: Leave as All.
   
   7. Destination Port Range: Enter 443.
   
   8. Description: An optional description of the rule.
   
   d. Click Save Security List Rules at the bottom of the dialog box.
   
   For more information about setting up security rules, see Security Rules on page 2833.

   Task 4: (Optional) Update IAM Policies to Restrict Object Storage Bucket Access
   
   This task is applicable only if you're using a service gateway to access Object Storage. You can optionally create a network source and write an IAM policy to allow only the resources in a specific VCN to write objects to a particular bucket.
   
   Important:
   
   If you use one of the following IAM policies to restrict access to a bucket, the bucket is not accessible from the Console. It's accessible only from within the specific VCN.
   
   Also, the IAM policies allow requests to Object Storage only if they go from the specified VCN through the service gateway. If they go through the internet gateway, the requests are denied.
   
   • Create a network source to specify the allowed VCN. For information on creating network sources, see Managing Network Sources on page 2427.
   
   • Create the policy. The following example lets resources in the example ObjectBackup group write objects to an existing bucket called db-backup that resides in a compartment called ABC.
   
   Allow group ObjectBackup to read buckets in compartment ABC
   
   Allow group ObjectBackup to manage objects in compartment ABC where all [target.bucket.name='db-backup', request.networkSource.name='<VCN_NETWORK_SOURCE>', any [request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT']]}

   You can specify multiple VCNs by creating and specifying multiple network sources in the policy. The next example has network sources for two VCNs. You might do this if you've set up your on-premises network with private access to Oracle services through a VCN, and you've also set up one or more other VCNs with their own service gateways. For more information, see Overview of On-Premises Network Private Access to Oracle Services on page 2804.
   
   Allow group ObjectBackup to read buckets in compartment ABC
Allow group ObjectBackup to manage objects in compartment ABC where
all {target.bucket.name='db-backup',
    any {request.networkSource.name='<NETWORK_SOURCE_FOR_VCN_1>',
        request.networkSource.name='<NETWORK_SOURCE_FOR_VCN_2>',
        any {request.permission='OBJECT_CREATE',
        request.permission='OBJECT_INSPECT'})

Managing a Service Gateway in the Console

To create a service gateway

See the instructions in Task 1: Create the service gateway on page 3260.

To switch to a different service CIDR label

To avoid disrupting your Object Storage connections while switching between the OCI <region> Object Storage
service CIDR label and All <region> Services in Oracle Services Network, use the following process:

1. **Update the service gateway:** Remove the existing service CIDR label, and then add the one you want to switch to.
   You can't enable both labels for the service gateway.
2. **Update relevant route rules:** For each rule that uses the service gateway as the target, switch the rule's destination
   service from the existing service CIDR label to the one you want to switch to.
3. **Update relevant security rules:** Change any security rules that specify the existing service CIDR label to instead
   use the one you want to switch to. The rules can be in network security groups or security lists.

If you instead delete your existing service gateway and create a new one, your Object Storage connections will be
interrupted. Remember that before you can delete a service gateway, you must delete any route rules that specify that
gateway as a target.

To update a service gateway

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click Service Gateways.
4. For the service gateway you're interested in, click the Actions icon (three dots), and then click Edit.
5. Make your changes and click Save.

To block or allow traffic for a service gateway

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
3. Click Service Gateways.
4. For the service gateway you're interested in, click the Actions icon (three dots), and then click Block Traffic (or
   Allow Traffic if you're enabling traffic for the service gateway).
   When the traffic is blocked, the service gateway's icon turns gray, and the label changes to BLOCKED. When the
   traffic is allowed, the service gateway's icon turns green, and the label changes to AVAILABLE.

To associate a route table with an existing service gateway

You perform this task only if you're implementing an advanced transit routing scenario.

A service gateway can exist without a route table associated with it. However, after you associate a route table with a
service gateway, there must always be a route table associated with it. But, you can associate a different route table.
You can also edit the table's rules, or delete some or all of the rules.

**Prerequisite:** The route table must exist and belong to the VCN that the service gateway belongs to.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the service gateway you're interested in, click the Actions icon (three dots), and then click either:
   - **Associate With Route Table:** If the service gateway has no route table associated with it yet.
   - **Associate Different Route Table:** If you're changing which route table is associated with the service gateway.
5. Select the compartment where the route table resides, and select the route table itself.
6. Click **Associate**.

**To delete a service gateway**

Prerequisite: The service gateway does not have to block traffic, but there must not be a route table that lists it as a target.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click **Service Gateways**.
4. For the service gateway you're interested in, click the Actions icon (three dots), and then click **Delete**.
5. Confirm when prompted.

**To manage tags for a service gateway**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. For the service gateway you're interested in, click the Actions icon (three dots), and then click **View Tags**. From there you can view the existing tags, edit them, and apply new ones.

For more information, see **Resource Tags** on page 211.

**To move a service gateway to a different compartment**

You can move a service gateway from one compartment to another. When you move a service gateway to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. In **Resources**, click **Service Gateways**.
4. Find the service gateway in the list, click the the Actions icon (three dots), and then click **Move Resource**.
5. Choose the destination compartment from the list.
6. Click **Move Resource**.

The service gateway moves to the new compartment immediately. Depending on your permissions, you can select the compartment in the left side menu to view the service gateway.

For more information about using compartments and policies to control access to your cloud network, see **Access Control** on page 2831. For general information about compartments, see **Managing Compartments** on page 2431.

**Managing a Service Gateway with the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

**Caution:**

If anyone in your organization implements a service gateway, be aware that you **may need to update any client code that works with Networking service route rules and security lists**. There are possible breaking API changes. For more information, see the **service gateway release notes**.

To manage your service gateways, use these operations:

- **ListServiceGateways**
- **CreateServiceGateway**
- **GetServiceGateway**
- **UpdateServiceGateway**
Networking

- DeleteServiceGateway
- ChangeServiceGatewayCompartment
- ListServices: Use this to determine the available service CIDR labels.
- GetService: Gets the details for a particular service CIDR label.
- AttachServiceld: Enables a service CIDR label for a service gateway.
- DetachServiceld: Disables a service CIDR label for a service gateway.

To manage route tables, see Route Tables on page 2921. To manage security lists, see Security Lists on page 2850. To manage network security groups, see Network Security Groups on page 2841. To manage IAM policies, see Managing Policies on page 2450.

Access to Other VCNs: Peering

VCN peering is the process of connecting multiple virtual cloud networks (VCNs). There are two types of VCN peering:

- Local VCN peering (within region)
- Remote VCN peering (across regions)

You can use VCN peering to divide your network into multiple VCNs (for example, based on departments or lines of business), with each VCN having direct, private access to the others. There's no need for traffic to flow over the internet or through your on-premises network by way of an IPSec VPN or FastConnect. You can also place shared resources into a single VCN that all the other VCNs can access privately.

Because remote VCN peering crosses regions, you can use it (for example) to mirror or back up your databases in one region to another.

Important Implications of Peering

This section summarizes some access control, security, and performance implications for peered VCNs. In general, you can control access and traffic between two peered VCNs by using IAM policies, route tables in each VCN, and security lists in each VCN.

Controlling the Establishment of Peerings

With IAM policies, you can control:

- Who can subscribe your tenancy to another region (required for remote VCN peering).
- Who in your organization has the authority to establish VCN peerings (for example, see the IAM policies in Setting Up a Local Peering on page 3271 and Setting Up a Remote Peering on page 3284). Be aware that deletion of these IAM policies does not affect any existing peerings, only the ability for future peerings to be created.
- Who can manage route tables and security lists.

Controlling Traffic Flow Over the Connection

Even if a peering connection has been established between your VCN and another, you can control the packet flow over the connection with route tables in your VCN. For example, you can restrict traffic to only specific subnets in the other VCN.

Without terminating the peering, you can stop traffic flow to the other VCN by simply removing route rules that direct traffic from your VCN to the other VCN. You can also effectively stop the traffic by removing any security list rules that enable ingress or egress traffic with the other VCN. This doesn't stop traffic flowing over the peering connection, but stops it at the VNIC level.

For more information about the routing and security lists, see the discussions in these sections:

Local VCN peering:

- Important Local Peering Concepts on page 3268
- Task E: Configure the route tables on page 3277
Controlling the Specific Types of Traffic Allowed

It’s important that each VCN administrator ensure that all outbound and inbound traffic with the other VCN is intended/expected and well defined. In practice, this means implementing security list rules that explicitly state the types of traffic your VCN can send to the other and accept from the other.

Important:

Your instances running Oracle-provided Linux images or Windows images also have OS firewall rules that control access to the instance. When troubleshooting access to an instance, make sure that all of the following items are set correctly:

- The rules in the network security groups that the instance is in
- The rules in the security lists associated with the instance’s subnet
- The instance’s OS firewall rules

For more information, see Oracle-Provided Images on page 629.

If your instance is running Oracle Autonomous Linux 7, Oracle Linux 8, or Oracle Linux 7, you need to use firewalld to interact with the iptables rules. For your reference, here are commands for opening a port (1521 in this example):

```
sudo firewall-cmd --zone=public --permanent --add-port=1521/tcp
sudo firewall-cmd --reload
```

For instances with an iSCSI boot volume, the preceding --reload command can cause problems. For details and a workaround, see Instances experience system hang after running firewall-cmd --reload.

In addition to security lists and firewalls, you should evaluate other OS-based configuration on the instances in your VCN. There could be default configurations that don’t apply to your own VCN’s CIDR, but inadvertently apply to the other VCN’s CIDR.

Using Default Security List Rules

If your VCN’s subnets use the default security list with the default rules it comes with, be aware that there are two rules that allow ingress traffic from anywhere (that is, 0.0.0.0/0, and thus the other VCN):

- Stateful ingress rule that allows TCP port 22 (SSH) traffic from 0.0.0.0/0 and any source port
- Stateful ingress rule that allows ICMP type 3, code 4 traffic from 0.0.0.0/0 and any source port

Make sure to evaluate these rules and whether you want to keep or update them. As stated earlier, you should ensure that all inbound or outbound traffic that you permit is intended/expected and well defined.

Preparing for Performance Impact and Security Risks

In general, you should prepare your VCN for the ways it could be affected by the other VCN. For example, the load on your VCN or its instances could increase. Or your VCN could experience a malicious attack directly from or by way of the other VCN.
Regarding performance: If your VCN is providing a service to another, be prepared to scale up your service to accommodate the demands of the other VCN. This might mean being prepared to launch additional instances as necessary. Or if you're concerned about high levels of network traffic coming to your VCN, consider using stateless security list rules to limit the level of connection tracking your VCN must perform. Stateless security list rules can also help slow the impact of a denial-of-service (DoS) attack.

Regarding security risks: You can't necessarily control whether the other VCN is connected to the internet. If it is, be aware that your VCN can be exposed to bounce attacks in which a malicious host on the internet can send traffic to your VCN but make it look like it's coming from the VCN you're peered with. To guard against this, as mentioned earlier, use your security lists to carefully limit the inbound traffic from the other VCN to expected and well-defined traffic.

**Local VCN Peering (Within Region)**

This topic is about *local VCN peering*. In this case, *local* means that the VCNs reside *in the same region*. If the VCNs are in different regions, see Remote VCN Peering (Across Regions) on page 3280.

**Overview of Local VCN Peering**

*Local VCN peering* is the process of connecting two VCNs in the same region so that their resources can communicate using private IP addresses without routing the traffic over the internet or through your on-premises network. The VCNs can be in the same Oracle Cloud Infrastructure *tenancy* or different ones. Without peering, a given VCN would need an internet gateway and public IP addresses for the instances that need to communicate with another VCN.

For more information, see Access to Other VCNs: Peering on page 3265.

**Summary of Networking Components for Peering**

At a high level, the Networking service components required for a local peering include:

- Two VCNs with non-overlapping CIDRs, in the same region
- A *local peering gateway (LPG)* on each VCN in the peering relationship.
- A *connection* between those two LPGs.
- Supporting route rules to enable traffic to flow over the connection, and only to and from select subnets in the respective VCNs (if desired).
- Supporting security rules to control the types of traffic allowed to and from the instances in the subnets that need to communicate with the other VCN.

The following diagram illustrates the components.

![Diagram of local VCN peering](image_url)

**Note:**

A given VCN can use the peered LPGs to reach these resources:

- VNICs in the other VCN
Networking

• An on-premises network attached to the other VCN, if an advanced routing scenario called **transit routing** has been set up for the VCNs

A VCN can't use its peered VCN to reach other destinations outside of the VCNs (such as the internet). For example, if VCN-1 in the preceding diagram were to have an internet gateway, the instances in VCN-2 could not use it to send traffic to endpoints on the internet. However, be aware that VCN-2 could receive traffic from the internet by way of VCN-1. For more information, see **Important Implications of VCN Peering** on page 3271.

**Explicit Agreement Required from Both Sides**

Peering involves two VCNs that might be owned by the same party or two different ones. The two parties might both be in your company but in different departments. Or the two parties might be in entirely different companies (for example, in a service-provider model).

Peering between two VCNs requires explicit agreement from both parties in the form of Oracle Cloud Infrastructure Identity and Access Management policies that each party implements for their own VCN's **compartment** or tenancy. If the VCNs are in different tenancies, each administrator must provide their tenancy **OCID** and put in place special policy statements to enable the peering.

**Advanced Scenario: Transit Routing**

There's an advanced routing scenario called **transit routing** that enables communication between an on-premises network and multiple VCNs over a single Oracle Cloud Infrastructure FastConnect or IPSec VPN. The VCNs must be in the same region and locally peered in a hub-and-spoke layout. As part of the scenario, the VCN that is acting as the hub has a route table associated with each LPG (typically route tables are associated with a VCN's subnets).

When you create an LPG, you can optionally associate a route table with it. Or if you already have an existing LPG without a route table, you can associate a route table with it. The route table must belong to the LPG's VCN. A route table associated with an LPG can contain only rules that use the VCN's attached DRG as the target.

An LPG can exist without a route table associated with it. However, after you associate a route table with an LPG, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

**Important Local Peering Concepts**

The following concepts help you understand the basics of VCN peering and how to establish a local peering.

**PEERING**

A **peering** is a single peering relationship between two VCNs. Example: If VCN-1 peers with three other VCNs, then there are three peerings. The **local** part of **local peering** indicates that the VCNs are in the same region. A given VCN can have a maximum of ten local peerings at a time.

**Caution:**

The two VCNs in the peering relationship must not have overlapping CIDRs. However, if VCN-1 is peered with three other VCNs, those three VCNs can have overlapping CIDRs with each other. You would set up the subnets in VCN-1 to have route rules that direct traffic to the targeted peered VCN.

**VCN ADMINISTRATORS**

In general, VCN peering can occur only if both of the VCN administrators agree to it. In practice, this means that the two administrators must:

• Share some basic information with each other.
• Coordinate to set up the required Oracle Cloud Infrastructure Identity and Access Management policies to enable the peering.
• Configure their VCNs for the peering.

Depending on the situation, a single administrator might be responsible for both VCNs and the related policies.

For more information about the required policies and VCN configuration, see Setting Up a Local Peering on page 3271.

**ACCEPTOR AND REQUESTOR**

To implement the IAM policies required for peering, the two VCN administrators must designate one administrator as the requestor and the other as the acceptor. The requestor must be the one to initiate the request to connect the two LPGs. In turn, the acceptor must create a particular IAM policy that gives the requestor permission to connect to LPGs in the acceptor's compartment. Without that policy, the requestor's request to connect fails.

**LOCAL PEERING GATEWAY (LPG)**

A local peering gateway (LPG) is a component on a VCN for routing traffic to a locally peered VCN. As part of configuring the VCNs, each administrator must create an LPG for their VCN. A given VCN must have a separate LPG for each local peering it establishes (maximum ten LPGs per VCN). To continue with the previous example: VCN-1 would have three LPGs to peer with three other VCNs. In the API, a LocalPeeringGateway is an object that contains information about the peering. You can't reuse an LPG to later establish another peering.

**PEERING CONNECTION**

When the requestor initiates the request to peer (in the Console or API), they're effectively asking to connect the two LPGs. The requestor must have information to identify each LPG (such as the LPG’s compartment and name, or the LPG’s OCID). Each administrator must put the required IAM policies in place for their compartment or tenancy.

Either VCN administrator can terminate a peering by deleting their LPG. In that case, the other LPG's status switches to REVOKED. The administrator could instead render the connection non-functional by removing the route rules or security rules that enable traffic to flow across the connection (see the next sections).

**ROUTING TO THE LPG**

As part of configuring the VCNs, each administrator must update the VCN’s routing to enable traffic to flow between the VCNs. In practice, this looks just like routing you set up for any gateway (such as an internet gateway or dynamic routing gateway). For each subnet that needs to communicate with the other VCN, you update the subnet's route table. The route rule specifies the destination traffic's CIDR and your LPG as the target. Your LPG routes traffic that matches that rule to the other LPG, which in turn routes the traffic to the next hop in the other VCN.

In the following diagram, VCN-1 and VCN-2 are peered. Traffic from an instance in Subnet A (10.0.0.15) that is destined for an instance in VCN-2 (192.168.0.15) is routed to LPG-1 based on the rule in Subnet A's route table. From there the traffic is routed to LPG-2, and then from there, on to its destination in Subnet X.
As mentioned earlier, a given VCN can use the peered LPGs to reach VNICs in the other VCN, or the on-premises network if transit routing is set up for the VCNs. But a VCN can’t use the peered VCN to reach other destinations outside of the VCNs (such as the internet). For example, in the preceding diagram, VCN-2 cannot use the internet gateway attached to VCN-1.

SECURITY RULES

Each subnet in a VCN has one or more security lists that control traffic in and out of the subnet's VNICs at the packet level. You can use security lists to control the type of traffic allowed with the other VCN. As part of configuring the VCNs, each administrator must determine which subnets in their own VCN need to communicate with VNICs in the other VCN and update their subnet's security lists accordingly.

If you use network security groups (NSGs) to implement security rules, notice that you have the option to write security rules for an NSG that specify another NSG as the source or destination of traffic. However, the two NSGs must belong to the same VCN.
Important Implications of VCN Peering

If you haven't yet, read Important Implications of Peering on page 3265 to understand important access control, security, and performance implications for peered VCNs.

Setting Up a Local Peering

Here's the general process for setting up a peering between two VCNs in the same region:

1. **Create the LPGs:** Each VCN administrator creates an LPG for their own VCN.
2. **Share information:** The administrators share the basic required information.
3. **Set up the required IAM policies for the connection:** The administrators set up IAM policies to enable the connection to be established.
4. **Establish the connection:** The requestor connects the two LPGs.
5. **Update route tables:** Each administrator updates their VCN's route tables to enable traffic between the peered VCNs as desired.
6. **Update security rules:** Each administrator updates their VCN's security rules to enable traffic between the peered VCNs as desired.

If desired, the administrators can perform tasks E and F before establishing the connection. In that case, each administrator must know the CIDR block or specific subnets from the other's VCN and share that in task B. After the connection is established, you can also get the CIDR block of the other VCN by viewing your own LPG's details in the Console. Look for Peer Advertised CIDR. Or if you're using the API, see the peerAdvertisedCidr parameter.

**Task A: Create the LPGs**

Each administrator creates an LPG for their own VCN. “You” in the following procedure means an administrator (either the acceptor or requestor).

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required IAM Policy to Create LPGs</strong></td>
</tr>
<tr>
<td>If the administrators already have broad network administrator permissions (see Let network admins manage a cloud network on page 2143), then they have permission to create, update, and delete LPGs. Otherwise, here's an example policy giving the necessary permissions to a group called LPGAdmins. The second statement is required because creating an LPG affects the VCN it belongs to, so the administrator must have permission to manage VCNs.</td>
</tr>
<tr>
<td>Allow group LPGAdmins to manage local-peering-gateways in tenancy</td>
</tr>
<tr>
<td>Allow group LPGAdmins to manage vcns in tenancy</td>
</tr>
</tbody>
</table>

1. In the Console, confirm you're viewing the compartment that contains the VCN that you want to add the LPG to. For information about compartments and access control, see Access Control on page 2831.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
3. Click the VCN you're interested in.
4. Under Resources, click Local Peering Gateways.
5. Click Create Local Peering Gateway.
6. Enter the following:
   - **Name**: A friendly name for the LPG. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in compartment**: The compartment where you want to create the LPG, if different from the compartment you're currently working in.
   - **Associate with Route Table (optional)**: Only if you're setting up the advanced routing scenario called transit routing. Select the compartment that contains the route table you want to associate with the LPG, and the route table itself. You can skip this part and associate the LPG with a route table later if you like.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

7. Click **Create Local Peering Gateway**.

   The LPG is then created and displayed on the **Local Peering Gateways** page in the compartment you chose.

**Task B: Share information**

If you're the **requestor**, give this information to the acceptor (for example, by email or other out-of-band method):

   - If the VCNs are in the **same tenancy**: Name of the IAM group that should be granted permission to create a connection in the acceptor's compartment. In the example in the next task, the group is RequestorGrp.
   - If the VCNs are in **different tenancies**: OCID for your tenancy, and OCID for the IAM group that should be granted permission to create a connection in the acceptor's compartment. In the example in the next task, it's the OCID for the RequestorGrp.
   - Optional: Your VCN's CIDR, or specific subnets for peering with the other VCN.

If you're the **acceptor**, give this information to the requestor:

   - If the VCNs are in the **same tenancy**: OCID for your LPG. Optionally, also the names of your VCN, LPG, and the compartment each is in.
   - If the VCNs are in **different tenancies**: OCID for your LPG, and OCID for your tenancy.
   - Optional: Your VCN's CIDR, or specific subnets for peering with the other VCN.

**Task C: Set up the IAM policies (VCNs in same tenancy)**

In this version of task C, both VCNs are in the same tenancy. If they're in different tenancies, instead see Task C: Set up the IAM policies (VCNs in different tenancies) on page 3274.

Both the requestor and acceptor must ensure that the right policies are in place:

   - **Policy R (implemented by the requestor)**:
     
     ```
     Allow group RequestorGrp to manage local-peering-from in compartment RequestorComp
     ```

     The requestor is in an IAM group called RequestorGrp. This policy lets anyone in the group initiate a connection from any LPG in the requestor’s compartment (RequestorComp). Policy R can be attached to either the tenancy (root compartment) or to RequestorComp. For information about why you would attach it to one versus the other, see Policy Basics on page 2137.

   - **Policy A (implemented by the acceptor)**:
     
     ```
     Allow group RequestorGrp to manage local-peering-to in compartment AcceptorComp
     Allow group RequestorGrp to inspect vcns in compartment AcceptorComp
     ```
Networking

**Allow group RequestorGrp to inspect local-peering-gateways in compartment AcceptorComp**

The first statement in the policy lets the requestor connect to any LPG in the acceptor's compartment (AcceptorComp). This statement reflects the required agreement from the acceptor for the peering to be established. Policy A can be attached to either the tenancy (root compartment) or to AcceptorComp.

**Tip:**

The second and third statements in Policy A let the requestor list the VCNs and LPGs in AcceptorComp. The statements are required for the requestor to use the Console UI to select from a list of VCNs and LPGs in AcceptorComp and establish the connection. The following diagram focuses only on the first statement, which is the critical one that permits the connection.

Both Policy R and Policy A give RequestorGrp access. However, Policy R has a resource-type called local-peering-from, and Policy A has a resource-type called local-peering-to. Together, these policies let someone in RequestorGrp establish the connection from an LPG in the requestor's compartment to an LPG in the acceptor's compartment. The API call to create the connection specifies which two LPGs.

**Tip:**

The permission granted by Policy R might already be in place if the requestor has permission in another policy to manage all of the Networking components in RequesterComp. For example, there might be a general Network Admin policy like this:

**Allow group NetworkAdmin to manage virtual-network-family in compartment RequestorComp**
Networking

If the requestor is in the NetworkAdmin group, then they already have the required permissions covered in Policy R (the virtual-network-family includes LPGs). And further, if the policy is instead written to cover the entire tenancy instead of only compartment RequestorComp, then the requestor already has all the required permissions in both compartments to establish the connection. In that case, policy A is not required.

Task C: Set up the IAM policies (VCNs in different tenancies)

In this version of task C, the VCNs are in different tenancies (in other words, it's a cross-tenancy peering). If the VCNs are in the same tenancy, instead see Task C: Set up the IAM policies (VCNs in same tenancy) on page 3272.

Both the requestor and acceptor must ensure that the right policies are in place:

- **Policy R (implemented by the requestor):**

  Define tenancy Acceptor as <acceptor_tenancy_OCID>

  Allow group RequestorGrp to manage local-peering-from in compartment RequestorComp

  Endorse group RequestorGrp to manage local-peering-to in tenancy Acceptor

  Endorse group RequestorGrp to associate local-peering-gateways in compartment RequestorComp
  with local-peering-gateways in tenancy Acceptor

  The requestor is in an IAM group called RequestorGrp. This policy lets anyone in that group initiate a connection from any LPG in the requestor's compartment (RequestorComp).

  The first statement is a "define" statement that assigns a friendly label to the acceptor's tenancy OCID. The statement happens to use "Acceptor" as the label, but it could be a value of the requestor's choice. All "define" statements in a policy must be the first ones (at the top).

  The second statement lets the RequestorGrp establish a connection from an LPG in the requestor's compartment.

  The third and fourth statements are special ones required because the LPGs are in different tenancies. They let the RequestorGrp connect an LPG in the requestor's tenancy to an LPG in the acceptor's tenancy.

  If the desire is to give the RequestorGrp permission to connect to an LPG in any tenancy, the policy would instead look like this:

  Allow group RequestorGrp to manage local-peering-from in compartment RequestorComp

  Endorse group RequestorGrp to manage local-peering-to in any-tenancy

  Endorse group RequestorGrp to associate local-peering-gateways in compartment RequestorComp
  with local-peering-gateways in any-tenancy

  Regardless, Policy R must be attached to the requestor's tenancy (root compartment), and not the requestor's compartment. Policies that enable cross-tenancy access must be attached to the tenancy. For more information about attachment of policies, see Policy Basics on page 2137.
• **Policy A (implemented by the acceptor):**

```
Define tenancy Requestor as <requestor_tenancy_OCID>
Define group RequestorGrp as <RequestorGrp_OCID>
Admit group RequestorGrp of tenancy Requestor to manage local-peering-to
  in compartment AcceptorComp
Admit group RequestorGrp of tenancy Requestor to associate local-peering-
  gateways in tenancy Requestor
  with local-peering-gateways in compartment AcceptorComp
```

Similar to the requestor's policy, this policy first uses "define" statements to assign friendly labels to the requestor's tenancy OCID and the RequestorGrp OCID. As mentioned earlier, the acceptor could use other values for those labels if desired.

The third and fourth statements let the RequestorGrp connect to an LPG in the acceptor's compartment (AcceptorComp). **These statements reflect the critical agreement required for the peering to be established.** The word Admit indicates that the access applies to a group **outside the tenancy** where the policy resides.

Policy A must be attached to the acceptor's tenancy (root compartment), and not the acceptor's compartment.
Task D: Establish the connection

The requestor must perform this task.

Prerequisite: The requestor must have the OCID of the acceptor's LPG.

Tip:

If you're using the Console and the peering is between two VCNs in the same tenancy: Instead of specifying the acceptor's LPG OCID, you can instead pick the acceptor's VCN and LPG from lists of resources in the tenancy. However, you need to know both the name and compartment for the acceptor's VCN and LPG instead of the LPG's OCID. For reference, see Task B: Share information on page 3272.

1. In the Console, view the details for the requestor LPG that you want to connect to the acceptor LPG.
2. For the requestor LPG, click the Actions icon (three dots), and then click Establish Peering Connection.
3. Specify which LPG you want to peer with:
   - If the VCNs are in different tenancies: Select Enter Local Peering Gateway OCID, and enter the acceptor LPG's OCID.
   - If the VCNs are in the same tenancy: Do one of the following:
     - Select Enter Local Peering Gateway OCID, and enter the acceptor LPG's OCID.
     - Select Browse Below, and then select the acceptor's VCN and LPG from the lists provided. Remember that the VCN and LPG each might be in a different compartment than the one you're currently working in.

4. Click Establish Peering Connection.

The connection is established and the LPG's state changes to PEERED.

At this point, the details of each LPG update to show the Peer VCN CIDR Block for the other VCN. This is the CIDR of the other VCN across the peering from the LPG. Each administrator can use this information to update the route tables and security rules for their own VCN.

Task E: Configure the route tables

As mentioned earlier, each administrator can do this task before or after the connection is established.

Prerequisite: Each administrator must have the CIDR block or specific subnets for the other VCN. If the connection is already established, look at the Peer VCN CIDR Block for your LPG in the Console. Otherwise, get the information from the other administrator by email or other method.

For your own VCN:

1. Determine which subnets in your VCN need to communicate with the other VCN.
2. Update the route table for each of those subnets to include a new rule that directs traffic destined for the other VCN's CIDR to your LPG:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click the VCN you're interested in.
   c. Under Resources, click Route Tables.
   d. Click the route table you're interested in.
   e. Click Add Route Rule and enter the following:
      - Target Type: Local Peering Gateway.
      - Destination CIDR Block: The other VCN's CIDR block. If you want, you can specify a subnet or particular subset of the peered VCN's CIDR.
      - Target Compartment: The compartment where the LPG is located, if not the current compartment.
      - Target: The LPG.
      - Description: An optional description of the rule.
   f. Click Add Route Rule.

Any subnet traffic with a destination that matches the rule is routed to your LPG. For more information about setting up route rules, see Route Tables on page 2921.

Later, if you no longer need the peering and want to delete your LPG, you must first delete all the route rules in your VCN that specify the LPG as the target.

Tip:

Without the required routing, traffic doesn't flow between the peered LPGs. If a situation occurs where you need to temporarily stop the peering, you can simply remove the route rules that enable traffic. You don't need to delete the LPGs.

Task F: Configure the security rules

As mentioned earlier, each administrator can do this task before or after the connection is established.
Prerequisite: Each administrator must have the CIDR block or specific subnets for the other VCN. In general, you should use the same CIDR block you used in the route table rule in Task E: Configure the route tables on page 3277.

What rules should you add?

- Ingress rules for the types of traffic you want to allow from the other VCN, specifically from the VCN's CIDR or specific subnets.
- Egress rule to allow outgoing traffic from your VCN to the other VCN. If the subnet already has a broad egress rule for all types of protocols to all destinations (0.0.0.0/0), then you don't need to add a special one for the other VCN.

**Note:**

The following procedure uses security lists, but you could instead implement the security rules in a network security group and then create all of the subnet's resources in that NSG.

For your own VCN:

1. Determine which subnets in your VCN need to communicate with the other VCN.
2. Update the security list for each of those subnets to include rules to allow the desired egress or ingress traffic specifically with the CIDR block or subnet of the other VCN:
   a. In the Console, while viewing the VCN you're interested in, click Security Lists.
   b. Click the security list you're interested in.
   c. Under Resources, click either Ingress Rules or Egress Rules depending on the type of rule you want to work with.
   d. If you want to add a new rule, click Add Ingress Rule (or Add Egress Rule).
      
      **Example**
      
      Let's say you want to add a stateful rule that enables ingress HTTPS (port 443) traffic from the other VCN's CIDR. Here are the basic steps you take when adding a rule:

      1. Leave the Stateless check box unselected.
      2. Source Type: Leave as CIDR.
      3. Source CIDR: Enter the same CIDR block that the route rules use (see Task E: Configure the route tables on page 3277).
      4. IP Protocol: Leave as TCP.
      5. Source Port Range: Leave as All.
      6. Destination Port Range: Enter 443.
      7. Description: An optional description of the rule.
   e. If you want to delete an existing rule, click the Actions icon (three dots), and then click Remove.
   f. If you wanted to edit an existing rule, click the Actions icon (three dots), and then click Edit.

For more information about security rules, see Security Rules on page 2833.

**Using the Console**

*To create a local peering gateway*

See the instructions in Task A: Create the LPGs on page 3271.

*To associate a route table with an existing local peering gateway*

This task is related to an advanced routing scenario called transit routing.

An LPG can exist without a route table associated with it. However, after you associate a route table with an LPG, there must always be a route table associated with it. But, you can associate a different route table. You can also edit the table's rules, or delete some or all of the rules.

**Prerequisite:** The route table must exist and belong to the VCN that the LPG belongs to.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN you're interested in.
4. For the LPG you're interested in, click the Actions icon (three dots), and then click either:
   - **Associate With Route Table:** If the LPG has no route table associated with it yet.
   - **Replace Route Table Association:** If you're changing which route table is associated with the LPG.
5. Select the compartment where the route table resides, and select the route table itself.
6. Click **Associate**.

### To delete a local peering gateway

**Prerequisite:** First delete all the route rules in your VCN that specify the LPG as the target. Deleting those rules stops the routing in your VCN to the LPG. However, the LPG's state may still be PEERED if the other LPG still exists. Whenever an LPG is deleted, the LPG at the other side of the peering changes to the REVOKED state.

1. Open the navigation menu. Under Core Infrastructure, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click Local Peering Gateways.
4. For the LPG you want to delete, click the Actions icon (three dots), and then click **Terminate**.
5. Confirm when prompted.

#### Note:

After deleting an LPG (and thus terminating a peering), it's recommended you review your security rules to remove any rules that enabled traffic with the other VCN.

### To manage tags for a local peering gateway

1. Open the navigation menu. Under Core Infrastructure, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
4. Click the Actions icon (three dots) for the local peering gateway, and then click View Tags. From there you can view the existing tags, edit them, and apply new ones.

For more information, see Resource Tags on page 211.

### To move a local peering gateway to a different compartment

You can move a local peering gateway from one compartment to another. When you move a local peering gateway to a new compartment, inherent policies apply immediately.

1. Open the navigation menu. Under Core Infrastructure, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
4. Click the Actions icon (three dots) for the local peering gateway, and then click **Move Resource**.
5. Choose the destination compartment from the list.
6. Click **Move Resource**.

For more information about using compartments and policies to control access to your cloud network, see Access Control on page 2831. For general information about compartments, see Managing Compartments on page 2431.

### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage your LPGs and create connections, use these operations:

- ListLocalPeeringGateways
- CreateLocalPeeringGateway
- GetLocalPeeringGateway
• UpdateLocalPeeringGateway
• DeleteLocalPeeringGateway
• ConnectLocalPeeringGateways
• ChangeLocalPeeringGatewayCompartment

Remote VCN Peering (Across Regions)

This topic is about remote VCN peering. In this case, remote means that the VCNs reside in different regions. If the VCNs you want to connect are in the same region, see Local VCN Peering (Within Region) on page 3267.

Overview of Remote VCN Peering

Remote VCN peering is the process of connecting two VCNs in different regions (but the same tenancy). The peering allows the VCNs' resources to communicate using private IP addresses without routing the traffic over the internet or through your on-premises network. Without peering, a given VCN would need an internet gateway and public IP addresses for the instances that need to communicate with another VCN in a different region.

Summary of Networking Components for Remote Peering

At a high level, the Networking service components required for a remote peering include:

• Two VCNs with non-overlapping CIDRs, in different regions that support remote peering. The VCNs must be in the same tenancy.

Note:

All VCN CIDRs Must Not Overlap
The two VCNs in the peering relationship must not have overlapping CIDRs. Also, if a particular VCN has multiple peering relationships, those other VCNs must not have overlapping CIDRs with each other. For example, if VCN-1 is peered with VCN-2 and also VCN-3, then VCN-2 and VCN-3 must not have overlapping CIDRs.

• A dynamic routing gateway (DRG) attached to each VCN in the peering relationship. Your VCN already has a DRG if you're using an IPSec VPN or an Oracle Cloud Infrastructure FastConnect private virtual circuit.

• A remote peering connection (RPC) on each DRG in the peering relationship.

• A connection between those two RPCs.

• Supporting route rules to enable traffic to flow over the connection, and only to and from select subnets in the respective VCNs (if desired).

• Supporting security rules to control the types of traffic allowed to and from the instances in the subnets that need to communicate with the other VCN.

The following diagram illustrates the components.
**Spoke-to-Spoke: Remote Peering with Transit Routing**

Imagine that in each region you have multiple VCNs in a hub-and-spoke layout, as shown in the following diagram. This type of layout within a region is discussed in detail in [Transit Routing: Access to Multiple VCNs in the Same Region](#) on page 2780. The spoke VCNs in a given region are locally peered with the hub VCN in the same region, using local peering gateways.

You can set up remote peering between the two hub VCNs. You can then also set up transit routing for the hub VCN's DRG and LPGs, as discussed in [Transit Routing: Access to Multiple VCNs in the Same Region](#) on page 2780. This setup allows a spoke VCN in one region to communicate with one or more spoke VCNs in the other region without needing a remote peering connection directly between those VCNs.

For example, you could configure routing so that resources in VCN-1-A could communicate with resources in VCN-2-A and VCN-2-B by way of the hub VCNs. That way, VCN 1-A is not required to have a separate remote peering with each of the spoke VCNs in the other region. You could also set up routing so that VCN-1-B could communicate with the spoke VCNs in region 2, without needing its own remote peerings to them.

---

**Explicit Agreement Required from Both Sides**

Peering involves two VCNs in the same tenancy that might be administered by the same party or two different ones. The two parties might both be in your company but in different departments.

Peering between two VCNs requires explicit agreement from both parties in the form of Oracle Cloud Infrastructure Identity and Access Management policies that each party implements for their own VCN's compartment.
Important Remote Peering Concepts

The following concepts help you understand the basics of VCN peering and how to establish a remote peering.

**PEERING**

A peering is a single peering relationship between two VCNs. Example: If VCN-1 peers with two other VCNs, then there are two peerings. The remote part of remote peering indicates that the VCNs are in different regions. For remote peering, the VCNs must be in the same tenancy.

**VCN ADMINISTRATORS**

In general, VCN peering can occur only if both of the VCN administrators agree to it. In practice, this means that the two administrators must:

- Share some basic information with each other.
- Coordinate to set up the required Oracle Cloud Infrastructure Identity and Access Management policies to enable the peering.
- Configure their VCNs for the peering.

Depending on the situation, a single administrator might be responsible for both VCNs and the related policies. The VCNs must be in the same tenancy.

For more information about the required policies and VCN configuration, see Setting Up a Remote Peering on page 3284.

**ACCEPTOR AND REQUESTOR**

To implement the IAM policies required for peering, the two VCN administrators must designate one administrator as the requestor and the other as the acceptor. The requestor must be the one to initiate the request to connect the two RPCs. In turn, the acceptor must create a particular IAM policy that gives the requestor permission to connect to RPCs in the acceptor's compartment. Without that policy, the requestor's request to connect fails.

**REGION SUBSCRIPTION**

To peer with a VCN in another region, your tenancy must first be subscribed to that region. For information about subscribing, see Managing Regions on page 2445.

**REMOTE PEERING CONNECTION (RPC)**

A remote peering connection (RPC) is a component you create on the DRG attached to your VCN. The RPC's job is to act as a connection point for a remotely peered VCN. As part of configuring the VCNs, each administrator must create an RPC for the DRG on their VCN. A given DRG must have a separate RPC for each remote peering it establishes for the VCN (maximum 10 RPCs per tenancy). To continue with the previous example: the DRG on VCN-1 would have two RPCs to peer with two other VCNs. In the API, a RemotePeeringConnection is an object that contains information about the peering. You can't reuse an RPC to later establish another peering with it.

**CONNECTION BETWEEN TWO RPCS**

When the requestor initiates the request to peer (in the Console or API), they're effectively asking to connect the two RPCs. This means the requestor must have information to identify each RPC (such as the RPC's region and OCID).

Either VCN administrator can terminate a peering by deleting their RPC. In that case, the other RPC's status switches to REVOKED. The administrator could instead render the connection non-functional by removing the route rules that enable traffic to flow across the connection (see the next section).

**ROUTING TO THE DRG**

As part of configuring the VCNs, each administrator must update the VCN's routing to enable traffic to flow between the VCNs. For each subnet that needs to communicate with the other VCN, you update the subnet's route table. The route rule specifies the destination traffic's CIDR and your DRG as the target. Your DRG routes traffic that matches that rule to the other DRG, which in turn routes the traffic to the next hop in the other VCN.
In the following diagram, VCN-1 and VCN-2 are peered. Traffic from an instance in Subnet A (10.0.0.15) that is destined for an instance in VCN-2 (192.168.0.15) is routed to DRG-1 based on the rule in Subnet A's route table. From there the traffic is routed through the RPCs to DRG-2, and then from there, on to the destination in Subnet X.

Note:
As mentioned earlier, a given VCN can use the connected RPCs to reach only VNICs in the other VCN, and not destinations outside of the VCNs (such as the internet or your on-premises network). For example, in the preceding diagram, VCN-2 cannot use the internet gateway attached to VCN-1.

SECURITY RULES
Each subnet in a VCN has one or more security lists that control traffic in and out of the subnet's VNICs at the packet level. You can use security lists to control the type of traffic allowed with the other VCN. As part of configuring the VCNs, each administrator must determine which subnets in their own VCN need to communicate with VNICs in the other VCN and update their subnet's security lists accordingly.

If you use network security groups (NSGs) to implement security rules, notice that you have the option to write security rules for an NSG that specify another NSG as the source or destination of traffic. However, the two NSGs must belong to the same VCN.
Important Implications of Peering

If you haven't yet, read Important Implications of Peering on page 3265 to understand important access control, security, and performance implications for peered VCNs.

Setting Up a Remote Peering

This section covers the general process for setting up a peering between two VCNs in different regions.

Important:

The following procedure assumes that:

- Your tenancy is subscribed to the other VCN's region. If it's not, see Managing Regions on page 2445.
- You already have a DRG attached to your VCN. If you don't, see Dynamic Routing Gateways (DRGs) on page 2927.

1. Create the RPCs: Each VCN administrator creates an RPC for their own VCN's DRG.
2. Share information: The administrators share the basic required information.
3. Set up the required IAM policies for the connection: The administrators set up IAM policies to enable the connection to be established.
4. Establish the connection: The requestor connects the two RPCs (see Important Remote Peering Concepts on page 3282 for the definition of the requestor and acceptor).
5. Update route tables: Each administrator updates their VCN's route tables to enable traffic between the peered VCNs as desired.
6. Update security rules: Each administrator updates their VCN's security rules to enable traffic between the peered VCNs as desired.

If desired, the administrators can perform tasks E and F before establishing the connection. Each administrator needs to know the CIDR block or specific subnets from the other's VCN and share that in task B.

Task A: Create the RPCs

Each administrator creates an RPC for their own VCN's DRG. "You" in the following procedure means an administrator (either the acceptor or requestor).

Note:

Required IAM Policy to Create RPCs

If the administrators already have broad network administrator permissions (see Let network admins manage a cloud network on page 2143), then they have permission to create, update, and delete RPCs. Otherwise, here's an example policy giving the necessary permissions to a group called RPCAdmins. The second statement is required because creating an RPC affects the DRG it belongs to, so the administrator must have permission to manage DRGs.

Allow group RPCAdmins to manage remote-peering-connections in tenancy
Allow group RPCAdmins to manage drgs in tenancy

1. In the Console, confirm you're viewing the compartment that contains the DRG that you want to add the RPC to. For information about compartments and access control, see Access Control on page 2831.
2. Open the navigation menu. Under Core Infrastructure, go to Networking and click Dynamic Routing Gateways.
3. Click the DRG you're interested in.
5. Click Create Remote Peering Connection.
6. Enter the following:
   - **Name**: A friendly name for the RPC. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   - **Create in compartment**: The compartment where you want to create the RPC, if different from the compartment you're currently working in.

7. Click **Create Remote Peering Connection**.

   The RPC is then created and displayed on the **Remote Peering Connections** page in the compartment you chose.

8. If you're the acceptor, record the RPC's region and OCID to later give to the requestor.

**Task B: Share information**

- If you're the acceptor, give this information to the requestor (for example, by email or other out-of-band method):
  - The region your VCN is in (the requestor's tenancy must be subscribed to this region).
  - Your RPC's OCID.
  - The CIDR blocks for subnets in your VCN that should be available to the other VCN. The requestor needs this information when setting up routing for the requestor VCN.

- If you're the requestor, give this information to the acceptor:
  - The region your VCN is in (the acceptor's tenancy must be subscribed to this region).
  - The name of the IAM group that should be granted permission to create a connection in the acceptor's compartment (in the example in the next task, the group is RequestorGrp).
  - The CIDR blocks for subnets in your VCN that should be available to the other VCN. The acceptor needs this information when setting up routing for the acceptor VCN.

**Task C: Set up the IAM policies (VCNs in same tenancy)**

Both the requestor and acceptor must ensure the right policies are in place. These consist of:

- **Policy R (implemented by the requestor):**
  
  Allow group RequestorGrp to manage remote-peering-from in compartment RequestorComp

  The requestor is in an IAM group called RequestorGrp. This policy lets anyone in the group initiate a connection from any RPC in the requestor's compartment (RequestorComp). Policy R can be attached to either the tenancy (root compartment) or to RequestorComp. For information about why you would attach it to one versus the other, see **Policy Basics** on page 2137.

- **Policy A (implemented by the acceptor):**
  
  Allow group RequestorGrp to manage remote-peering-to in compartment AcceptorComp

  This policy lets the requestor connect to any RPC in the acceptor's compartment (AcceptorComp). This statement reflects the required agreement from the acceptor for the peering to be established. Policy A can be attached to either the tenancy (root compartment) or to AcceptorComp.
Networking

Both Policy R and Policy A give RequestorGrp access. However, Policy R has a resource-type called remote-peering-from, and Policy A has a resource-type called remote-peering-to. Together, these policies let someone in RequestorGrp establish the connection from an RPC in the requestor's compartment to an RPC in the acceptor's compartment. The API call to actually create the connection specifies which two RPCs.

Tip:
The permission granted by Policy R might already be in place if the requestor has permission in another policy to manage all of the Networking components in RequesterComp. For example, there might be a general Network Admin policy like this: Allow group NetworkAdmin to manage virtual-network-family in compartment RequestorComp. If the requestor is in the NetworkAdmin group, then they already have the required permissions covered in Policy R (the virtual-network-family includes RPCs). And further, if the policy is instead written to cover the entire tenancy (Allow group NetworkAdmin to manage virtual-network-family in tenancy), then the requestor already has all the required permissions in both compartments to establish the connection. In that case, policy A is not required.

Task D: Establish the connection
The requestor must perform this task.

Prerequisite: The requestor must have:
• The region the acceptor's VCN is in (the requestor's tenancy must be subscribed to the region).
• The OCID of the acceptor's RPC.

1. In the Console, view the details for the requestor RPC that you want to connect to the acceptor RPC.
2. Click Establish Connection.
3. Enter the following:
   • Region: The region that contains the acceptor's VCN. The drop-down list includes only those regions that both support remote VCN peering and your tenancy is subscribed to.
   • Remote Peering Connection OCID: The OCID of the acceptor's RPC.
4. Click **Establish Connection**.

The connection is established and the RPC's state changes to PEERED.

**Task E: Configure the route tables**

As mentioned earlier, each administrator can do this task before or after the connection is established.

Prerequisite: Each administrator must have the CIDR block or specific subnets for the other VCN.

For your own VCN:

1. Determine which subnets in your VCN need to communicate with the other VCN.
2. Update the route table for each of those subnets to include a new rule that directs traffic destined for the other VCN to your DRG:
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
   b. Click the VCN you're interested in.
   c. Under **Resources**, click **Route Tables**.
   d. Click the route table you're interested in.
   e. Click **Add Route Rule** and enter the following:
      - **Target Type**: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      - **Destination CIDR Block**: The other VCN's CIDR block. If you want, you can specify a subnet or particular subset of the peered VCN's CIDR.
      - **Description**: An optional description of the rule.
   f. Click **Add Route Rule**.

Any subnet traffic with a destination that matches the rule is routed to your DRG. For more information about setting up route rules, see **Route Tables** on page 2921.

**Tip:**

Without the required routing, traffic doesn't flow between the peered DRGs. If a situation occurs where you need to temporarily stop the peering, you can simply remove the route rules that enable traffic. You don't need to delete the RPCs.

**Task F: Configure the security rules**

As mentioned earlier, each administrator can do this task before or after the connection is established.

Prerequisite: Each administrator must have the CIDR block or specific subnets for the other VCN. In general, you should use the same CIDR block you used in the route table rule in **Task E: Configure the route tables** on page 3287.

What rules should you add?

- Ingress rules for the types of traffic you want to allow from the other VCN, specifically from the VCN's CIDR or specific subnets.
- Egress rule to allow outgoing traffic from your VCN to the other VCN. If the subnet already has a broad egress rule for all types of protocols to all destinations (0.0.0.0/0), then you don't need to add a special one for the other VCN.

**Note:**

The following procedure uses security lists, but you could instead implement the security rules in a network security group and then create all of the subnet's resources in that NSG.

For your own VCN:

1. Determine which subnets in your VCN need to communicate with the other VCN.
2. Update the security list for each of those subnets to include rules to allow the desired egress or ingress traffic specifically with the CIDR block or subnet of the other VCN:
   a. In the Console, while viewing the VCN you're interested in, click **Security Lists**.
   b. Click the security list you're interested in.
   c. Under **Resources**, click either **Ingress Rules** or **Egress Rules** depending on the type of rule you want to work with.
   d. If you want to add a new rule, click **Add Ingress Rule** (or **Add Egress Rule**).
   e. If you want to delete an existing rule, click the Actions icon (three dots), and then click **Remove**.
   f. If you wanted to edit an existing rule, click the Actions icon (three dots), and then click **Edit**.

For more information about security rules, see **Security Rules** on page 2833.

Example

Let's say you want to add a stateful rule that enables ingress HTTPS (port 443) traffic from the other VCN's CIDR. Here are the basic steps you take when adding a rule:

1. In the **Allow Rules for Ingress** section, click **+Add Rule**.
2. Leave the **Stateless** checkbox unchecked.
3. **Source Type:** Leave as CIDR.
4. **Source CIDR:** Enter the same CIDR block that the route rules use (see Task E: Configure the route tables on page 3287).
5. **IP Protocol:** Leave as TCP.
6. **Source Port Range:** Leave as All.
7. **Destination Port Range:** Enter 443.
8. **Description:** An optional description of the rule.

**Using the Console**

*To create a remote peering connection*

See the instructions in Task A: Create the RPCs on page 3284.

*To delete a remote peering connection*

Deleting an RPC terminates the peering. The RPC at the other side of the peering changes to the REVOKED state.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Dynamic Routing Gateways**.
2. Click the DRG you're interested in.
4. Click the RPC you're interested in.
5. Click **Terminate**.
6. Confirm when prompted.

**Note:**

After deleting an RPC (and thus terminating a peering), it's recommended you review your route tables and security rules to remove any rules that enabled traffic with the other VCN.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To manage your RPCs and create connections, use these operations:

- **ListAllowedPeerRegionsForRemotePeering**
- **ListRemotePeeringConnections**
- **CreateRemotePeeringConnection**
Access to Oracle Cloud Infrastructure Classic

There are two ways to set up a connection between an Oracle Cloud Infrastructure Classic IP network and an Oracle Cloud Infrastructure virtual cloud network (VCN):

- **Option 1: Connection over the Oracle network**
  - You file a ticket with My Oracle Support and Oracle provisions a connection between the IP network's private gateway and the VCN's attached dynamic routing gateway (DRG). The connection runs over Oracle's network and not the internet.
  - The two environments must be in the same geographical area, and the connection is available only between the specific regions listed in Overview on page 3289.
  - The two environments must belong to the same company. Oracle validates ownership when setting up the connection.

- **Option 2: Connection over an IPSec VPN**
  - You set up an IPSec VPN between the IP network's VPN as a Service (VPNaaS) gateway and the VCN's attached DRG. The connection runs over the internet.
  - The two environments do not have to be in the same geographical area or regions.
  - The two environments do not have to belong to the same company.

Connection Over Oracle Network

This topic describes one way to set up a connection between an Oracle Cloud Infrastructure Classic IP network and an Oracle Cloud Infrastructure virtual cloud network (VCN). The connection runs over Oracle's network.

Another option is to connect the two clouds with an IPSec VPN. For more information, see Connection Over IPSec VPN on page 3294.

Highlights

- You can run a hybrid workload between your Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure environments.
- Oracle connects the IP network's private gateway to the VCN's attached dynamic routing gateway (DRG). The connection runs over the Oracle network. You configure routing and security rules in the environments to enable traffic.
- The two environments must belong to the same company and not have overlapping CIDRs. The cloud resources can communicate over the connection only with private IP addresses.
- The two environments must both be in the Ashburn area, the London area, or the Sydney area, and in specific regions listed in the next section. Connectivity to other regions is not supported.
- The connection is free of charge.

Overview

You can request Oracle to provision a connection between your Oracle Cloud Infrastructure environment and your Oracle Cloud Infrastructure Classic environment. The connection facilitates a hybrid deployment with application components that are set up across the two environments. You can also use the connection to migrate workloads from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. Compared to an IPSec VPN: the resources in the two environments have a more reliable and consistent network connection, with better throughput, because the traffic uses Oracle's internal links. Compared to FastConnect: you don't incur the additional cost and operational overhead of working with a FastConnect partner.

The following diagram shows an example of a hybrid deployment. Oracle Analytics Cloud is running in an Oracle Cloud Infrastructure Classic IP network and accessing the Database service in Oracle Cloud Infrastructure over the connection.
Here are other important details to know:

- The connection is supported only between these regions:
  - Oracle Cloud Infrastructure Australia East (Sydney) region and the Sydney Classic region
  - Oracle Cloud Infrastructure US East (Ashburn) region and the Ashburn Classic region
  - Oracle Cloud Infrastructure UK South (London) region and the Slough Classic region
- The connection enables communication that uses private IP addresses only.
- The CIDR blocks of the IP network and VCN subnets that need to communicate must not overlap.
- The IP network and VCN must belong to the same company. Oracle validates this when setting up the connection.
- This connection enables communication only between resources in the Oracle Cloud Infrastructure Classic IP network and Oracle Cloud Infrastructure VCN. It does not enable traffic between your on-premises network through the IP network to the VCN, or from your on-premises network through the VCN to the IP network.
- The connection also does not enable traffic to flow from the IP network through the connected VCN to a peered VCN in the same Oracle Cloud Infrastructure region, or a different region.

The following table lists the comparable networking components required on each side of the connection.

<table>
<thead>
<tr>
<th>Component</th>
<th>Oracle Cloud Infrastructure Classic</th>
<th>Oracle Cloud Infrastructure VCN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud network</td>
<td>IP network</td>
<td>VCN</td>
</tr>
</tbody>
</table>
### Component | Oracle Cloud Infrastructure Classic | Oracle Cloud Infrastructure
--- | --- | ---
Gateway | private gateway | dynamic routing gateway (DRG)
Routing | routes | route tables with route rules
Security rules | security rules | network security groups, security lists

## Connecting Your IP Network and VCN

The following flow chart shows the overall process of connecting your IP network and VCN.

### Prerequisites:

You must already have:

- An Oracle Cloud Infrastructure Classic IP network.
- An Oracle Cloud Infrastructure VCN with subnets.

**Task 1: Set up a private gateway for your IP network**

If you do not already have a private gateway for your IP network, create one.
Task 2: Set up a dynamic routing gateway (DRG) for your VCN

If you do not already have a DRG attached to your VCN, create a DRG and attach it:

- To create a DRG on page 2929
- To attach a DRG to a VCN on page 2930

Task 3: Configure route tables

For the IP network

When you create the private gateway and attach an IP network to it, traffic from cloud resources in the IP network uses the private gateway as the next hop. You do not need to update any routes for the IP network.

For the VCN

You must add a route rule that directs traffic from the VCN's subnets to the DRG:

1. Determine which subnets in your VCN need to communicate with the IP network.
2. Update the route table for each of those subnets to include a new rule that directs traffic destined for the IP network's CIDR to your DRG:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click the VCN you're interested in.
   c. Under Resources, click Route Tables.
   d. Click the route table you're interested in.
   e. Click Add Route Rule and enter the following:
      - Destination CIDR Block: The IP network's CIDR block.
      - Target Type: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      - Description: An optional description of the rule.
   f. Click Add Route Rule.

Any subnet traffic with a destination that matches the rule is routed to your DRG. For more information about setting up route rules, see Route Tables on page 2921.

Later, if you no longer need the connection and want to delete your DRG, you must first delete all the route rules in your VCN that specify the DRG as the target.

Task 4: Configure the security rules

To ensure traffic flows between the IP network and VCN, the IP network security rules and the VCN's security rules must be set to allow traffic.

Here are the types of rules to add:

- Ingress rules for the types of traffic you want to allow into one cloud from the other, specifically from the other cloud's CIDR block.
- Egress rule to allow outgoing traffic from one cloud to the other. If the VCN's subnet already has a broad egress rule for all types of protocols to all destinations (0.0.0.0/0), then you don't need to add a special one for the IP network.

For the IP network

Configure the network security rules for the IP network to allow traffic.

For the VCN

Note:

The following procedure uses security lists, but you could instead implement the security rules in one or more network security groups and then place the VCN's resources in NSGs.
1. Determine which subnets in your VCN need to communicate with the IP network.
2. Update the security list for each of those subnets to include rules to allow egress or ingress traffic specifically with the CIDR block of the IP network:
   a. In the Console, while viewing the VCN you're interested in, click Security Lists.
   b. Click the security list you're interested in.

   Under Resources, you can click Ingress Rules or Egress Rules to switch between the different types of rules.
   c. Add one or more rules, each for the specific type of traffic you want to allow.

For more information about setting up security rules, see Security Rules on page 2833.

### Important:

The VCN's default security list does not allow ICMP echo reply and echo request (ping). You must add rules to enable that traffic. See Rules to Enable Ping on page 2841

Example:

Let's say you want to add a stateful rule that enables ingress HTTPS (port 443) traffic from the IP network's CIDR. Here are the basic steps you take when adding a rule:

1. On the **Ingress Rules** page, click **Add Ingress Rule**.
2. Leave the **Stateless** check box unselected.
3. **Source CIDR**: Enter the same CIDR block that the route rules use (see Task 3: Configure route tables on page 3292).
4. **IP Protocol**: Leave as TCP.
5. **Source Port Range**: Leave as All.
6. **Destination Port Range**: Enter 443.
7. **Description**: Optionally enter a description of the rule.
8. Click **Add Ingress Rule**.

### Task 5: Create a My Oracle Support ticket

To have Oracle set up the connection, create a ticket at My Oracle Support and provide the following information:

- Ticket name: Create IP Network - VCN Connection - `<your_company_name>` - Ashburn
- OCI-C identity domain
- OCI-C private gateway name
- Region
- OCI tenancy OCID
- OCI DRG OCID

For example:

- Ticket name: Create IP Network - VCN Connection - ACME - Ashburn
- OCI-C identity domain: 123456789, uscom-east-1
- OCI-C private gateway name: Compute-acme/jack.jones@example.com/privategateway1
- Region: uscom-east-1 (OCI-C) / us-ashburn-1 (OCI)
- OCI tenancy OCID: ocid1.tenancy.oc1..examplefbpnk5cmdl7gkr6kcakfqmvhvbpcv
- OCI DRG OCID: ocid1.drg.oc1.iad.exampleutg6cmd3fqwqbea7ctadcatm

It can take three to four business days before your My Oracle Support ticket is complete and the connection is ready to test.

### Task 6: Test the connection

After you receive confirmation from your support person that the connection is ready, test the connection. Depending on how you've set up your IP network's security rules and VCN security rules, you should be able to launch an
instance in your VCN and access it from an instance in the IP network. Or you should be able to connect from the VCN instance to an instance in the IP network. If you can, your connection is ready to use.

**Terminating the Connection**

If you want to terminate the connection, file a ticket at My Oracle Support.

**Connection Over IPSec VPN**

This topic describes one way to set up a connection between an Oracle Cloud Infrastructure Classic IP network and an Oracle Cloud Infrastructure virtual cloud network (VCN). The connection runs over an IPSec VPN.

Another option is to have Oracle set up a connection over the Oracle network. For more information, see Connection Over Oracle Network on page 3289.

**Highlights**

- You can run a hybrid workload between your Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure environments.
- You set up an IPSec VPN between the IP network's VPN as a Service (VPNaas) gateway and the VCN's attached dynamic routing gateway (DRG). The connection runs over the internet. You configure routing and security rules in the environments to enable traffic.
- The two environments must not have overlapping CIDRs. The cloud resources can communicate over the connection only with private IP addresses.
- The two environments do not have to be in the same geographical area or region.
- The connection is free of charge.

**Overview**

You can connect your Oracle Cloud Infrastructure environment and your Oracle Cloud Infrastructure Classic environment with an IPSec VPN. The connection facilitates a hybrid deployment with application components that are set up across the two environments. You can also use the connection to migrate workloads from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. Compared to using the Oracle network for the connection: you can set up the IPSec VPN yourself in a matter of minutes. Compared to FastConnect: you don't incur the additional cost and operational overhead of working with a FastConnect partner.

The following diagram shows an example of a hybrid deployment. Oracle Analytics Cloud is running in an Oracle Cloud Infrastructure Classic IP network and accessing the Database service in Oracle Cloud Infrastructure over the connection.
Here are other important details to know:

- The connection is supported in any of the Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic regions. The two environments do not need to be in the same geographical area.
- The connection enables communication that uses private IP addresses only.
- The CIDR blocks of the IP network and VCN subnets that need to communicate must not overlap.
- This connection enables communication only between resources in the Oracle Cloud Infrastructure Classic IP network and Oracle Cloud Infrastructure VCN. It does not enable traffic between your on-premises network through the IP network to the VCN, or from your on-premises network through the VCN to the IP network.
- The connection also does not enable traffic to flow from the IP network through the connected VCN to a peered VCN in the same Oracle Cloud Infrastructure region, or a different region.

The following table lists the comparable networking components required on each side of the connection.

<table>
<thead>
<tr>
<th>Component</th>
<th>Oracle Cloud Infrastructure Classic</th>
<th>Oracle Cloud Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud network</td>
<td>IP network</td>
<td>VCN</td>
</tr>
<tr>
<td>Gateway</td>
<td>VPNaaS gateway</td>
<td>dynamic routing gateway (DRG)</td>
</tr>
<tr>
<td>Security rules</td>
<td>security rules</td>
<td>network security groups, security lists</td>
</tr>
</tbody>
</table>
Setting Up the IPSec VPN Between Your IP Network and VCN

The following flow chart shows the overall process of connecting your IP network and VCN with an IPSec VPN.

Prerequisites:

You must already have:

• An Oracle Cloud Infrastructure Classic IP network.
• An Oracle Cloud Infrastructure VCN with subnets.
**Task 1: Set up a VPNaaS gateway for your IP network**

1. Use these values when setting up the VPNaaS gateway:
   - **IP Network**: The Oracle Cloud Infrastructure Classic IP network you want to connect to your VCN. You can only specify a single IP network.
   - **Customer Gateway**: A placeholder value such as 129.213.240.51. Using this placeholder value lets you move forward in the process. You update the value later with the Oracle Cloud Infrastructure VPN router’s IP address.
   - **Customer Reachable Routes**: The CIDR block for the VCN. You can specify only a single VCN.
   - **Specify Phase 2 ESP Proposal**: Check box selected.
   - **ESP Encryption**: AES 256
   - **ESP Hash**: SHA1
   - **IPSec Lifetime**: 1800
   - **Require Perfect Forward Secrecy**: Check box selected.

2. Record the resulting public IP address of the VPNaaS gateway.

**Task 2: Set up the VCN's components and IPSec tunnel**

**Task 2a: Set up a dynamic routing gateway (DRG) for your VCN**

If you do not already have a DRG attached to your VCN, create a DRG and attach it:
   - To create a DRG on page 2929
   - To attach a DRG to a VCN on page 2930

**Task 2b: Configure routing to the DRG**

Add a route rule that directs traffic from the VCN's subnets to the DRG. Use the IP network's CIDR block as the destination for the rule.

1. Determine which subnets in your VCN need to communicate with the IP network.
2. Update the route table for each of those subnets to include a new rule that directs traffic destined for the IP network's CIDR to your DRG:
   a. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
   b. Click the VCN you're interested in.
   c. Under **Resources**, click **Route Tables**.
   d. Click the route table you're interested in.
   e. Click **Add Route Rule** and enter the following:
      - **Destination CIDR Block**: The IP network's CIDR block.
      - **Target Type**: Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      - **Description**: An optional description of the rule.
   f. Click **Add Route Rule**.

Any subnet traffic with a destination that matches the rule is routed to your DRG. For more information about setting up route rules, see **Route Tables** on page 2921.

Later, if you no longer need the connection and want to delete your DRG, you must first delete all the route rules in your VCN that specify the DRG as the target.

**Task 2c: Configure the security rules**

To ensure traffic flows between the IP network and VCN, set the IP network security rules and the VCN's security rules to allow the wanted traffic.

Here are the types of rules to add:
   - Ingress rules for the types of traffic you want to allow into one cloud from the other, specifically from the other cloud's CIDR block.
Networking

- Egress rule to allow outgoing traffic from one cloud to the other. If the VCN's subnet already has a broad egress rule for all types of protocols to all destinations (0.0.0.0/0), then you don't need to add a special one for the IP network.

For the IP network

Configure the network security rules for the IP network to allow the wanted traffic.

For the VCN

Note:
The following procedure uses security lists, but you could instead implement the security rules in one or more network security groups and then place the VCN's resources in NSGs.

1. Determine which subnets in your VCN need to communicate with the IP network.
2. Update the security list for each of those subnets to include rules to allow the wanted egress or ingress traffic specifically with the CIDR block of the IP network:
   a. In the Console, while viewing the VCN you're interested in, click Security Lists.
   b. Click the security list you're interested in.
      Under Resources, you can click Ingress Rules or Egress Rules to switch between the different types of rules.
   c. Add one or more rules, each for the specific type of traffic you want to allow.

   For more information about setting up security list rules, see Security Lists on page 2850.

Important:
The VCN's default security list does not allow ICMP echo reply and echo request (ping). Add rules to enable that traffic. See Rules to Enable Ping on page 2841

Example

Let's say you want to add a stateful rule that enables ingress HTTPS (port 443) traffic from the IP network's CIDR. Here are the basic steps you take when adding a rule:

2. Leave the Stateless check box unselected.
3. Source CIDR: Enter the same CIDR block that the route rules use (see Task 2b: Configure routing to the DRG on page 3297).
4. IP Protocol: Leave as TCP.
5. Source Port Range: Leave as All.
6. Destination Port Range: Enter 443.
7. Click Add Ingress Rule.
8. Description: Optionally enter a description of the rule.

Task 2d: Create a CPE object

Create a CPE object. An IP address is required. Use the VPNaaS gateway's public IP address.

Task 2e: Create the IPSec connection

From your DRG, create an IPSec connection to the CPE object. You must provide one or more static routes. The values must match the IP network's subnets or aggregate.

The resulting IPSec connection consists of two tunnels. Record the IP address and shared secret for one of those tunnels. In the next task, you will provide those values.

Task 3: Update the VPNaaS connection with the tunnel information

Update the VPNaaS connection. Use these values:
• **Customer Gateway:** The tunnel's IP address from the preceding task.

• **VPNaaS VPN Connection’s Pre-shared Key:** The tunnel's shared secret from the preceding task.

After the VPNaaS connection is updated and provisioned, the state of your VCN's IPSec tunnel should change to Available. Provisioning might take a few minutes.

**Task 4: Test the connection**

After the tunnel state changes to Available, test the connection. Depending on how you've set up your IP network's security rules and VCN security rules, you should be able to **launch an instance** in your VCN and access it from an instance in the IP network. Or you should be able to connect from the VCN instance to an instance in the IP network. If you can, your connection is ready to use.

**Terminating the Connection**

If you want to terminate the connection, delete the IPSec connection:

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **VPN Connections**.

   A list of the IPSec connections in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. Click the IPSec connection you're interested in.

3. Click **Terminate**.

4. Confirm the deletion when prompted.

The IPSec connection will be in the Terminating state for a short period while it's being deleted.

**Access to Microsoft Azure**

Oracle and Microsoft have created a cross-cloud connection between Oracle Cloud Infrastructure and Microsoft Azure in certain regions. This connection lets you set up cross-cloud workloads without the traffic between the clouds going over the internet. This topic describes how to set up virtual networking infrastructure resources to enable this kind of cross-cloud deployment.

**Highlights**

• You can connect a Microsoft Azure virtual network (VNet) with an Oracle Cloud Infrastructure virtual cloud network (VCN) and run a cross-cloud workload. In the typical use case, you deploy your Oracle Database on Oracle Cloud Infrastructure, and deploy an Oracle, .NET, or custom application in Microsoft Azure.

• The two virtual networks must belong to the same company and not have overlapping CIDRs. The connection requires you to create an Azure ExpressRoute circuit and an Oracle Cloud Infrastructure FastConnect virtual circuit.

• Currently, the connection is only available in these areas:

  • Between the Oracle Cloud Infrastructure location in the US East (Ashburn) region and the **Azure Washington DC and Washington DC2 locations**.
  
  • Between the Oracle Cloud Infrastructure location in the UK South (London) region and the **Azure London location**.
  
  • Between the Oracle Cloud Infrastructure location in the Canada Southeast (Toronto) region and the **Azure Canada Central location**.
  
  • Between the Oracle Cloud Infrastructure location in the Netherlands Northwest (Amsterdam) region and the **Azure Amsterdam2 location**.
  
  • Between the Oracle Cloud Infrastructure location in the Japan East (Tokyo) region and the **Azure Tokyo location**.
  
  • Between the Oracle Cloud Infrastructure location in the US West (San Jose) region and the **Azure Silicon Valley location**.

**Overview of Supported Traffic**

Here are more details about the supported types of traffic.
**VNet-to-VCN Connection: Extension from One Cloud to Another**

You can connect your VNet and VCN so that traffic that uses private IP addresses goes over the cross-cloud connection.

For example, the following diagram shows a VNet that is connected to a VCN. Resources in the VNet are running a .NET application that access an Oracle database that runs on Database service resources in the VCN. The traffic between the application and database uses a logical circuit that runs on the cross-cloud connection between Azure and Oracle Cloud Infrastructure.

To enable the connection between the VNet and VCN, you set up an Azure ExpressRoute circuit and an Oracle Cloud Infrastructure FastConnect virtual circuit. The connection has built-in redundancy, which means you need to set up only a single ExpressRoute circuit and single FastConnect virtual circuit. The bandwidth for the connection is the bandwidth value you choose for the ExpressRoute circuit.

For instructions, see [Setting Up a VNet-to-VCN Connection](#) on page 3302.

**Peered VCNs**

The connection enables traffic to flow from the VNet through the connected VCN to a peered VCN in the same Oracle Cloud Infrastructure region, or a different region.
Types of Traffic Not Supported by the Connection

This cross-cloud connection does not enable traffic between your on-premises network through the VCN to the VNet, or from your on-premises network through the VNet to the VCN.

Important Implications of Connecting Clouds

This section summarizes some access control, security, and performance implications of connecting your VCN to a VNet. In general, you can control access and traffic by using IAM policies, route tables in the VCN, and security rules in the VCN.

The sections that follow discuss implications from the perspective of your VCN. Similar implications affect your VNet. As with your VCN, you can use Azure resources such as route tables and network security groups to secure your VNet.

Controlling the Establishment of a Connection

With Oracle Cloud Infrastructure IAM policies, you can control:

- Who in your organization has the authority to create a FastConnect virtual circuit (see Setting Up a VNet-to-VCN Connection on page 3302). Deletion of the relevant IAM policy does not affect any existing connections to a VNet, only the ability for a future connection to be created.
- Who can manage route tables, network security groups, and security lists.

Controlling Traffic Flow Over the Connection

Even if a connection has been established between your VCN and VNet, you can control the packet flow over the connection with route tables in your VCN. For example, you can restrict traffic to only specific subnets in the VNet.

Without terminating the connection, you can stop traffic flow to the VNet by simply removing route rules that direct traffic from your VCN to the VNet. You can also effectively stop the traffic by removing any security rules that enable ingress or egress traffic with the VNet. This doesn't stop traffic flowing over the connection, but stops it at the VNIC level.

Controlling the Specific Types of Traffic Allowed

It's important that you ensure that all outbound and inbound traffic with the VNet is intended or expected and well defined. Implement Azure network security group and Oracle security rules that explicitly state the types of traffic one cloud can send to the other and accept from the other.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your Oracle Cloud Infrastructure instances running Oracle-provided Linux images or Windows images also have firewall rules that control access to the instance. When troubleshooting access to an instance, ensure that the following items are set correctly: the network security groups that the instance is in, the security lists associated with the instance's subnet, and the instance's firewall rules. For more information, see Oracle-Provided Images on page 629.</td>
</tr>
<tr>
<td>If your instance is running Oracle Autonomous Linux 7, Oracle Linux 8, or Oracle Linux 7, you need to use firewalld to interact with the iptables rules. For your reference, here are commands for opening a port (1521 in this example):</td>
</tr>
<tr>
<td>sudo firewall-cmd --zone=public --permanent --add-port=1521/tcp</td>
</tr>
<tr>
<td>sudo firewall-cmd --reload</td>
</tr>
</tbody>
</table>
For instances with an iSCSI boot volume, the preceding `--reload` command can cause problems. For details and a workaround, see Instances experience system hang after running firewall-cmd --reload.

In addition to security rules and firewalls, you should evaluate other OS-based configuration on the instances in your VCN. There could be default configurations that don't apply to your own VCN's CIDR, but inadvertently apply to the VNet's CIDR.

Using Default Security List Rules with Your VCN

If your VCN's subnets use the default security list with the default rules, two rules in that list allow ingress traffic from anywhere (that is, 0.0.0.0/0, and thus the VNet):

- Stateful ingress rule that allows TCP port 22 (SSH) traffic from 0.0.0.0/0 and any source port
- Stateful ingress rule that allows ICMP type 3, code 4 traffic from 0.0.0.0/0 and any source port

Evaluate these rules and whether you want to keep or update them. As stated earlier, you should ensure that all permitted inbound or outbound traffic is intended or expected and well defined.

Preparing for Performance Impact and Security Risks

In general, you should prepare your VCN for the ways it could be affected by the VNet. For example, the load on your VCN or its instances could increase. Or your VCN could experience a malicious attack directly from or by way of the VNet.

Regarding performance: If your VCN is providing a service to the VNet, be prepared to scale up your service to accommodate the demands of the VNet. This might mean being prepared to launch more instances as necessary. Or if you're concerned about high levels of network traffic coming to your VCN, consider using stateless security rules to limit the level of connection tracking your VCN must perform. Stateless security rules can also help slow the impact of a denial-of-service (DoS) attack.

Regarding security risks: If the VNet is connected to the internet, your VCN can be exposed to bounce attacks. A bounce attack involves a malicious host on the internet sending traffic to your VCN that looks like it's coming from the VNet. To guard against this, as mentioned earlier, use your security rules to carefully limit the inbound traffic from the VNet to expected and well-defined traffic.

Setting Up a VNet-to-VCN Connection

This section describes how to set up the logical connection between a VNet and VCN (for background, see Overview of Supported Traffic on page 3299).

Prerequisites: Resources You Need

You must already have:

- An Azure VNet with subnets and virtual network gateway
- An Oracle Cloud Infrastructure VCN with subnets and an attached dynamic routing gateway (DRG). It's easy to forget to attach the DRG to your VCN after you create it. If you already have an IPSec VPN or FastConnect between your on-premises network and VCN, then your VCN already has an attached DRG. You use that same DRG here when setting up the connection to Azure.

As a reminder, here is a table that lists the comparable networking components involved in each side of the connection.

<table>
<thead>
<tr>
<th>Component</th>
<th>Azure</th>
<th>Oracle Cloud Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual network</td>
<td>VNet</td>
<td>VCN</td>
</tr>
<tr>
<td>Virtual circuit</td>
<td>ExpressRoute circuit</td>
<td>FastConnect private virtual circuit</td>
</tr>
<tr>
<td>Gateway</td>
<td>virtual network gateway</td>
<td>dynamic routing gateway (DRG)</td>
</tr>
</tbody>
</table>
**Prerequisites: BGP Information You Need**

The connection between the VNet and VCN uses BGP dynamic routing. When you set up the Oracle virtual circuit, you provide the BGP IP addresses that will be used for the two redundant BGP sessions between Oracle and Azure:

- A primary pair of BGP addresses (one IP address for the Oracle side, one IP address for the Azure side)
- A separate, secondary pair of BGP addresses (one IP address for the Oracle side, one IP address for the Azure side)

**For each pair, you must provide a separate /30 block of addresses** (each /30 has four IP addresses).

The second and third addresses in each /30 are used for the BGP IP address pair. Specifically:

- The second address in the block is for the Oracle side of the BGP session
- The third address in the block is for the Azure side of the BGP session

The first and last addresses in the block are used for other internal purposes.

For example, if the /30 is 10.0.0.20/30, then the addresses in the block are:

- 10.0.0.20
- 10.0.0.21: Use this for the Oracle side (in the Oracle Console, enter the address as 10.0.0.21/30)
- 10.0.0.22: Use this for the Azure side (in the Oracle Console, enter the address as 10.0.0.22/30, and notice that this address is referred to as the "Customer" side in the Console)
- 10.0.0.23

Remember that you must also provide a /30 block for the secondary BGP addresses. For example: 10.0.0.24/30. In this case, 10.0.0.25 is for the Oracle side, and 10.0.0.26 is for the Azure side. In the Oracle Console, you must enter these as 10.0.0.25/30 and 10.0.0.26/30.

**Prerequisites: Required IAM Policy**

It's assumed that you have the necessary Azure Active Directory access and Oracle Cloud Infrastructure IAM access to create and work with the relevant Azure and Oracle networking resources. Specifically for IAM: If your user is in the Administrators group, you have the required authority.

If your user is not, then a policy like this one generally covers all the Networking resources:

```yaml
Allow group NetworkAdmins to manage virtual-network-family in tenancy
```

To only create and manage a virtual circuit, you must have a policy like this:

```yaml
Allow group VirtualCircuitAdmins to manage drgs in tenancy
Allow group VirtualCircuitAdmins to manage virtual-circuits in tenancy
```

For more information, see [IAM Policies for Networking](#) on page 232.
Overall Process

The following flow chart shows the overall process of connecting your VNet and VCN.

1. Configure VNet's security groups and VCN's security lists
2. Set up Azure ExpressRoute circuit
3. Confirm both circuits are provisioned
4. Configure routing for VNet and VCN

Task 1: Configure the network security groups and security rules

The first task is to determine what traffic needs to flow between the relevant subnets within the VNet and VCN, and then configure the VNet security groups and VCN security rules accordingly. Here are the general types of rules to add:

- Ingress rules for the types of traffic you want to allow into one cloud from the other, specifically from the other cloud's relevant subnets.
- Egress rule to allow outgoing traffic from one cloud to the other. If the VCN's subnet already has a broad egress rule for all types of protocols to all destinations (0.0.0.0/0), then you don't need to add a special one for the traffic to the VNet. The VCN's default security list includes a broad default egress rule like this.

More specifically, here are recommended types of traffic to allow between the VNet and VCN:

- Ping traffic in both directions for testing the connection from each side
- SSH (TCP port 22)
- Client connections to an Oracle database (SQL*NET on TCP port 1521)

Only allow traffic to and from specific address ranges of interest (for example, the other cloud's relevant subnets).
For the VNet: Determine which subnets in your VNet need to communicate with the VCN. Then configure the network security groups for those subnets to allow traffic.

For the VCN:

**Note:**
The following procedure uses security lists, but you could instead implement the security rules in one or more network security groups and then place the VCN's relevant resources in NSGs.

1. Determine which subnets in your VCN need to communicate with the VNet.
2. Update the security list for each of those subnets to include rules to allow egress or ingress traffic specifically with the VNet's CIDR block or a subnet of the VNet:
   a. In the Console, while viewing the VCN you're interested in, click **Security Lists**.
   b. Click the security list you're interested in.
   c. Click **Edit All Rules** and create one or more rules, each for the specific type of traffic you want to allow.
   d. Click **Save Security List Rules** at the bottom of the dialog box.

For more information about setting up security rules, see Security Rules on page 2833.

**Example: Outgoing ping from VCN to VNet**
The following egress security rule lets an instance initiate a ping request to a host outside the VCN (echo request ICMP type 8). This is a stateful rule that automatically allows the response. No separate ingress rule for echo reply ICMP type 0 is required.

1. In the **Allow Rules for Egress** section, click **+Add Rule**.
2. Leave the **Stateless** check box unselected.
3. **Destination CIDR**: The relevant subnet in the VNet (10.0.0.0/16 in the preceding diagram)
4. **IP Protocol**: ICMP
5. **Type and Code**: 8
6. **Description**: An optional description of the rule.

**Example: Incoming ping to VCN from VNet**
The following ingress security rule lets an instance receive a ping request from a host in the VNet (echo request ICMP type 8). This is a stateful rule that automatically allows the response. No separate egress rule for echo reply ICMP type 0 is required.

1. In the **Allow Rules for Ingress** section, click **+Add Rule**.
2. Leave the **Stateless** check box unselected.
3. **Source CIDR**: The relevant subnet in the VNet (10.0.0.0/16 in the preceding diagram)
4. **IP Protocol**: ICMP
5. **Type and Code**: 8
6. **Description**: An optional description of the rule.

**Example: Incoming SSH to VCN**
The following ingress security rule lets an instance receive an SSH connection (TCP port 22) from a host in the VNet.

1. In the **Allow Rules for Ingress** section, click **+Add Rule**.
2. Leave the **Stateless** check box unselected.
3. **Source CIDR**: The relevant subnet in the VNet (10.0.0.0/16 in the preceding diagram)
4. **IP Protocol**: TCP
5. **Source Port Range**: All
6. **Destination Port Range**: 22
7. **Description**: An optional description of the rule.
**Example: SQL*Net connections to database**

The following ingress security rule allows SQL*Net connections (TCP port 1521) from hosts in the VNet.

1. In the **Allow Rules for Ingress** section, click **+Add Rule**.
2. Leave the **Stateless** check box unselected.
3. **Source CIDR**: The relevant subnet in the VNet (10.0.0.0/16 in the preceding diagram)
4. **IP Protocol**: TCP
5. **Source Port Range**: All
6. **Destination Port Range**: 1521
7. **Description**: An optional description of the rule.

**Task 2: Set up Azure ExpressRoute circuit**

Set up an ExpressRoute circuit to Oracle Cloud FastConnect. During the circuit setup, you receive a service key from Microsoft. Record that service key, because you must provide it to Oracle in the next task.

In the next task, you set up a FastConnect private virtual circuit to Microsoft Azure: ExpressRoute. When that virtual circuit finishes being provisioned, your ExpressRoute circuit updates to show that private peering is enabled.

**Task 3: Set up an Oracle Cloud Infrastructure FastConnect virtual circuit**

1. In the Console, confirm you're viewing the **compartment** that you want to work in. If you're not sure which one, use the compartment that contains the DRG that you'll connect to. This choice of compartment, along with a corresponding IAM policy, controls who can access the virtual circuit you're about to create.
2. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **FastConnect**. The resulting FastConnect page is where you create a new virtual circuit and later return to when you need to manage the virtual circuit.
3. Click **Create Connection**.
4. Select **FastConnect partner** and choose **Microsoft Azure: ExpressRoute** from the list.
5. Enter the following for your virtual circuit:
   • **Name**: A friendly name of your choice. The value does not need to be unique across your virtual circuits, and you can change it later. Avoid entering confidential information.
   • **Create in Compartment**: Leave as is (the compartment you're currently working in).
   • **Virtual Circuit Type**: Select **Private Virtual Circuit**.
   • **Dynamic Routing Gateway Compartment**: Select the compartment where the DRG resides (it should already be selected).
   • **Dynamic Routing Gateway**: Select the DRG.
   • **Provisioned Bandwidth**: Choose the same bandwidth level you chose for the ExpressRoute circuit (or the closest value available).
   • **Provider Service Key**: Enter the key you received from Microsoft when you set up the ExpressRoute circuit.
   • **Customer Primary BGP IP Address**: This field is the Azure primary BGP IP address. Enter the third address in the primary /30 block that you provide, and include /30 at the end. For example: 10.0.0.22/30. For more information about this field and the next ones, see Setting Up a VNet-to-VCN Connection on page 3302.
   • **Oracle Primary BGP IP address (optional)**: You can leave this field blank and Oracle infers the address based on the /30 block you provided for the Azure BGP IP address. In this example, the correct value would be 10.0.0.21/30.
   • **Customer Secondary BGP IP Address**: This field is the Azure secondary BGP IP address. Enter the third address in the secondary /30 block that you provide, and include /30 at the end. For example: 10.0.0.26/30.
   • **Oracle Primary BGP IP Address (optional)**: You can leave this field blank and Oracle infers the address based on the /30 block you provided for the Azure BGP IP address. In this example, the correct value would be 10.0.0.25/30.
6. Click **Continue**.
   The virtual circuit is created.
7. Click **Close**.
After you create the Oracle virtual circuit, you do not need to contact Azure to request provisioning of the circuit. It happens automatically.

**Task 4: Confirm that both circuits are provisioned**

Within a few minutes, both circuits should be provisioned. To verify:

- For the ExpressRoute circuit, confirm that private peering is provisioned.
- For the FastConnect virtual circuit, confirm that its status is UP. See *To get the status of your FastConnect virtual circuit* on page 3307.

**Task 5: Configure the route tables**

**For the VNet:** Determine which subnets in your VNet need to communicate with the VCN. Then configure the route tables for those subnets to route traffic to the VNet gateway.

**For the VCN:**

1. Determine which subnets in your VCN need to communicate with the VNet.
2. Update the route table for each of those subnets to include a new rule that directs traffic destined for the VNet's CIDR to your DRG:
   a. In the Console, while viewing the VCN you're interested in, click *Route Tables*.
   b. Click the route table you're interested in.
   c. Click *Edit Route Rules*.
   d. Click *+ Another Route Rule* and enter the following:
      - **Target Type:** Dynamic Routing Gateway. The VCN's attached DRG is automatically selected as the target, and you don't have to specify the target yourself.
      - **Destination CIDR Block:** The relevant subnet in the VNet (10.0.0.0/16 in the preceding diagram).
      - **Description:** An optional description of the rule.
   e. Click *Save*.

Any subnet traffic with a destination that matches the rule is routed to your DRG. The DRG then knows to route the traffic to the VNet based on the virtual circuit's BGP session information.

Later, if you no longer need the connection and want to delete your DRG, you must first delete all the route rules in your VCN that specify the DRG as the target.

For more information about setting up route rules, see *Route Tables* on page 2921.

**Task 6: Test the connection**

Depending on how you've set up your VNet security groups and VCN security rules, you should be able to create an instance in your VCN and access it from a host in the VNet. Or you should be able to connect from the instance to a host in the VNet. If you can, your connection is ready to use.

**Important:**

If you decide to terminate the connection, you must follow a particular process. See *To terminate the connection to Azure* on page 3309.

**Managing a VNet-to-VCN Connection**

**To get the status of your FastConnect virtual circuit**

1. Open the navigation menu. Under *Core Infrastructure*, go to *Networking* and click *FastConnect*.
2. Select the compartment where the connection resides, and then click the connection you're interested in. If the icon for the virtual circuit is green and says UP, the virtual circuit is provisioned and BGP has been correctly configured. The virtual circuit is ready to use.
To edit a FastConnect virtual circuit

You can change these items for your virtual circuit:

- The name
- Which DRG it uses

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your virtual circuit is in the PROVISIONED state, changing which DRG it uses switches the state to PROVISIONING and may cause the connection to go down. After Oracle reprovisions the virtual circuit, its state returns to PROVISIONED. Confirm that the connection is back up and working.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
2. Select the compartment where the connection resides, and then click the connection.
3. Click the virtual circuit.
4. Click Edit and make your changes. Avoid entering confidential information.
5. Click Save.
To terminate the connection to Azure

The following flow chart shows the overall process of terminating a VNet-to-VCN connection.

1. In the Azure portal, view the ExpressRoute circuit, and then view its Connections. Confirm that there are no Connections still in existence for the ExpressRoute circuit. Delete all Connections before proceeding.

2. In the Oracle portal, delete your FastConnect virtual circuit:
   a. Open the navigation menu. Under Core Infrastructure, go to Networking and click FastConnect.
   b. Select the compartment where the connection resides, and then click the connection.
   c. Click the virtual circuit.
   d. Click Delete.
   e. Confirm when prompted.

   The virtual circuit's Lifecycle State switches to TERMINATING.

3. In the Azure portal, confirm that the private peering for the ExpressRoute circuit has been deleted. Also confirm that the ExpressRoute circuit's status has changed to "Not Provisioned".

4. In the Azure portal, delete the ExpressRoute circuit.

The connection between Azure and Oracle Cloud Infrastructure is terminated.
Access to Other Clouds with Libreswan

Libreswan is an open source IPSec implementation that is based on FreeS/WAN and Openswan. Most Linux distributions include Libreswan or make it easy to install. You can install it on hosts in either your on-premises network or a cloud provider network. This topic shows how to connect your Oracle Cloud Infrastructure virtual cloud network (VCN) with another cloud provider by using an IPSec VPN with a Libreswan VM as the customer-premises equipment (CPE).

In the example shown here, the other cloud provider is Amazon Web Services (AWS). The connection is a secure and encrypted site-to-site IPSec VPN between the Oracle and Amazon environments. It enables resources in the two clouds to communicate with each other using their private IP addresses as if they are in the same network segment.

A Libreswan CPE guide is also available for all other use cases.

Virtual tunnel interface (VTI) support for this route-based configuration requires minimum Libreswan version 3.18 and a recent Linux 3.x or 4.x kernel. This configuration was validated using Libreswan version 3.29.

Architecture

The following diagram shows the general layout of the connection.

Supported IPSec Parameters

For a vendor-neutral list of supported IPSec parameters for all regions, see Supported IPSec Parameters on page 2945.

The Oracle BGP ASN for the commercial cloud is 31898. If you're configuring VPN Connect for the US Government Cloud, see Required VPN Connect Parameters for Government Cloud on page 152 and also Oracle's BGP ASN on page 154. For the United Kingdom Government Cloud, see Oracle's BGP ASN on page 171.

Configuration

Important:

The configuration instructions in this section are provided by Oracle Cloud Infrastructure for Libreswan. If you need support or further assistance, consult the Libreswan documentation.
Libreswan supports both route-based and policy-based tunnels. The tunnel types can coexist without interfering with each other. The Oracle VPN headends use route-based tunnels. Oracle recommends that you configure Libreswan with the Virtual Tunnel Interface (VTI) configuration syntax.

Refer to Supported IPSec Parameters on page 3310 for more details about the specific parameters used in this document.

**Default Libreswan Configuration Files**

The default Libreswan installation creates the following files:

- `/etc/ipsec.conf`: The root of the Libreswan configuration.
- `/etc/ipsec.secrets`: The root of the location where Libreswan looks for secrets (the tunnel pre-shared keys).
- `/etc/ipsec.d/`: A directory for storing the `.conf` and `.secrets` files for your Oracle Cloud Infrastructure tunnels (for example: `oci-ipsec.conf` and `oci-ipsec.secrets`). Libreswan encourages you to create these files in this folder.

The default `/etc/ipsec.conf` file includes this line:

```bash
include /etc/ipsec.d/*.conf
```

The default `/etc/ipsec.secrets` file includes this line:

```bash
include /etc/ipsec.d/*.secrets
```

The preceding lines automatically merge all the `.conf` and `.secrets` files in the `/etc/ipsec.d` directory into the main configuration and secrets files that Libreswan uses.

**About Using IKEv2**

Oracle supports Internet Key Exchange version 1 (IKEv1) and version 2 (IKEv2). If you configure the IPSec connection in the Console to use IKEv2, you must configure your CPE to use only IKEv2 and related IKEv2 encryption parameters that your CPE supports. For a list of parameters that Oracle supports for IKEv1 or IKEv2, see Supported IPSec Parameters on page 2945.

You specify the IKE version when setting up the IPSec configuration file in task 4 in the next section. In that example file, there's a comment showing how to configure IKEv1 versus IKEv2.

**Configuration Process**

**Task 1: Prepare the AWS Libreswan instance**

1. Using the AWS Console or APIs, create a Libreswan VM by using its provisioning process. Use Oracle Linux, CentOS, or Red Hat as the main operating system.
2. After the new instance starts, connect to it with SSH and install the Libreswan package:

```bash
sudo yum -y install libreswan
```
3. In the AWS Console, disable the source and destination checks on the Libreswan VM instance by right-clicking the instance, clicking Networking, and then clicking Change Source/Dest. Check. When prompted, click Yes, Disable.

4. On the Libreswan VM, configure IP_forward to allow AWS clients to send and receive traffic through the Libreswan VM. In the /etc/sysctl.conf file, set the following values and apply the updates with `sudo sysctl -p`.

   ```
   net.ipv4.ip_forward=1
   net.ipv4.conf.all.send_redirects = 0
   net.ipv4.conf.all.accept_redirects = 0
   net.ipv4.conf.default.send_redirects = 0
   net.ipv4.conf.default.accept_redirects = 0
   net.ipv4.conf.eth0.send_redirects = 0
   net.ipv4.conf.eth0.accept_redirects = 0
   ```

5. In the AWS Console, edit your AWS route table. Add a rule with the VCN CIDR (172.0.0.0/16) as the destination and the AWS Libreswan instance ID (i-016ab864b43cb368e in this example) as the target.

6. In the AWS Console, enable inbound TCP and UDP traffic on ports 4500 and 500 to allow Oracle Cloud Infrastructure IPSec VPN communication with the AWS Libreswan VM. This task includes editing both the AWS
security groups and network ACLs. You can set the source value can be the Oracle public IP (the Oracle VPN headend IPSec tunnel endpoint) instead of 0.0.0.0/0.

For security groups:

For network ACLs:
Task 2: Configure the Oracle Cloud Infrastructure DRG and CPE object

1. In the Oracle Console, create a customer-premises equipment (CPE) object that points to the Libreswan AWS instance public IP address (34.200.255.174).

2. If you don’t already have a DRG attached to your VCN: in the Oracle Console, create a DRG and then attach it to the VCN (172.0.0.0/16).
3. In the Oracle Console, create an IPSec connection and point it to the AWS VPC CIDR (10.0.0.0/16). In other words, when you create the IPSec connection, set its static route to the AWS VPC CIDR.

For each configured IPSec connection, Oracle creates two tunnels and assigns these items to each one:
- Oracle VPN headend IPSec tunnel endpoint
- Oracle VPN tunnel shared secret

You can view the IPSec tunnel status and Oracle VPN headend IP by clicking the Actions icon (three dots) for the IPSec connection, and then clicking View Details. Initially each tunnel is in the DOWN state (offline) because you still have some additional configuration to do later on the AWS Libreswan VM.

To view the shared secret, click the Actions icon (three dots) for an individual tunnel, and then click View Details. Next to Shared Secret, click Show.

4. In the Oracle Console, edit the VCN's security rules to enable ingress TCP and UDP traffic on ports 4500 and 500 like you did for the AWS security groups and network ACLs. You can use the AWS Libreswan VM public IP address instead of 0.0.0.0/0 if it's a persistent public IP. Also open all protocols and ports for ingress traffic from the AWS VPC CIDR (10.0.0.0/16). Remember: Security lists are associated with a subnet, so edit the security
Networking

list associated with each subnet that needs to communicate with the AWS VPC. Or, if you're using VCN network security groups, edit the rules in the relevant NSGs.

5. In the Oracle Console, edit the VCN’s route tables to add a rule that has the AWS VPC CIDR (10.0.0.0/16) as the destination CIDR block and the DRG you created earlier as the target. Remember: Route tables are associated with a subnet, so edit the route table associated with each subnet that needs to communicate with the AWS VPC. The following screenshot shows the route table for the VCN with an added route for the AWS VPC CIDR.

Task 3: Determine the required configuration values

The Libreswan configuration uses the following variables. Determine the values before proceeding with the configuration.

- `${cpeLocalIP}`: The IP address of your Libreswan device.
- `${cpePublicIpAddress}`: The public IP address for Libreswan. This is the IP address of your outside interface. Depending on your network topology, the value might be different from `${cpeLocalIP}`.
- `${oracleHeadend1}`: For the first tunnel, the Oracle public IP endpoint obtained from the Oracle Console.
- `${oracleHeadend2}`: For the second tunnel, the Oracle public IP endpoint obtained from the Oracle Console.
- `${vti1}`: The name of the first VTI used. For example, vti1.
- `${vti2}`: The name of the second VTI used. For example, vti2.
- `${sharedSecret1}`: The pre-shared key for the first tunnel. You can use the default Oracle-provided pre-shared key, or provide your own when you set up the IPSec connection in the Oracle Console.
- `${sharedSecret2}`: The pre-shared key for the second tunnel. You can use the default Oracle-provided pre-shared key, or provide your own when you set up the IPSec connection in the Oracle Console.
- `${vcnCidrNetwork}`: The VCN IP range.

Task 4: Set up the configuration file: `/etc/ipsec.d/oci-ipsec.conf`

Libreswan configuration uses the concept of left and right to define the configuration parameters for your local CPE device and the remote gateway. Either side of the connection (the conn in the Libreswan configuration) can be left or right, but the configuration for that connection must be consistent. In this example:

- **Left**: Your local Libreswan CPE
- **Right**: The Oracle VPN headend

Use the following template for your `/etc/ipsec.d/oci-ipsec.conf` file. The file defines the two tunnels that Oracle creates when you set up the IPSec connection.
Important:
If your CPE is behind a 1–1 NAT device, uncomment the `leftid` parameter and set it equal to the `${cpePublicIpAddress}`.

```plaintext
conn oracle-tunnel-1
  left=${cpeLocalIP}
  # leftid=${cpePublicIpAddress} # See preceding note about 1-1 NAT device
  right=${oracleHeadend1}
  authby=secret
  leftsubnet=0.0.0.0/0
  rightsubnet=0.0.0.0/0
  auto=start
  mark=5/0xffffffff # Needs to be unique across all tunnels
  vti-interface=${vti1}
  vti-routing=no
  ikev2=no # To use IKEv2, change to ikev2=insist
  ike=aes_cbc256-sha2_384;modp1536
  phase2alg=aes_gcm256;modp1536
  encapsulation=yes
  ikelifetime=28800s
  salifetime=3600s

conn oracle-tunnel-2
  left=${cpeLocalIP}
  # leftid=${cpePublicIpAddress} # See preceding note about 1-1 NAT device
  right=${oracleHeadend2}
  authby=secret
  leftsubnet=0.0.0.0/0
  rightsubnet=0.0.0.0/0
  auto=start
  mark=6/0xffffffff # Needs to be unique across all tunnels
  vti-interface=${vti2}
  vti-routing=no
  ikev2=no # To use IKEv2, change to ikev2=insist
  ike=aes_cbc256-sha2_384;modp1536
  phase2alg=aes_gcm256;modp1536
  encapsulation=yes
  ikelifetime=28800s
  salifetime=3600s
```

Task 5: Set up the secrets file: `/etc/ipsec.d/oci-ipsec.secrets`

Use the following template for your `/etc/ipsec.d/oci-ipsec.secrets` file. It contains two lines per IPSec connection (one line per tunnel).

```plaintext
${cpePublicIpAddress} ${ipAddress1}: PSK "${sharedSecret1}"
${cpePublicIpAddress} ${ipAddress2}: PSK "${sharedSecret2}"
```

Task 6: Restart the Libreswan configuration

After setting up your configuration and secrets files, you must restart the Libreswan service with the following command.

```plaintext
Important:
Restarting the Libreswan service may impact existing tunnels.
```

```
service ipsec restart
```
**Task 7: Configure IP routing**

Use the following `ip` command to create static routes that send traffic to your VCN through the IPSec tunnels. If you're logged in with an unprivileged user account, you might need to use `sudo` before the command.

```
<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static routes created with the IP route command do not persist through a reboot. To determine how to make your routes persist, refer to the documentation of your Linux distribution of choice.</td>
</tr>
</tbody>
</table>
```

```
ip route add ${VcnCidrBlock} nexthop dev ${vti1} nexthop dev ${vti2}
ip route show
```

**Verification**

A Monitoring service is also available from Oracle Cloud Infrastructure to actively and passively monitor your cloud resources. For information about monitoring your VPN Connect, see [VPN Connect Metrics](#) on page 3164.

If you have issues, see [VPN Connect Troubleshooting](#) on page 3166.

**Checking the Libreswan Status**

Check the current state of your Libreswan tunnels by using the following command:

```
ipsec status
```

The tunnel is established if you see a line that includes the following:

```
STATE_MAIN_I4: ISAKMP SA established
```

If you're using IKEv2, you see the following:

```
STATE_V2_IPSEC_I (IPsec SA established)
```

In the future, if you need to open a support ticket with Oracle about your Libreswan tunnel, include the output of the preceding `ipsec status` command.

**Checking the Tunnel Interface Status**

Check if the virtual tunnel interfaces are up or down by using the `ifconfig` command or the `ip link show` command. You can also use applications such as tcpdump with the interfaces.

Here's an example of the `ifconfig` output with a working Libreswan implementation that shows the available VTIs.

```
ifconfig
<output trimmed>
vti01: flags=209<UP,POINTOPOINT,RUNNING,NOARP> mtu 8980
   inet6 2001:db8::1 prefixlen 64 scopeid 0x20<link>
      tunnel txqueuelen 1000 (IPIP Tunnel)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 10 dropped 0 overruns 0 carrier 10 collisions 0

vti02: flags=209<UP,POINTOPOINT,RUNNING,NOARP> mtu 8980
   inet6 2001:db8::2 prefixlen 64 scopeid 0x20<link>
      tunnel txqueuelen 1000 (IPIP Tunnel)
      RX packets 0 bytes 0 (0.0 B)
```

Networking

| RX errors 0 dropped 0 overruns 0 frame 0 |
| TX packets 0 bytes 0 (0.0 B)          |
| TX errors 40 dropped 0 overruns 0 carrier 40 collisions 0 |

Here's an example of the `ip link show` output:

```
ip link show
<output trimmed>

9: vti01@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 8980 qdisc noqueue
   state UNKNOWN mode DEFAULT group default qlen 1000
   link/ipip 10.1.2.3 peer 192.168.0.51

10: vti02@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 8980 qdisc noqueue
    state UNKNOWN mode DEFAULT group default qlen 1000
    link/ipip 10.1.2.3 peer 192.168.0.49
```

Also, in the Oracle Console, each IPSec tunnel should now be in the UP state.

**Network Performance**

The content in the sections below apply to **Category 7** and **Section 3.c** of the Oracle PaaS and IaaS Public Cloud Services Pillar documentation. You can download a PDF from the Oracle Cloud Infrastructure Service Level Agreement page.

Oracle Cloud Infrastructure provides a service-level agreement (SLA) for network throughput between instances in the same availability domain in a virtual cloud network (VCN). You might think of this as a measurement of LAN performance.

**Important:**

This SLA applies only to bare metal instances.

To meet the SLA, the network throughput for instances within the same availability domain and VCN must be at least 90% of the stated maximum for at least 99.9% of the billing month. Network throughput is measured in megabits per second (Mbps) or gigabits per second (Gbps).

For the stated maximum bandwidth by instance shape, see the "Network Bandwidth" column in the "Shape" tables.

**Testing Methodology**

Launch two bare metal instances in the same availability domain and VCN. Install and run the `iperf3` utility, with one instance as server and the other as client. Look at the `iperf3` bandwidth results to determine your VCN's network throughput.

1. Launch two bare metal instances in the same availability domain in a single VCN. Designate one as the server and the other as the client. For launch instructions, see Creating an Instance on page 695.
2. Install `iperf3` on both instances. Example Linux command:
   ```bash
   sudo yum install -y iperf3
   ```
3. Enable communication to the server instance on TCP port 5201 (for `iperf3`):
   a. For the subnet that the server instance is in, add a rule to the subnet's security list to allow stateless ingress traffic on TCP port 5201 from any source IP address (0.0.0.0/0) and any source port. For instructions, see
To update rules in an existing security list on page 2853. If you are instead using network security groups (NSGs) with the instance, add the rule to the instance's NSG.

b. On the instance itself, open the firewall to allow iperf3 traffic. Example Linux commands:

```
Caution:
For instances with an iSCSI boot volume, the following --reload command can cause problems. For details and a workaround, see Instances experience system hang after running firewall-cmd --reload.
```

```
sudo firewall-cmd --zone=public --permanent --add-port 5201/tcp
sudo firewall-cmd --reload
```

4. Start the iperf3 test:
   a. On the server instance, run iperf3 in server mode. Example Linux command:

```
iperf3 -s
```

   b. On the client instance, run iperf3 in client mode and specify the private IP address of the server instance. Example Linux command:

```
iperf3 -c <server_instance_private_ip_address>
```

5. Look at the iperf3 results on the client instance. The network throughput between the two instances is shown under "Bandwidth" in the last five lines of the client's iperf3 test output. For example:

```
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval         Transfer      Bandwidth        Retr
[  4] 0.00-10.00  sec  XX.YY GBytes  NN.NN Gbits/sec  752
 sender
[  4] 0.00-10.00  sec  XX.YY GBytes  NN.NN Gbits/sec
 receiver
iperf Done.
```

Frequently Asked Questions

Q: My VCN isn't meeting the bandwidth SLA. What should I do?
A: Ensure that the CPU on the instance isn't loaded heavily with other services or applications. Confirm with a utility such as `top` to look at the average CPU utilization. It should be less than one.

Q: Can I use the preceding iperf instructions to test performance between hosts that are not in the same availability domain, or between a host in the VCN and a host in the on-premises network?
A: Yes. The instructions can be used to test performance between any two endpoints. For accurate results, when transferring data outside an availability domain, you must add `--parallel 5` at the end of the client connection command.

Networking Metrics

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

There are multiple Monitoring service metric namespaces related to networking resources.

For instance connectivity:

- `oci_vcn`: Metrics related to `VNICs`. See VNIC Metrics on page 3321.

For cloud connectivity:
Networking

- **oci_fastconnect**: Metrics related to *FastConnect*. See *FastConnect Metrics* on page 3236.
- **oci_vpn**: Metrics related to an *IPSec VPN connection*. See *VPN Connect Metrics* on page 3164.
- **oci_service_gateway**: Metrics related to a *service gateway*. See *Service Gateway Metrics* on page 3325.

**VNIC Metrics**

You can monitor the health, capacity, and performance of your Networking service VNICs by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace `oci_vcn` (the Networking service).

Resources: virtual network interface cards (VNICs).

**Overview of Metrics for an Instance and Its Network Devices**

If you're not already familiar with the different types of metrics available for an instance and its storage and network devices, see *Compute Instance Metrics* on page 788.

**Overview of Metrics: oci_vcn**

Each Compute instance has one or more Networking service *VNICs*. A VNIC connects the instance to a subnet in a virtual cloud network (VCN). A given VNIC controls how the instance communicates with endpoints inside the VCN (other instances) and endpoints outside the VCN (hosts on the internet, in your on-premises network, in another VCN, and so on).

With the Networking service metrics (in metric namespace `oci_vcn`), you can get this information for a VNIC:

- **Traffic to and from the network**: Per-VNIC traffic levels (packets and bytes), which can help you identify meaningful increases or decreases in traffic coming in and out of your instances
- **Packets dropped due to security list violations**: Per-VNIC drops (dropped packets), which can help you identify changes in traffic caused by security list changes

The following diagram illustrates the general concept. A given instance resides in a subnet within a VCN that has one or more gateways to communicate with other networks. The instance is enlarged to show its VNIC, which the instance uses to communicate with the network. In this context, the term network means both the other instances in the VCN and hosts outside the VCN available through the gateways.

The VNIC receives traffic from the network and sends traffic to the network. The Networking service drops packets according to security list rules you set up for the instance's subnet. Traffic coming to the VNIC from the network is measured after the Networking service drops the packets that violate the subnet's security list rules. Traffic leaving the VNIC is measured before the Networking service drops the packets that violate the subnet's security list rules.
Networking

The Compute service separately reports network-related metrics as measured on the instance itself and aggregated across all the attached VNICs. Those metrics are available in the oci_computeagent metric namespace. For more information, see Compute Instance Metrics on page 788.

Raw Data Point Frequency

For every 1-minute interval, the Networking service posts one raw data point to the Monitoring service. The Monitoring service charts show data points at 1-minute, 5-minute, 1-hour (60-minute), and 1-day intervals. Supported values for interval depend on the specified time range in the metric query (not applicable to alarm queries). More interval values are supported for smaller time ranges. For example, if you select one hour for the time range, then all interval values are supported. If you select 90 days for the time range, then only the 1h or 1d interval values are supported. The available statistics are calculated by using the count of 1-minute data points in the select interval. For example, for a given metric:

- The mean for each 5-minute interval is calculated over five raw data points.
The mean for each 60-minute interval is calculated over 60 raw data points.

**Required IAM Policy**

When writing an IAM policy for viewing VNIC metrics, it's important to remember that:

- The VNIC and the VNIC's metrics (emitted by the `oci_vcn` metric namespace) reside in the subnet's compartment, and not the instance's compartment.
- The VNIC attachment (which is an object different from the VNIC itself) resides in the instance's compartment.

If the instance and subnet are in the same compartment, these details aren't so important when you write the IAM policy.

**Minimum required policy for getting VNIC metrics**

The following policy contains the one statement required to get VNIC metrics, which are part of the `oci_vcn` metric namespace.

If you're using the Console, this policy lets you go to the Monitoring tab in the Console and view the metrics for one or more VNICs in the specified compartment. The policy uses an example group called VnicMetricReaders. The condition at the end (`where target.metrics.namespace='oci_vcn'`) allows the group to view only the metrics in the `oci_vcn` metric namespace.

Allow group VnicMetricReaders to read metrics in compartment `<subnet_compartment>` where target.metrics.namespace='oci_vcn'

**Policy for viewing a VNIC's details and metrics in the Console**

The following policy lets you view an instance in the Console, click through to a specific VNIC, and then view that VNIC's details and metrics.

Allow group VnicMetricReaders to read metrics in compartment `<subnet_compartment>` where target.metrics.namespace='oci_vcn'

Allow group VnicMetricReaders to read instance-family in compartment `<instance_compartment>`

Allow group VnicMetricReaders to inspect virtual-network-family in compartment `<subnet_compartment>`

The second and third statements let you view the instance's details and the VNIC's details, respectively.

**Available Metrics: oci_vcn**

The metrics listed in the following table are automatically available for any VNIC on any instance you create. You do not need to enable monitoring on the instance to get these metrics for the VNIC or VNICs on the instance.

You also can use the Monitoring service to create custom queries.

Each metric includes the following dimension:

**RESOURCEID**

The *OCID* of the VNIC.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VnicEgressDropsSecurityList</td>
<td>Egress Packets Dropped by Security List</td>
<td>packets</td>
<td>Packets sent by the VNIC, destined for the network, dropped due to security rule violations.</td>
<td>resourceId</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>VnicIngressDrops</td>
<td>Ingress Packets</td>
<td>packets</td>
<td>Packets received from the network, destined for the VNIC, dropped due to security rule violations.</td>
<td></td>
</tr>
<tr>
<td>VnicFromNetwork</td>
<td>Bytes from Network</td>
<td>bytes</td>
<td>Bytes received at the VNIC from the network, after drops.</td>
<td></td>
</tr>
<tr>
<td>VnicFromNetwork</td>
<td>Packets from Network</td>
<td>packets</td>
<td>Packets received at the VNIC from the network, after drops.</td>
<td></td>
</tr>
<tr>
<td>VnicToNetwork</td>
<td>Bytes to Network</td>
<td>bytes</td>
<td>Bytes sent from the VNIC to the network, before drops.</td>
<td></td>
</tr>
<tr>
<td>VnicToNetwork</td>
<td>Packets to Network</td>
<td>packets</td>
<td>Packets sent from the VNIC to the network, before drops.</td>
<td></td>
</tr>
</tbody>
</table>

* The Compute service separately reports network-related metrics as measured on the instance itself and aggregated across all the attached VNICs. Those metrics are available in the oci_computeagent metric namespace. For more information, see Compute Instance Metrics on page 788.

**Tips for Working with VNIC Metrics**

Here are some tips to help you use VNIC metrics.

**Default Metric Charts for One VNIC Versus Multiple VNICs**

The default charts for VNIC metrics use these default settings:

- Time range = the last hour
- Interval = 1 minute
- Statistic displayed: Sum
- Aggregation of metric streams = not selected (which means each VNIC is displayed as a separate line on the chart)

You can view the default charts with data for only a single VNIC by viewing the VNIC's details in the Console. When looking at a single VNIC, these statistics are the most useful: sum, mean, max, and min.

You can view the default charts with data for multiple VNICs by going to the Service Metrics page in the Console. Select the necessary compartment and metric namespace (oci_vcn) at the top of the page. For all the charts, you can either show each VNIC as a separate line, or show a single line that aggregates the data for all the VNICs in your selected compartment. To aggregate the data, select the check box for Aggregate Metric Streams.

When viewing aggregated data, you can use the P90 - P99.9 statistics to help identify typical behavior of your instance fleet and outliers. To view these statistics over an even larger number of data points, expand the chart's start and end time (for example, view the last 7 days instead of the last hour), and set the interval to 1 hour.

For general information about how to work with and modify the default metric charts, see Using the Console on page 2672 in the Monitoring documentation.
Alarms for VNIC Metrics

You can set up alarms for a given metric. For VNICs, an alarm makes the most sense for the egress security list drops metric (VnicEgressDropsSecurityList). In a normal situation, you shouldn't have egress security list drops. If you do, it might be due to one of the following causes:

- An application is behaving in an unexpected manner
- Your security list is incorrectly configured

In either case, an alarm is warranted.

Using the Console

To view default metric charts for a single VNIC

1. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.
2. Click the instance to view its details.
3. Under Resources, click Attached VNICs.
4. Click the VNIC to view its details.
5. Under Resources, click Metrics.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for multiple VNICs

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that contains the VNICs you're interested in. Remember that a given VNIC resides in its subnet's compartment.
3. For Metric Namespace, select oci_vcn.

The Service Metrics page dynamically updates the page to show charts for each metric emitted by the selected metric namespace.

Tip:

If the compartment has multiple VNICs, the charts default to show a separate line for each VNIC. By selecting the check box for Aggregate Metric Streams on the right side of the page, you can show a single line aggregated across all the VNICs.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Service Gateway Metrics

You can monitor the health, capacity, and performance of your service gateways by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

This topic describes the metrics emitted by the metric namespace oci_service_gateway.

Resources: Service gateways
Overview of Metrics: oci_service_gateway

A service gateway is used to enable on-premises hosts or VCN hosts to privately access Oracle services (such as Object Storage and Autonomous Database) without exposing the resources to the public internet.

The available metrics help you determine quickly if your service gateway is up, how much data is flowing through the gateway, and if packets are being dropped for unexpected errors.

- Traffic to and from the service gateway: Per-gateway traffic levels (packets and bytes), which can help you identify meaningful increases or decreases in traffic coming in and out of the gateway.
- Packets dropped: Per-gateway drops (dropped packets), which can help you identify changes in traffic caused by issues such as gateway misconfiguration or unrecognized packet protocol.

Required IAM Policy

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_service_gateway

The metrics listed in the following table are automatically available for each service gateway that you create. You do not need to enable monitoring to get these metrics.

You also can use the Monitoring service to create custom queries.

Each metric includes one or more of the following dimensions:

- **RESOURCEID**: The OCID of the service gateway.
- **DROPTYPE**: The type of packet drop:
  - sgwDisabledDrops: Packets dropped because the service gateway is disabled.
  - sgwMtuExceededDrops: Packets dropped because the Maximum Transmission Unit (MTU) has been exceeded.
  - sgwServiceDestUnknown: Packets dropped because of an unknown or incorrect service destination.
  - sgwTtlExpiryDrops: Packets dropped because the TTL (Time To Live) value in the IPv4 header of the packet has expired.
  - sgwMisconfigurationDrops: Packets dropped because the gateway service moniker is misconfigured. For example, the gateway's associated route table points to a different CIDR service than the one specified in the gateway configuration.
  - sgwUnknownProtocolDrops: Packets dropped because the protocol in the IPv4 header of the packet is not recognized.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>packetsToService</td>
<td>Packets to Service</td>
<td>Packets</td>
<td>The number of packets successfully sent from the service gateway toward Oracle services.</td>
<td>resourceId</td>
</tr>
<tr>
<td>packetsFromService</td>
<td>Packets from Service</td>
<td>Packets</td>
<td>The number of packets successfully sent from the service gateway toward customer instances.</td>
<td></td>
</tr>
<tr>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------</td>
<td>-------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>bytesToService</td>
<td>Bytes</td>
<td>The number of bytes successfully sent from the service gateway toward Oracle services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bytesFromService</td>
<td>Bytes</td>
<td>The number of bytes successfully sent from the service gateway toward customer instances.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sgwDropsFromService</td>
<td>Packets</td>
<td>The number of packets dropped while sending packets from the service gateway toward customer instances.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sgwDropsToService</td>
<td>Packets</td>
<td>The number of packets dropped while sending packets from the service gateway toward Oracle services.</td>
<td>resourceId, dropType</td>
<td></td>
</tr>
</tbody>
</table>

**Using the Console**

To view default metric charts for all service gateways in a compartment:

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. In Compartment, select the compartment you're interested in.
3. For Metric Namespace, select oci_service_gateway.
4. The Service Metrics page dynamically updates the page to show charts for each metric emitted by the selected metric namespace.

By default, the charts show a separate line for each resource in the compartment.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

**Troubleshooting**

These topics cover some common issues and how to address them:

- Hanging Connection on page 3327
- Subnet or VCN Deletion on page 3334
- Redundancy Remedies on page 3336
- VPN Connect Troubleshooting on page 3166
- FastConnect Troubleshooting on page 3241

**Hanging Connection**

This topic covers one of the most common issues seen with communications between your cloud network and on-premises network: a hanging connection, even though you can ping hosts across the connection.

**Summary of Problem and Solutions**

**Symptom:** Your virtual cloud network (VCN) is connected to your existing on-premises network via an IPSec VPN, or Oracle Cloud Infrastructure FastConnect. Hosts on one side of the connection can ping hosts on the other side, but the connection hangs. For example:

- You can SSH to a host across the connection, but after you log in to the host, the connection hangs.
• You can start a Virtual Networking Computing (VNC) connection, but the session hangs.
• You can start an SFTP download, but the download hangs.

General problem: Path Maximum Transmission Unit Discovery (PMTUD) is probably not working on one or both sides of the connection. It must be working on both sides of the connection so that both sides can know if they're trying to send packets that are too large for the connection and adjust accordingly. For a brief overview of Maximum Transmission Unit (MTU) and PMTUD, see Overview of MTU on page 3329 and Overview of PMTUD on page 3330.

Solutions for fixing PMTUD:

1. **Ensure that your hosts are configured to use PMTUD:** If the hosts in your on-premises network don't use PMTUD (that is, if they don't set the Don't Fragment flag in the packets), they have no way to discover if they're sending packets that are too large for the connection. Your instances on the Oracle side of the connection use PMTUD by default. Do not change that configuration on the instances.

2. **Ensure both the VCN security lists and the instance firewalls allow ICMP type 3 code 4 messages:** When PMTUD is in use, the sending hosts receive a special ICMP message if they send packets that are too large for the connection. Upon receipt of the message, the host can dynamically update the size of the packets to fit the connection. However, your instances can't receive these important ICMP messages if both the security lists for the subnet in the VCN and the instance firewalls aren't configured to accept them.

   Tip:
   
   If you're using stateful security list rules (for TCP, UDP, or ICMP traffic), you don't need to ensure that your security list has an explicit rule to allow ICMP type 3 code 4 messages because the Networking service tracks the connections and automatically allows those messages. Stateless rules require an explicit ingress security list rule for ICMP type 3 code 4 messages. Confirm that the instance firewalls are set up correctly.

3. **Ensure that your router honors the Don't Fragment flag:** If the router doesn't honor the flag and thus ignores the use of PMTUD, it sends fragmented packets to the instances in the VCN, which is bad (see Why Avoid Fragmentation? on page 3329). The VCN's security lists are most likely configured in such a way that they recognize only the initial fragment, and the remaining ones are dropped, causing the connection to hang. Instead, your router should use PMTUD and honor the Don't Fragment flag to determine the correct size of unfragmented packets to send through the connection.

The parts of the solution are numbered and called out in red italics in the following diagram. It shows an example scenario with your on-premises network connected to your VCN over an IPSec VPN.
Keep reading for a brief overview of MTU and PMTUD, and how to check if PMTUD is working on both sides of the network connection.

**Why Avoid Fragmentation?**

You may be wondering why you want to avoid fragmentation. First, it adversely affects the performance of your application. Fragmentation requires reassembly of the fragments and retransmission if fragments are lost. Reassembly and retransmission require time and CPU resources.

Second, only the first fragment contains the source and destination port information. This means that firewalls or your VCN's security lists will probably drop the other packets, because they are typically configured to evaluate the port information. For fragmentation to work with your firewalls and security lists, you would have to configure them to be more permissive than usual, which is not desirable.

**Overview of MTU**

The communications between any two hosts across an Internet Protocol (IP) network use packets. Each packet has a source and destination IP address and a payload of data. Every network segment between the two hosts has a *Maximum Transmission Unit (MTU)* that represents the number of bytes that a single packet can carry.

The standard internet MTU size is 1500 bytes. This is also true for most home networks and many corporate networks (and their Wi-Fi networks). Some data centers, including those for Oracle Cloud Infrastructure, can have a larger MTU. The Compute instances use an MTU of 9000 by default. On a Linux host, you can use the `ifconfig` command to display the MTU of the host's network connection. For example, here's the `ifconfig` output from an Ubuntu instance (the MTU is highlighted in red italics):

```
ifconfig
ens3 Link encap:Ethernet HWaddr 00:00:00:00:00:01
inet addr:10.0.6.9 Bcast:10.0.6.31 Mask:255.255.255.224
inet6 addr: 2001:db8::/32 Scope:Link
UP BROADCAST RUNNING MULTICAST
MTU: 9000
Metric: 1
```

For comparison, here's the output from a machine connected to a corporate network:

```
ifconfig
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>

mtu 1500
```

Notice that its MTU is the more typical 1500 bytes.

If the host is connected through a corporate VPN, the MTU is even smaller, because the VPN tunnel must encapsulate the traffic inside an IPsec packet and send it across the local network. For example:

```
ifconfig
utun0: flags=81d1<UP,POINTOPOINT, RUNNING, NOARP, PROMISC, MULTICAST>

mtu 1300
```

How do the two hosts figure out how large of a packet they can send to each other? For many types of network traffic, such as HTTP, SSH, and FTP, the hosts use TCP to establish new connections. During the initial three-way handshake between two hosts, they each send the *Maximum Segment Size (MSS)* for how large their payload can be. This is smaller than the MTU. (TCP runs inside the Internet Protocol (IP), which is why it's referred to as TCP/IP. Segments are to TCP what packets are to IP.)
Networking

Using the `tcpdump` application, you can see the MSS value shared during the handshake. Here's an example from `tcpdump` (with the MSS highlighted in red italics):

```
12:11:58.846890 IP 192.168.0.25.22 > 10.197.176.19.58824: Flags [S.], seq 2799552952, ack 2580095593, win 26844, options [mss 1260, sackOK,TS val 44858491 ecr 1321638674,nop,wscale 7], length 0
```

The preceding packet is from an SSH connection to an instance from a laptop connected to a corporate VPN. The local network the laptop uses for its internet connection has an MTU of 1500 bytes. The VPN tunnel enforces an MTU of 1300 bytes. Then when the SSH connection is attempted, TCP (running inside the IP connection) tells the Oracle Cloud Infrastructure instance that it supports TCP segments that are less than or equal to 1260 bytes. With a corporate VPN connection, the laptop connected to the VPN typically has the smallest MTU and MSS compared to anything it's communicating with across the internet.

A more complex case is when the two hosts have a larger MTU than some network link between them that is not directly connected to either of them. The following diagram illustrates an example.

The example shows two servers, each directly connected to its own routed network that supports a 9000-byte MTU. The servers are in different data centers. Each data center is connected to the internet, which supports a 1500-byte MTU. An IPSec VPN tunnel connects the two data centers. That tunnel crosses the internet, so the inside of the tunnel has a smaller MTU than the internet. In this diagram, the MTU is 1380 bytes.

If the two servers try to communicate (with SSH, for example), during the three-way handshake, they agree on an MSS around 8960. The initial SSH connection might succeed, because the maximum packet sizes during the initial SSH connection setup are usually less than 1380 bytes. When one side tries to send a packet larger than the smallest link between the two endpoints, Path MTU Discovery (PMTUD) becomes critical.

**Overview of PMTUD**

Path MTU Discovery is defined in RFC 1191. It works by requiring the two communicating hosts to set a Don't Fragment flag in the packets they each send. If a packet from one of these hosts reaches a router where the egress (or outbound) interface has an MTU smaller than the packet length, the router drops that packet. The router also returns an ICMP type 3 code 4 message to the host. This message specifically says "Destination Unreachable, Fragmentation Needed and Don't Fragment Was Set" (defined in RFC 792). Effectively the router tells the host: "You told me not to fragment packets that are too large, and this one's too large. I'm not sending it." The router also tells the host the maximum size packets allowed through that egress interface. The sending host then adjusts the size of its outbound packets so they're smaller than the value the router provided in the message.

Here's an example that shows the results when an instance tries to ping a host (203.0.113.2) over the internet with an 8000-byte packet and the Don't Fragment flag set (that is, with PMTUD in use). The returned ICMP message is highlighted in red italics:

```
ping 203.0.113.2 -M do -s 8000
PING 203.0.113.2 (203.0.113.2) 8000(8028) bytes of data.
```
Networking

From 10.0.0.2 icmp_seq=1
Frag needed and DF set (mtu = 1500)

The response is exactly what's expected. The destination host is across the internet, which has an MTU of 1500 bytes. Even though the sending host's local network connection has an MTU of 9000 bytes, the host can't reach the destination host with the 8000-byte packet and gets an ICMP message accordingly. PMTUD is working correctly.

For comparison, here's the same ping, but the destination host is across an IPSec VPN tunnel:

ping 192.168.6.130 -M do -s 8000
PING 192.168.0.130 (192.168.0.130) 8000(8028) bytes of data.
From 192.0.2.2 icmp_seq=1 Frag needed and DF set
(mtu = 1358)

Here the VPN router sees that to send this packet to its destination, the outbound interface is a VPN tunnel. That tunnel goes across the internet, so the tunnel must fit inside the internet's 1500-byte MTU link. The result is that the inside of the tunnel only allows packets up to 1360 bytes (which the router then lowered to 1358, which can make things more confusing).

Finding Where PMTUD Is Broken

If PMTUD isn't working somewhere along the connection, you need to figure out why and where. Typically it's because the ICMP type 3 code 4 packet (from the router with the constrained link that can't fit the packet) never gets back to the sending host. This can happen if there's something blocking that kind of traffic between the host and the router. And it can happen on either side of the VPN tunnel (or other constrained MTU link).

Try Pinging From Each Side of the Connection

To troubleshoot the broken PMTUD, you must determine if PMTUD is working on each side of the connection. In this scenario, let's assume the connection is an IPSec VPN.

How to ping: Like in Overview of PMTUD on page 3330, ping a host on the other side of the connection with a packet that you know is too large to fit through the VPN tunnel (for example, 1500 bytes or larger). Depending on which operating system the sending host uses, you might need to format the ping command slightly different to ensure the Don't Fragment flag is set. For both Ubuntu and Oracle Linux, you use the -M flag with the ping command.

Here's information about the -M flag:

-M pmtudisc_opt
Select Path MTU Discovery strategy. pmtudisc_option may be either do (prohibit fragmentation, even local one), want (do PMTU discovery, fragment locally when packet size is large), or dont (do not set DF flag).

Here's an example ping (with the -M flag and the resulting ICMP message highlighted in red italics)

ping
-M do
-s 1500 192.168.6.130
PING 192.168.0.130 (192.168.0.130) 1500(1528) bytes of data.
From 10.0.0.2 icmp_seq=1
Frag needed and DF set (mtu = 1358)
**Good: PMTUD is working**

If the result includes the line "From x.x.x.x icmp_seq=1 Frag needed and DF set (mtu = xxxx)", then PMTUD is working on that side of the tunnel. Note that the source address of the ICMP message is the public IP address of the tunnel the traffic is trying to go out (for example 203.0.113.13 in the preceding Ubuntu example).

Also, ping from the other side of the connection to confirm PMTUD is working from that side. Both sides of the connection must recognize that there is a tunnel between them that can't fit the large packets.

**Bad: If you're testing your side of the connection and the ping succeeds**

If you're sending the ping from a host in your on-premises network, and the ping succeeds, that probably means your edge router is not honoring the Don't Fragment flag. Instead the router is fragmenting the large packet. The first fragment reaches the destination host, so the ping succeeds, which is misleading. If you try to do more than just ping, the fragments after the first get dropped, and the connection will hang.

**Verify that your router configuration honors the Don't Fragment flag.** The router's default configuration is to honor it, but someone might have changed the default.

**Bad: If you're testing the VCN side of the connection and you don't see the ICMP message**

When testing from the VCN side of the connection, if you don't see the ICMP message in the response, there is probably something dropping the ICMP packet before it reaches your instance.

There could be two issues:

- **Security list:** The Networking security list could be missing an ingress rule that allows ICMP type 3 code 4 messages to reach the instance. This is an issue only if you're using stateless security list rules. If you're using stateful rules, your connections are tracked and the ICMP message is automatically allowed without needing a specific security list rule to allow it. If you're using stateless rules, ensure that the subnet the instance is in has a security list with an ingress rule that allows ICMP traffic type 3 code 4 from source 0.0.0.0/0 and any source port. For more information, see Security Lists on page 2850, and specifically To update rules in an existing security list on page 2853.

- **Instance firewall:** The instance's firewall rules (set in the OS) could be missing a rule that allows ICMP type 3 code 4 messages to reach the instance. Specifically for a Linux instance, ensure that iptables or firewalld is configured to allow the ICMP type 3 code 4 messages.

**Avoiding the Need for PMTUD**

Oracle recommends using PMTUD. However, in some situations it's possible to configure servers so they don't need to rely on it. Consider the case of the instances in your VCN communicating across an IPSec VPN to hosts in your on-premises network. You know the range of IP addresses for your on-premises network. You can add a special route to your instances that specifies the maximum MTU to use when communicating with hosts in that address range. The instance-to-instance communication within the VCN still uses an MTU of 9000 bytes.

The following information shows how to set that route on a Linux instance.

The default route table on the instance typically has two routes: the default route (for the default gateway), and a local route (for the local subnet). For example:

```
ip route show
default via 10.0.6.1 dev ens3
10.0.6.0/27 dev ens3 proto kernel scope link src 10.0.6.9
```

You can add another route that points to the same default gateway, but with the address range of the on-premises network and a smaller MTU. For example, in the following command, the on-premises network is 1.0.0.0/8, the default gateway is 10.0.6.1, and the maximum MTU size is 1300 for packets being sent to the on-premises network.

```
ip route add 1.0.0.0/8 via 10.0.6.1 mtu 1300
```

The updated route table looks like this:

```
ip route show
```

```
Within the VCN, the instance-to-instance communication continues to use 9000 MTU. However, communication to the on-premises network uses a maximum of 1300. This example assumes there's no part of the connection between the on-premises network and VCN that uses an MTU smaller than 1300.

**Important:**
The preceding commands do not persist if you reboot the instance. You can make the route permanent by adding it to a configuration file in the OS. Oracle Linux, for example, uses an interface-specific file called `/etc/sysconfig/network-scripts/route-<interface>`. For more information, see the documentation for your variant of Linux.

**VCN Troubleshooting**

**Breaking API Changes**
If anyone in your organization implements a regional subnet, be aware that you may need to update any client code that works with Networking service subnets and private IPs. There are possible breaking API changes. For more information, see the regional subnet release note.

**DNS Resolver Endpoints**
Network security groups (NSGs) act as a virtual firewall for your DNS resolver endpoints. An NSG consists of a set of ingress and egress security rules that apply only to the associated DNS resolver endpoints.

**Secondary IP Address**
If you've assigned a secondary IP to a secondary VNIC, and you're using policy-based routing for the secondary VNIC, make sure to configure the route rules to look up the same route table for the secondary IP address.

**DNS in Your VCN**
You use the Domain Name Server DHCP option to specify the DNS Type for the associated subnet. If you change the option's value, either restart the DHCP client on the instance or reboot the instance. Otherwise, the change does not get picked up until the DHCP client refreshes the lease (within 24 hours).

By default, the Internet and VCN Resolver does not let instances resolve the hostnames of hosts in your on-premises network connected to your VCN by IPSec VPN connection or FastConnect. That functionality can be achieved either by using a custom resolver or by configuring the VCN's private DNS resolver.

**Requirements for DNS Labels and Hostnames**
- VCN and subnet labels: Max 15 alphanumeric characters and must start with a letter. **Notice that hyphens and underscores are NOT allowed.** The value cannot be changed later.
- Hostnames: Max 63 characters and must be compliant with RFCs 952 and 1123. The value can be changed later.

Don't confuse the DNS label or hostname with the friendly name you can assign to the object (that is, the *display name*), which doesn't have to be unique.

**Firewalls**
Your instances running Oracle-provided Linux images or Windows images also have OS firewall rules that control access to the instance. When troubleshooting access to an instance, make sure that all of the following items are set correctly:
- The rules in the network security groups that the instance is in
• The rules in the security lists associated with the instance's subnet
• The instance's OS firewall rules

For more information, see Oracle-Provided Images on page 629.

If your instance is running Oracle Autonomous Linux 7, Oracle Linux 8, or Oracle Linux 7, you need to use firewalld to interact with the iptables rules. For your reference, here are commands for opening a port (1521 in this example):

```
sudo firewall-cmd --zone=public --permanent --add-port=1521/tcp
sudo firewall-cmd --reload
```

For instances with an iSCSI boot volume, the preceding --reload command can cause problems. For details and a workaround, see Instances experience system hang after running firewall-cmd --reload.

**Subnet or VCN Deletion**

This topic covers reasons why deletion of a subnet or VCN might fail.

Remember:

• To delete a VCN, it must first be empty and have no related resources or attached gateways (for example: no internet gateway, dynamic routing gateway, and so on).
• To delete a VCN's subnets, they must first be empty.

**Delete All Option**

The Console has an easy "Delete all" process that deletes a VCN and its related Networking resources (subnets, route tables, security lists, sets of DHCP options, internet gateway, and so on). If the VCN is attached to a dynamic routing gateway (DRG), the attachment is deleted, but the DRG remains.

The "Delete All" process deletes one resource at a time and takes a minute or two. A progress report is displayed to show you what's been deleted so far.

Before using the "Delete All" process, verify there are no instances, load balancers, DB systems, or orphaned mount targets in any of the subnets. For more information, see Subnet or VCN Deletion on page 3334.

If there are still resources in any subnet, or if you don't have permission to delete a particular Networking resource, the "Delete All" process stops and an error message is displayed. Any resources deleted up to that point cannot be restored. You might need to contact your tenancy administrator to help you delete any remaining resources.

**The Subnet Isn't Empty**

The most common reason a subnet (and thus a VCN) can't be deleted is because the subnet contains one or more of these resources:

• Load balancer
• Mount target
• DB system

**Note:**

When you create one of the preceding resources, you specify a VCN and subnet for it. The relevant service creates at least one VNIC in the subnet and attaches the VNIC to the resource. The service manages the VNICs on your behalf, so they are not readily apparent to you in the Console. The VNIC enables the resource to communicate with other resources over the network. Although this documentation commonly talks about the resource itself being in the subnet, it's actually the resource's attached VNIC. This documentation uses the term *parent resource* to refer to this type of resource.

If the subnet is empty when you try to delete it, its state changes to TERMINATING briefly and then to TERMINATED.
Networking

If the subnet is not empty, you instead get an error indicating that there are still resources that you must delete first. The error includes the OCID of a VNIC that is in the subnet (there could be more, but the error returns only a single VNIC’s OCID).

You can use the Oracle Cloud Infrastructure command line interface (CLI) or another SDK or client to call the GetVnic operation with the VNIC OCID. The response includes the VNIC’s display name. Depending on the type of parent resource, the display name can indicate which parent resource the VNIC belongs to. You can then delete that parent resource, or you can contact your administrator to determine who owns the resource. When the VNIC’s parent resource is deleted, the attached VNIC is also deleted from the subnet. If there are remaining VNICs in the subnet, repeat the process of determining and deleting each parent resource until the subnet is empty. Then you can delete the subnet.

For example, if you're using the CLI, use this command to get information about the VNIC:

```bash
oci network vnic get --vnic-id <VNIC_OCID>
```

Load balancer example

Here is an example CLI response for a VNIC that belongs to a load balancer. The display name shows the load balancer's OCID:

```json
{
  "data": {
    "availability-domain": "fooD:PHX-AD-1",
    "compartment-id": "ocid1.compartment.oc1..<unique_id_1>",
    "defined-tags": {},
    "display-name": "VNIC for LB ocid1.loadbalancer.oc1.phx.<unique_id_2>",
    "freeform-tags": {},
    "hostname-label": null,
    "id": "ocid1.vnic.oc1.phx.<unique_id_3>",
    "is-primary": false,
    "lifecycle-state": "AVAILABLE",
    "mac-address": "00:00:17:00:BB:CA",
    "private-ip": "10.0.0.6",
    "public-ip": null,
    "skip-source-dest-check": false,
    "subnet-id": "ocid1.subnet.oc1.phx.<unique_id_4>",
    "time-created": "2019-05-11T04:28:31.950000+00:00"
  },
  "etag": "5d8213fa"
}
```

File Storage example

Here's an example for a VNIC that belongs to a File Storage mount target:

```json
"display-name": "fss-<integer>",
```

Although the display name does not include an OCID, the fss characters indicate that the resource is for the File Storage service.

Database example

Here's an example of the display name for a VNIC that belongs to a DB system:

```json
"display-name": "ocid1.dbnode.oc1.phx.<unique_id>",
```

A Network Security Group Isn’t Empty

Another reason a VCN can't be deleted is because it contains a one or more network security groups (NSGs) that are not yet empty. To delete an NSG, it must not contain any VNICs (or parent resources with VNICs). You can
determine what parent resources are in an NSG by using either the Console or REST API. For more information, see To delete an NSG on page 2849.

There Are Resources in Compartments You Don't Have Access To

You might not be able to see all the resources in a subnet or VCN. This is because subnets and VCNs can contain resources in multiple compartments, and you might not have access to all the compartments. For example, the subnet might contain instances that your team manages but also DB systems that another team manages. Another example: The VCN might have security lists or a gateway in a compartment that another team manages. You might need to contact your tenancy administrator to help you determine who owns the resources in the subnet or VCN.

Other useful links

- Virtual Network Interface Cards (VNICs) on page 2855
- DNS in Your Virtual Cloud Network on page 2910
- IP Addresses and DNS in Your VCN on page 2864

Redundancy Remedies

Oracle recommends setting up a redundant connection between your on-premises network and virtual cloud network (VCN) for high availability. This topic gives background and links to other topics that describe how to resolve some common redundancy issues with that connection.

About the DRG and Redundant Connections

When you connect your on-premises network to a virtual cloud network (VCN) in Oracle Cloud Infrastructure, you use a dynamic routing gateway (DRG). A DRG is a virtual representation of highly available hardware (physical routers) on the edge of the Oracle Cloud Infrastructure network. You attach a DRG to the VCN, and the DRG is the termination point for the connections from your on-premises network to that VCN. If you have multiple VCNs in your tenancy, each has its own DRG. A VCN can be attached to only a single DRG, and a DRG can be attached to only a single VCN.

A single DRG can have multiple connections to it from your on-premises network, which allows redundancy. Those connections could be the same type or different types. Here are the two types:

- FastConnect
- VPN Connect

For example, you might use FastConnect, but also set up VPN Connect to use as backup when FastConnect is temporarily unavailable because of maintenance. Or, you might have two VPN tunnels, with one as primary and the second as failover.

For high availability, the multiple connections to a DRG must not terminate on a single physical router in Oracle's edge network. If they do, your overall connection to Oracle Cloud Infrastructure is disrupted whenever Oracle performs maintenance on that router.

How to Identify and Fix a Redundancy Issue

You might have a redundancy issue in which a DRG in your tenancy has multiple on-premises connections that terminate on a single physical Oracle router. Or you might have only a single connection with no redundancy.

If you do, the Console displays an alert message when you view the DRG's details, or when you view the details of one of the connections (for example, the IPSec connection). The alert message includes a link to one of the following topics, which explain how to fix the particular issue:

- Case 1: Multiple FastConnect virtual circuits
- Case 2: FastConnect and VPN Connect
- Case 3: Multiple IPSec connections
- Case 4: Single FastConnect virtual circuit
- Case 5: Single IPSec connection with only a single tunnel
**Redundancy Remedy: Case 1**

This topic describes one of several redundancy issues that you might be alerted to in the Console.

**Summary of the Issue**

You have redundant FastConnect virtual circuits that connect your on-premises network to a VCN. However, both of those virtual circuits terminate on the same Oracle edge router. Your connection to Oracle is at risk when routine maintenance is performed on that router.

Depending on your situation, there are two possible ways to fix the problem.

*If You Are Using an Oracle Partner*

The following diagram illustrates the issue.

**Before the fix:**

In this case, you have multiple FastConnect virtual circuits, each using a different Oracle partner (called X and Y in the diagram). Each partner has two physical connections to Oracle, and each goes to a different Oracle router (called A and B in the diagram).

The problem is that both virtual circuits happen to terminate on the same Oracle router (router A in the diagram).

**After the fix:**

To fix the problem, work with one of the partners to establish a new virtual circuit that goes to the *other* Oracle router (router B in the diagram). When that new secondary virtual circuit is up and running, delete the old secondary virtual circuit (in the diagram, the one on physical connection Y-A).

*If You Are Using a Third-Party Provider or Colocated with Oracle*

The following diagram illustrates the issue.

**Before the fix:**
In this case, you have two physical connections (*cross-connect groups*), and both go to the same Oracle router (router A in the diagram).

**After the fix:**

---
To fix the problem, one of your physical connections must go to a different router (B in the diagram). To do that, set up a new physical connect (cross-connect group) in the Oracle Console. During setup, specify the proximity of that connection to other FastConnect connections in that location. For example, the following image shows how to request that your secondary cross-connect group is created on a different router than your primary connection in that FastConnect location (called MyConnection-1).

After you’ve worked to set up the cabling in the data center, and the new secondary cross-connect group is up and running, you can create a new virtual circuit on that cross-connect group. When the virtual circuit is up and running, confirm that failover works between the primary and new secondary cross-connect group. Then you can terminate the old virtual circuit and old cross-connect group.

**Redundancy Remedy: Case 2**

This topic describes one of several redundancy issues that you might be alerted to in the Console.

**Summary of the Issue**

You have a FastConnect virtual circuit that connects your on-premises network to a VCN. For redundancy you use VPN Connect, but with only a single active IPSec tunnel. Both the FastConnect virtual circuit and the IPSec tunnel terminate on the *same* Oracle edge router. Your connection to Oracle is at risk when routine maintenance is performed on that router.

**How to Fix the Issue**

The following diagram illustrates the issue.
Before the fix:

In this case, you have a FastConnect virtual circuit and VPN Connect as backup. Notice that each VPN Connect consists of two IPSec tunnels, and Oracle automatically provisions each tunnel on a different Oracle router. However, you must configure your CPE so that both tunnels are up/active.

The problem is that:
- Only one of the two IPSec tunnels is up/active.
- The one IPSec tunnel that is up terminates on the same Oracle router as the virtual circuit.

Notice that some CPEs only support one IPSec tunnel being up/active to a given destination.

After the fix:

If your CPE supports having two IPSec tunnels up/active to the same destination, configure the second tunnel to also be up/active. Oracle recommends configuring them both to use BGP dynamic routing for the IPSec tunnels.

If your CPE supports only a single active IPSec tunnel to a given destination, configure the other IPSec tunnel to be up. Then switch the original IPSec tunnel to be down/inactive. The following diagram illustrates that setup. Also, if your CPE supports BGP dynamic routing, configure the tunnel to use it instead of static routing.
Redundancy Remedy: Case 3

This topic describes one of several redundancy issues that you might be alerted to in the Console.

Summary of the Issue

You have redundant VPN Connect connections that connect your on-premises network to a VCN. Although each connection consists of two IPSec tunnels, only one tunnel per connection is up/active, and both of those tunnels terminate on the same Oracle edge router. Your connection to Oracle is at risk when routine maintenance is performed on that router.

How to Fix the Issue

The following diagram illustrates the issue.

Before the fix:

In this case, you have a primary connection and a secondary connection as backup. Notice that each VPN Connect consists of two IPSec tunnels, and Oracle provisions each on a different Oracle router. However, you must configure your CPE so that both tunnels are up/active.

The problem has two parts:

- In each connection, only one of the two IPSec tunnels is up/active.
- Both of the tunnels that are up/active terminate on the same Oracle router.
Some CPEs only support one IPSec tunnel being up/active to a given destination.

After the fix:

If your CPE supports having two IPSec tunnels up/active to the same destination, configure the second tunnel to also be up/active. Oracle recommends configuring all tunnels to use BGP dynamic routing.

If your CPE supports only a single active IPSec tunnel to a given destination, then for one of the connections only, switch which of the two IPSec tunnels is configured to be up. The following diagram illustrates that setup. Oracle recommends configuring both tunnels to use BGP dynamic routing.

Redundancy Remedy: Case 4

This topic describes one of several redundancy issues that you might be alerted to in the Console.

Summary of the Issue

You use FastConnect to connect your on-premises network to a VCN. Although you might have multiple virtual circuits in this connection, only one of them is up (the BGP status is UP). Your connection to Oracle is at risk when routine maintenance is performed on the Oracle router.

You can fix the problem in one of two possible ways.

Option A: Use a Second Virtual Circuit

The details of the fix depend on your situation.
If You Are Using an Oracle FastConnect Partner

The following diagram illustrates the issue.

**Before the fix:**

![Diagram showing a single FastConnect virtual circuit up.]

In this case, you have only a single FastConnect virtual circuit that is up.

**After the fix:**

![Diagram showing two FastConnect virtual circuits up, each to a different Oracle router.]

After the fix, you have two FastConnect virtual circuits that are up, each to a different Oracle router. Some partners give you an option to specify which physical location to use for each virtual circuit. Other partners automatically use a different physical connection for the secondary virtual circuit.

If You Are Using a Third-Party Provider or Colocated with Oracle

The following diagram illustrates the issue.

**Before the fix:**

![Diagram showing a single virtual circuit to a third-party provider or colocated with Oracle.]

After the fix, you have two FastConnect virtual circuits that are up, each to a different Oracle router. Some partners give you an option to specify which physical location to use for each virtual circuit. Other partners automatically use a different physical connection for the secondary virtual circuit.
Networking

In this case, you have only a single FastConnect virtual circuit that is up.

**After the fix:**

To fix the problem, set up a secondary physical connection to Oracle. It must go to a different router (B in the diagram). To do that, set up a new physical connect (cross-connect group) in the Oracle Console. During setup, specify the proximity of that connection to other FastConnect connections in that location. For example, the following
Networking

image shows how to request that your secondary cross-connect group is created on a different router than your primary connection in that FastConnect location (called MyConnection-1).

After you've worked with the data center to have the cabling set up, and the new secondary cross-connect group is up and running, you can create a new virtual circuit on that cross-connect group. Confirm that failover works between the primary and new secondary cross-connect group.

Option B: Use VPN Connect with Both Tunnels Up/Active

This option is recommended if your CPE supports having two IPSec tunnels up/active to the same destination. The details of the fix depend on your situation.

If You Are Using an Oracle Partner

The following diagram illustrates the issue.

Before the fix:

In this case, you have only a single FastConnect virtual circuit that is up.

After the fix:
Here you set up VPN Connect as backup. You must configure your CPE so that both IPSec tunnels are up/active. Oracle automatically provisions each tunnel on a different Oracle router. Therefore, the secondary tunnel (to router B in the diagram) will be available when Oracle performs maintenance on the virtual circuit's router (router A in the diagram). Oracle recommends configuring both tunnels to use BGP dynamic routing.

If You Are Using a Third-Party Provider or Colocated with Oracle

The following diagram illustrates the issue.

Before the fix:

In this case, you have only a single FastConnect virtual circuit that is up.
After the fix:

Here you set up VPN Connect as backup. You must configure your CPE so that both IPSec tunnels are up/active. Oracle automatically provisions each tunnel on a different Oracle router. Therefore, the secondary tunnel (to router B in the diagram) will be available when Oracle performs maintenance on the virtual circuit's router (router A in the diagram). Oracle recommends configuring both tunnels to use BGP dynamic routing.

**Redundancy Remedy: Case 5**

This topic describes one of several redundancy issues that you might be alerted to in the Console.

**Summary of the Issue**

You use VPN Connect to connect your on-premises network to a VCN. Although Oracle provisions two IPSec tunnels for the connection, only one of them is up/active. Your connection to Oracle is at risk when routine maintenance is performed on the Oracle router.

**How to Fix the Issue**

The following diagram illustrates the issue.

**Before the fix:**

Notice that a VPN Connect consists of two IPSec tunnels, and Oracle automatically provisions each on a different Oracle router.

**After the fix:**
If your CPE supports having two IPSec tunnels up/active to the same destination, configure the second tunnel to also be up/active. Oracle recommends configuring both tunnels to use BGP dynamic routing.
Chapter 27

Notifications

This chapter explains how to use the Notifications service.

Notifications Overview

The Oracle Cloud Infrastructure Notifications service broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency and durable messages for applications hosted on Oracle Cloud Infrastructure and externally. Use Notifications to get notified when event rules are triggered or alarms are breached, or to directly publish a message.

How Notifications Works

The Notifications service enables you to set up communication channels for publishing messages using topics and subscriptions. When a message is published to a topic, the Notifications service sends the message to all of the topic's subscriptions.

When a subscriber's endpoint does not acknowledge receipt of the message, the Notifications service retries delivery. This situation can occur when the endpoint is offline. For example, the email server for an email address may be down.

Delivery retry details

Notifications retries delivery following these steps until either (a) acknowledgement is received or (b) the subscription's retry duration is over. By default, the retry duration is two hours.

1. Immediate retry.
2. Exponential backoff retry for the period of the subscription's retry duration, using the following timing:
   a. 1 minute
   b. 2 minutes
   c. 4 minutes
   d. 8 minutes
   e. 16 minutes
   f. 32 minutes
3. Discarding of the message at the end of the retry duration.

You can change the retry duration for a subscription. For instructions using the Console, see To update the retry duration for a subscription on page 3363. For the API, use the following operation: UpdateSubscription.

Notifications Concepts

The following concepts are essential to working with Notifications.

message

The content that is published to a topic. Each message is delivered at least once per subscription. Every message sent out as email contains a link to unsubscribe from the related topic.
**Friendly formatting**: Select friendly formatting to increase human readability of messages.

Supported subscription protocols:

- **Email**

Supported message types:

- Service connector messages (when Notifications is the target service)
  
  See service connector message examples and steps to select friendly formatting for existing service connectors.

subscription

An endpoint for a *topic*. Published *messages* are sent to each subscription for a *topic*.

Supported subscription protocols:

- **Email**:
  
  Sends an email message when you publish a *message* to the subscription's parent *topic*.
  
  Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.
  
  Some message types allow friendly formatting.

- **Function**:
  
  Runs the specified function when you publish a *message* to the subscription's parent *topic*. For example, runs a function to resize VMs when an associated alarm is triggered.

- **HTTPS (Custom URL)**:
  
  Sends specified information when you publish a *message* to the subscription's parent *topic*.

- **PagerDuty**:
  
  Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

- **Slack**:
  
  Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.
  
  Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

- **SMS**:
  
  Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: E.164 format.

  **Note:**
  
  SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service Connector Hub. SMS messages sent by unsupported services are dropped. Troubleshoot dropped messages.

  Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Available Countries and Regions

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Country or region</td>
<td>ISO code</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
</tbody>
</table>
topic

A communication channel for sending messages to the subscriptions in the topic. Each topic name is unique across the tenancy.

Note:
Messages sent out as email by the Oracle Cloud Infrastructure Notifications service are processed and delivered through Oracle resources in U.S.-based regions.

Flow of Message Publication

Notifications publishes messages when event rules are triggered, alarms are breached, service connectors run, or someone directly publishes a message.

Event rules

Notifications sends event messages when rules are triggered. The event message is sent to the topic specified in the rule. For example, a message might be configured for new databases. See Managing Rules for Events on page 1801.

Alarms

Notifications sends alarm messages when alarms are breached. The alarm message is sent to the topic specified in the alarm. For example, an alarm message might be configured for high CPU usage. See Managing Alarms on page 2719.

Service connectors

Notifications sends service connector messages when service connectors are running. The service connector message is sent to the topic specified in the service connector. For example, a service connector might be configured to send usage logs. See Managing Service Connectors on page 3754.
Notifications

Direct publication

Notifications sends *messages* when you (or a service or app) publish the messages directly. The message is sent to the *topic* you specify. See Publishing Messages on page 3365.

Availability

The Notifications service is available in all Oracle Cloud Infrastructure commercial regions. See About Regions and Availability Domains on page 180 for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

Service Comparison for Sending Email Messages

Consider the following service features when deciding whether to use the Notifications service or the Email Delivery service to send your email messages. For more information about Email Delivery, see Overview of the Email Delivery Service on page 1738.

<table>
<thead>
<tr>
<th>Service Feature</th>
<th>Notifications service</th>
<th>Email Delivery service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires confirmation before sending email.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Allows email decorations, such as signatures.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Allows raw email messages.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports MIME attachments.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports special handling for failed email delivery.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Priced for small messages (less than 32 KB, with a 64-KB limit).</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Service Feature

<table>
<thead>
<tr>
<th>Notifications service</th>
<th>Email Delivery service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priced for large messages (greater than 32 KB, with a 2-MB limit)</td>
<td>No</td>
</tr>
</tbody>
</table>

### Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

### Moving Topics and Subscriptions to a Different Compartment

You can move topics and subscriptions from one compartment to another. When you move a topic to a new compartment, its associated subscriptions remain in their existing compartment. The same consideration applies when moving a subscription: its associated topic remains in its existing compartment.

After you move the topic or subscription to the new compartment, inherent policies apply immediately and affect access to the moved topic or subscription through the Console. For more information, see To move a resource to a different compartment on page 2444.

**Important:**

To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Notifications resources, see Details for the Notifications Service on page 2322.

### Ways to Access Notifications

You can access the Notifications service using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

**Console:** To access Notifications using the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.

**API:** To access Notifications through API, use Notifications API.

### Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.
Administrators: For common policies that give groups access to Notifications, see Allow a group to manage topics on page 2158, Allow a group to manage topic subscriptions on page 2158, and Allow a group to publish messages to topics on page 2158.

## Limits on Notifications

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

### Limits for publishing messages (PublishMessage operation)

All limits are per tenancy.

<table>
<thead>
<tr>
<th>Limit type</th>
<th>Limit amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size per request</td>
<td>64KB</td>
</tr>
<tr>
<td>Message delivery rate per endpoint for HTTP-based protocols (endpoints that begin with &quot;http:&quot; or &quot;https:&quot;), Message delivery rate per endpoint for Email protocol</td>
<td>60 messages per minute</td>
</tr>
<tr>
<td>Messages per minute (also known as Transactions Per Minute, or TPM)</td>
<td>10 messages per minute</td>
</tr>
<tr>
<td>Messages per minute (also known as Transactions Per Minute, or TPM)</td>
<td>60 per topic</td>
</tr>
</tbody>
</table>

### Best Practices for Your Subscriptions and Topics

This topic covers best practices related to subscriptions and topics.

#### Prevent Processing of Duplicate Items

As depicted at Flow of Message Publication on page 3353, an event, alarm, or direct publication can trigger a message. The Notifications service then sends the message to many types of subscriptions, including email, HTTPS endpoints, and functions.

Depending on your goals, you may want to prevent your system from processing duplicate messages from a given message trigger. This situation is especially relevant when messages are sent to function subscriptions, which can result in double invocations. (For an example of a function subscription, see Scenario A: Automatically Resize VMs on page 3366.)

To prevent your system from processing duplicate messages, write code that de-duplicates received messages by using identifiers specific to the trigger:

- For any message, consider using a custom de-dupe key entered in the body of the message.
- For alarm-triggered messages, use a combination of dedupekey and timestampEpochMillis from the alarm message.
- For event-triggered messages, use eventID from the event message.
- For directly published messages, use x-oci-ns-messageid in the header (provided by Notifications).

For handling duplicate requests sent to Oracle Cloud Infrastructure API endpoints, see Retry Token on page 4372.

For related troubleshooting information, see Troubleshooting Notifications on page 3385.

### Managing Topics and Subscriptions

This section describes how to manage topics and their subscriptions.

A topic is a communication channel for sending messages to its subscriptions. A topic can have zero, one, or multiple subscriptions that are notified whenever a message is published to a topic.
Notifications

Prerequisites
IAM policies: To use Notifications, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. For Functions, you must have `FN_INVoke` permission against the function to be able to add the function as a subscription to a topic. To authorize your function for access to other Oracle Cloud Infrastructure resources, such as Compute instances, include the function in a dynamic group and create a policy to grant the dynamic group access to those resources. For more information, see Accessing Other Oracle Cloud Infrastructure Resources from Running Functions on page 2088.

If you get a response that you don’t have permission or are unauthorized, check with your administrator. You may not have the required type of access in the current compartment. For more information on user authorizations, see Notifications Overview on page 3350.

Creating Automation with Functions and Events
You can create automation by publishing messages to function subscriptions. For an example of a function subscription, see Scenario A: Automatically Resize VMs on page 3366.

You can create also automation based on state changes of your topics and subscriptions (Notifications resources) by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

Using the Console
To create a topic
1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Click Create Topic at the top of the topic list.
3. In the Create Topic dialog box, configure your topic.
   - Name: Required. Specify a friendly name for the topic. It must be unique across the tenancy; validation is case-sensitive. Avoid entering confidential information.
   - Description: Optional. Enter a description for the topic. Avoid entering confidential information.
4. Click Create.

To delete a topic
1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. For the topic you want to delete, click the Actions icon (three dots), and then click Delete.
3. Confirm when prompted.

To update the description for a topic
1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Click the name of the topic you want to update.
3. On the topic detail page, next to Description, click the edit icon.
4. Edit the description.
5. Click the save icon.

To move a topic to a different compartment
Associated subscriptions remain in their current compartments. For more information, see Moving Topics and Subscriptions to a Different Compartment on page 3355.

Note:
To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about
permissions for Notifications resources, see Details for the Notifications Service on page 2322.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. In the Scope section, select a compartment.
3. Find the topic in the list, click the Actions icon (three dots), and then click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.

**To create a subscription**

**Note:**
While new subscriptions must be created in the same compartment as the topic, you can move them to different compartments after creating them.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Click the name of the topic that you want to add the subscription to.
3. On the topic detail page, click Create Subscription.
4. In the Create Subscription dialog box, configure your subscription for the protocol you want:

   **Email subscription**
   Sends an email message when you publish a message to the subscription's parent topic.
   
   Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.
   
   Some message types allow friendly formatting.
   
   • **Protocol:** Select Email.
   • **Email:** Type an email address.

   **Function subscription**
   Runs the specified function when you publish a message to the subscription's parent topic. For example, runs a function to resize VMs when an associated alarm is triggered.

   **Note:**
   You must have FN_INVOCATION permission against the function to be able to add the function as a subscription to a topic.

   The Notifications service has no information about a function after it's invoked. For more details, see the troubleshooting information at Function not invoked or run on page 3387.
Confirmation is not required for function subscriptions.

- **Subscription Protocol**: Select Function.
- **Function Compartment**: Select the compartment containing your function.
- **Function Application**: Select the application containing your function.
- **Function**: Select your function.

**HTTPS (Custom URL) subscription**

Sends specified information when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL using HTTPS protocol):

```
https://<anyvalidURL>
```

Basic access authentication is supported, allowing you to specify a username and password in the URL, as in `https://user:password@domain.com` or `https://user@domain.com`. The username and
password are encrypted over the SSL connection established when using HTTPS. For more information about Basic Access Authentication, see RFC-2617.

Query parameters are not allowed in URLs.

- **Protocol**: Select HTTPS (Custom URL).
- **URL**: Type (or copy and paste) the URL you want to use as the endpoint.

**PagerDuty subscription**

Creates a PagerDuty incident by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://events.pagerduty.com/integration/<integrationkey>/enqueue
```

Query parameters are not allowed in URLs.

To create an endpoint for a PagerDuty subscription (set up and retrieve an integration key), see the PagerDuty documentation.

- **Protocol**: Select PagerDuty.
- **URL**: Type (or copy and paste) the *integration key* portion of the URL for your PagerDuty subscription. (The other portions of the URL are hard-coded.)

**Slack subscription**

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Message contents and appearance vary by message type. See alarm messages, event messages, and service connector messages.

Sends a message to the specified Slack channel by default when you publish a *message* to the subscription's parent *topic*.

Endpoint format (URL):

```
https://hooks.slack.com/services/<webhook-token>
```

The `<webhook-token>` portion of the URL contains two slashes (/).

Query parameters are not allowed in URLs.

To create an endpoint for a Slack subscription (using a webhook for your Slack channel), see the Slack documentation.

- **Protocol**: Select Slack.
- **URL**: Type (or copy and paste) the Slack endpoint, including your webhook token.

**SMS subscription**

Sends a text message using Short Message Service (SMS) to the specified phone number when you publish a *message* to the subscription's parent *topic*. Supported endpoint formats: E.164 format.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS subscriptions are enabled only for messages sent by the following Oracle Cloud Infrastructure services: Monitoring, Service Connector Hub.</td>
</tr>
</tbody>
</table>
SMS messages sent by unsupported services are dropped. **Troubleshoot dropped messages.**

Message contents and appearance vary by message type. See [alarm messages](#), [event messages](#), and [service connector messages](#).

**Available Countries and Regions**

You can use Notifications to send SMS messages to the following countries and regions:

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Czechia</td>
<td>CZ</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
</tbody>
</table>
### Notifications

<table>
<thead>
<tr>
<th>Country or region</th>
<th>ISO code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
</tbody>
</table>

- **Protocol**: Select SMS.
- **Country**: Select the country for the phone number.
- **Phone Number**: Enter the phone number, using E.164 format.

Example SMS endpoints:

- Phone Number (E.164 format): +14255550100

5. **Click Create**.

The subscription has been created.

Subscriptions using protocols that require confirmation, such as Email, remain in "Pending" status until confirmation is received. For these subscriptions, a subscription confirmation URL is sent. For detailed steps, see To confirm a subscription on page 3362.

### To confirm a subscription

Confirmation is not required for function subscriptions.

Navigate to the confirmation URL that is sent to the subscription's endpoint and follow the provided instructions.

Some protocols provide confirmation URLs in unique ways:

- **HTTPS (Custom URL)**: You can find the confirmation URL in the request header or body of the subscription confirmation message (request of content-type: "application/json") that is sent to the endpoint.

  - In the request header, see the value of the X-OCI-NS-ConfirmationURL field.

  **Example request header**:

  ```
  "X-OCI-NS-SignatureVersion":"1.0"
  "X-OCI-NS-Signature":"<example-signature>"
  "X-OCI-NS-SigningCertURL":"<example-url>"
  "X-OCI-NS-TopicOcid":"ocid.compartment.oc1..<unique_ID>"
  "X-OCI-NS-Timestamp":"2019-04-19T21:26:00.310+0000"
  "X-OCI-NS-MessageId":"<unique_ID>"
  "X-OCI-NS-TopicName":"mytopic"
  "X-OCI-NS-MessageType":"SubscriptionConfirmation"
  "X-OCI-NS-ConfirmationURL":"<exampleConfirmationURL>"
  "X-OCI-NS-SubscriptionId":"ocid1.onssubscription.oc1.phx.<unique_ID>"
  ```
Notifications

"X-OCI-NS-State":"Pending"

- In the request body, see the value of the ConfirmationURL key.

Example ConfirmationURL key and value (request body):

"ConfirmationURL":"<exampleConfirmationURL>"

- PagerDuty: Incident titled "Oracle Notification Service Subscription Confirmation". For more information, see the PagerDuty documentation for Oracle Cloud Infrastructure.

- Slack: Message sent to Slack channel containing the text "To confirm the subscription".

- SMS: Message sent to phone number containing the text "REPLY 'CONFIRM <short-topic-id>' to confirm subscription."

  <short-topic-id> is the short code of the topic that the SMS subscription was added to. The short code is used to identify the topic in messages sent to SMS subscriptions. Each short code contains six case-insensitive alphanumeric characters.

To resend a subscription confirmation

The ability to resend subscription confirmations is only applicable for pending subscriptions.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. For the subscription you want to resend the confirmation for, click the Actions icon (three dots), and then click Resend Confirmation.

To update the retry duration for a subscription

The retry duration is part of the delivery policy for the subscription. By default, Notifications retries delivery of a message for up to two hours.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. For the subscription you want to update, click the Actions icon (three dots), and then click Update Delivery Policy.
3. In the Update Delivery Policy dialog box, click the edit icon for Max Retry Duration in Minutes, type the new value, and then click the save icon.

To move a subscription to a different compartment

The associated topic remains in its current compartment. For more information, see Moving Topics and Subscriptions to a Different Compartment on page 3355.

Note:

To move resources between compartments, resource users must have sufficient access permissions on the compartment that the resource is being moved to, as well as the current compartment. For more information about permissions for Notifications resources, see Details for the Notifications Service on page 2322.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. In the Scope section, select a compartment.
3. Find the subscription in the list, click the Actions icon (three dots), and then click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.
To delete a subscription (unsubscribe)

Note:
Every message sent out as email contains a link to unsubscribe from the related topic.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. For the subscription you want to delete, click the Actions icon (three dots), and then click Delete.
3. Confirm when prompted.

Managing Tags for a Topic or Subscription

You can apply tags to your resources, such as topics and subscriptions, to help you organize them according to your business needs. You can apply tags at the time you create a topic or subscription, or you can update the topic or subscription later with the tags you want. For general information about applying tags, see Resource Tags on page 211.

To manage tags for a topic

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Choose the Compartment that contains the topic you want to tag, and then click the topic's name.
3. Click the Tags tab to view or edit existing tags, or click Add Tags to add new ones.

For more information, see Resource Tags on page 211.

To manage tags for a subscription

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Choose the Compartment that contains the subscription you want to tag, and then click the name of the topic that has the subscription.
3. For the subscription you want to tag, click the Actions icon (three dots), and then click Add Tags.
   To view or edit existing tags, click the Actions icon (three dots), and then click View Tags.

For more information, see Resource Tags on page 211.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage topics:

- CreateTopic
- GetTopic
- ListTopics
- UpdateTopic
- ChangeTopicCompartment
- DeleteTopic

Use these API operations to manage subscriptions:

- CreateSubscription
- GetSubscription
- ListSubscriptions
- UpdateSubscription
- ChangeSubscriptionCompartment
Publishing Messages

This topic describes how to publish messages directly using the Notifications service. You can manually enter the message content or allow a service or app to programmatically define the message content.

Each message is broadcast to all subscriptions in the specified topic. Every message sent out as email contains a link to unsubscribe from the related topic.

Message delivery rate limits per endpoint: 60 messages per minute for HTTP-based protocols. (HTTP-based protocols use URL endpoints that begin with "http:" or "https:".) 10 messages per minute for Email protocol.

Prerequisites

• IAM policies: To use Notifications, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a response that you don’t have permission or are unauthorized, check with your administrator. You may not have the required type of access in the current compartment. For more information on user authorizations, see Notifications Overview on page 3350.

• Before you can publish a message, you need a topic with at least one subscription. See Managing Topics and Subscriptions on page 3356.

Creating Automation with Functions and Events

You can create automation by publishing messages to function subscriptions. For an example of a function subscription, see Scenario A: Automatically Resize VMs on page 3366.

You can create also automation based on state changes of your topics and subscriptions (Notifications resources) by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

Using the Console

To publish a message

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. On the Topics page, for the topic you want, click the Actions icon (three dots), and then click Publish Message.
3. In the Publish Message dialog box, fill in the fields:

• Title: Enter the title you want to send.

Rendering of the title by protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the email message.</td>
</tr>
<tr>
<td>HTTPS (Custom URL)</td>
<td>Not rendered.</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Title field of the published message.</td>
</tr>
<tr>
<td>Slack</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>
Notifications

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Rendering of the title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>Not rendered.</td>
</tr>
</tbody>
</table>

- **Message**: Enter the content you want to send.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message size limit per request: 64KB.</td>
</tr>
</tbody>
</table>

4. Click **Publish**.

For troubleshooting information related to published messages, see *Message not received* on page 3386.

**Using the API**

For information about using the API and signing requests, see *REST APIs* on page 4368 and *Security Credentials* on page 179. For information about SDKs, see *Software Development Kits and Command Line Interface* on page 4225.

Use these API operations to publish messages:

- PublishMessage

**Scenarios**

Here are a few basic scenarios to help you understand the Notifications service and generally how the components work together.

- **Scenario A: Automatically Resize VMs** on page 3366
- **Scenario B: Send Alarm Messages to Slack and SMS** on page 3373

**Scenario A: Automatically Resize VMs**

This topic explains how to set up automatic resizing for virtual machines (VMs) that exceed memory.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoid entering confidential information when assigning descriptions, tags, or friendly names to your cloud resources through the Oracle Cloud Infrastructure Console, API, or CLI.</td>
</tr>
</tbody>
</table>

This scenario involves writing a **function** to resize VMs and creating an **alarm** that sends a message to that function. When the alarm fires, the Notifications service sends the **alarm message** to the destination topic, which then fans out to the topic's subscriptions. In this scenario, the topic’s subscriptions include the function as well as your email address and an SMS phone number. The function is invoked on receipt of the alarm message.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Notifications service has no information about a function after it's invoked. For more details, see the troubleshooting information at <em>Function not invoked or run</em> on page 3387.</td>
</tr>
</tbody>
</table>
Notifications

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Monitoring, Notifications, and Functions. You must have FN_INVOCATION permission against the function to be able to add the function as a subscription to a topic. To resize VMs, the function must be authorized to update Compute instances. To authorize your function for access to other Oracle Cloud Infrastructure resources, such as Compute instances, include the function in a dynamic group and create a policy to grant the dynamic group access to those resources. For more information, see Accessing Other Oracle Cloud Infrastructure Resources from Running Functions on page 2088.

Task 1: Create and Authorize Your Function

Once you create your function to resize VMs using your preferred SDK and authorize your function to access VMs (include the function in a dynamic group and grant that dynamic group access), all other scenario steps can be completed in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

For more information about authorizing functions to access other Oracle Cloud Infrastructure resources, see Accessing Other Oracle Cloud Infrastructure Resources from Running Functions on page 2088.

Function code sample

```
import io
import json
import oci
from fdk import response

def increase_compute_shape(instance_id, alarm_msg_shape):
    signer = oci.auth.signers.get_resource_principals_signer()
    compute_client = oci.core.ComputeClient(config={}, signer=signer)
    current_shape = compute_client.get_instance(instance_id).data.shape
    print("INFO: current shape for Instance {0}: {1}".format(instance_id,current_shape), flush=True)
    if current_shape != alarm_msg_shape:
        sign
```
Notifications

```python
def increase_compute_shape(instance_id, shape):
    # improve the logic below to handle more scenarios, make sure the shapes you select are available in the region and AD
    if current_shape == "VM.Standard1.1":
        new_shape = "VM.Standard2.1"
    elif current_shape == "VM.Standard2.1":
        new_shape = "VM.Standard2.2"
    else:
        return "Instance {0} cannot get a bigger shape than its current shape {1}".format(instance_id, current_shape)
    print("INFO: new shape for Instance {0}: {1}".format(instance_id, new_shape), flush=True)
    try:
        update_instance_details = oci.core.models.UpdateInstanceDetails(shape=new_shape)
        resp = compute_client.update_instance(instance_id=instance_id,
                                               update_instance_details=update_instance_details)
        print(resp, flush=True)
    except Exception as ex:
        print('ERROR: cannot update instance {}'.format(instance_id), flush=True)
        raise
    return "The shape of Instance {} is updated, the instance is rebooting...".format(instance_id)

def handler(ctx, data: io.BytesIO=None):
    alarm_msg = {}
    message_id = func_response = ""
    try:
        headers = ctx.Headers()
        message_id = headers["x-oci-ns-messageid"]
    except Exception as ex:
        print('ERROR: Missing Message ID in the header', ex, flush=True)
        raise
    print("INFO: Message ID = ", message_id, flush=True)
    # the Message Id can be stored in a database and be used to check for duplicate messages
    try:
        alarm_msg = json.loads(data.getvalue())
        print("INFO: Alarm message: ")
        print(alarm_msg, flush=True)
    except (Exception, ValueError) as ex:
        print(str(ex), flush=True)
    if alarm_msg["type"] == "OK_TO_FIRING":
        if alarm_msg["alarmMetaData"][0]["dimensions"]:
            alarm_metric_dimension = alarm_msg["alarmMetaData"][0]["dimensions"][0]  #assuming the first dimension matches the instance to resize
            print("INFO: Instance to resize: ", alarm_metric_dimension["resourceId"], flush=True)
            func_response = increase_compute_shape(alarm_metric_dimension["resourceId"],
                                                   alarm_metric_dimension["shape"])
        else:
            print('ERROR: There is no metric dimension in this alarm message', flush=True)
            func_response = "There is no metric dimension in this alarm message"
    else:
        print('INFO: Nothing to do, alarm is not FIRING', flush=True)
        func_response = "Nothing to do, alarm is not FIRING"
return func_response
```

Oracle Cloud Infrastructure User Guide
return response.Response(
    ctx,
    response_data=func_response,
    headers={"Content-Type": "application/json"}
)

Include your function in a dynamic group

Find and note your function OCID (format is ocid1.fnfunc.ocl.iad.exampleuniqueID), then specify the following rule in the relevant dynamic group:

```
resource.id = '<function-ocid>'
```

Create a policy to grant the dynamic group access to VMs (Compute instances)

Add the following policy:

```
allow dynamic-group <dynamic-group-name> to use instances in tenancy
```

Task 2: Create the alarm, topic, and subscriptions

You can create the alarm, topic, and subscriptions in the Console, CLI, or API.

Using the Console

This section walks through creating the alarm, topic, and subscriptions using the Console. Your function must be deployed.

Note:

Another workflow for this scenario involves creating your topic and subscriptions first, then selecting this topic when you create your alarm.

For help with troubleshooting, see Troubleshooting Notifications on page 3385.

Create the alarm, topic, and function subscription

This example walks through using the Console to create an alarm that sends a message to run the function when high memory usage is detected. During this process, you'll create a topic that references your function. You can add the SMS and email subscriptions later.

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. Click Create alarm.
3. On the Create Alarm page, under Define alarm, set up your threshold:

   - Metric description:
     - Compartment: (select the compartment that contains your VM)
     - Metric Namespace: oci_computeagent
     - Metric Name: MemoryUtilization
     - Interval: 1m
     - Statistic: Max
   - Trigger rule:
     - Operator: greater than
     - Value: 90
     - Trigger Delay Minutes: 1
4. Select your function under **Notifications, Destinations**:
   - **Destination Service**: Notifications Service
   - **Compartment**: (select the *compartment* where you want to create the topic and associated subscriptions)
   - **Topic**: Click **Create a topic**

   **Note:**
   If you already created your topic and function subscription, you can select that topic here instead of creating a new one.

   - **Topic Name**: Alarm Topic
   - **Subscription Protocol**: Function
   - **Function Compartment**: (select the *compartment* that contains your function)
   - **Function Application**: (select the application that contains your function)
   - **Function**: (select your function)

5. Click **Save alarm**.

Add an SMS subscription

This example walks through using the Console to add an SMS subscription to the topic you created when you set up the alarm.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.
2. Click the name of the topic that you want to add the subscription to.
3. On the topic detail page, click **Create Subscription**.
4. In the **Create Subscription** dialog box, set up your SMS subscription:
   - **Protocol**: Select SMS.
   - **Country**: Select the country for the phone number.
   - **Phone Number**: Enter the phone number, using E.164 format.

   Example SMS endpoints:
   - **Phone Number (E.164 format)**: +14255550100

5. Click **Create**.

   The SMS subscription has been created and a subscription confirmation message is sent to the specified phone number. The subscription remains in "Pending" status until it has been confirmed.

6. To confirm your new SMS subscription, follow the instructions in the received confirmation message. (Look for the message containing the phrase "REPLY 'CONFIRM" followed by your topic name.)

Add an email subscription (optional)

This example walks through using the Console to add an optional email subscription to the topic you created when you set up the alarm.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.
2. Click the name of the topic that you want to add the subscription to.
3. On the topic detail page, click **Create Subscription**.
4. In the **Create Subscription** dialog box, set up your email subscription:
   - **Protocol**: Select Email.
   - **Email**: Type an email address.
5. Click Create.
   The email subscription has been created and a subscription confirmation URL is sent to the specified email
   address. The subscription remains in "Pending" status until it has been confirmed.

6. To confirm your new email subscription, open your email and navigate to the confirmation URL.

Using the CLI

This section walks through creating the topic, subscriptions, and alarm using the CLI. Your function must be
deployed.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on
page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

1. Create the topic
   Open a command prompt and run the oci ons topic create command:
   
   ```shell
   oci ons topic create --name "Alarm Topic" --compartment-id "<compartment-ocid>"
   ```

2. Add the subscriptions
   To this topic, add subscriptions referencing your function OCID, an SMS phone number, and an optional email
   address.
   
   • Create a function subscription: Open a command prompt and run the oci ons subscription create command:
     
     ```shell
     oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "ORACLE_FUNCTIONS" --subscription-endpoint "<function-ocid>"
     ```
   
   • Create an SMS subscription: Open a command prompt and run the oci ons subscription create command:
     
     ```shell
     oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "SMS" --subscription-endpoint "<sms-endpoint>"
     ```
   
   • Create an email subscription (optional): Open a command prompt and run the oci ons subscription create command:
     
     ```shell
     oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "EMAIL" --subscription-endpoint "john.smith@example.com"
     ```

3. Create the alarm
   Create an alarm that defines the memory threshold and references this topic as the destination: Open a command
   prompt and run the oci monitoring alarm create command:
   
   ```shell
   oci monitoring alarm create --display-name "VM Memory Alarm" --compartment-id "<compartment-ocid>" --metric-compartment-id "<compartment-ocid>" --metric-name "oci_computeagent" --query-text "MemoryUtilization[1m].max() > 90" --severity "CRITICAL" --destinations "<topic-ocid>" --is-enabled true
   ```

For help with troubleshooting, see Troubleshooting Notifications on page 3385.

Using the API

This section walks through creating the topic, subscriptions, and alarm using the API. Your function must be
deployed.
Notifications

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:

1. **CreateTopic**: Create a topic.

   **Example CreateTopic request**

   ```
   POST /20181201/topics
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
     "name": "Alarm Topic",
     "compartmentId": "<compartment_OCID>"
   }
   ```

2. **CreateSubscription**: To this topic, add subscriptions referencing your function OCID, SMS phone number, and an optional email address.

   **Example CreateSubscription request: Function**

   ```
   POST /20181201/subscriptions
   Host: cp.notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
     "topicId": "<topic_OCID>",
     "compartmentId": "<compartment_OCID>",
     "protocol": "ORACLE_FUNCTIONS",
     "endpoint": "<function_OCID>"
   }
   ```

   **Example CreateSubscription request: SMS**

   ```
   POST /20181201/subscriptions
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
     "topicId": "<topic_OCID>",
     "compartmentId": "<compartment_OCID>",
     "protocol": "SMS",
     "endpoint": "<sms-endpoint>"
   }
   ```

   **Example CreateSubscription request: Email**

   ```
   POST /20181201/subscriptions
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
     "topicId": "<topic_OCID>",
     "compartmentId": "<compartment_OCID>",
     "protocol": "EMAIL",
     "endpoint": "john.smith@example.com"
   }
   ```

3. **CreateAlarm**: Create an alarm that defines the memory threshold and references this topic.

   **Example CreateAlarm request**

   ```
   POST /20180401/alarms
   Host: telemetry.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
   }
   ```
Notifications

```
"displayName": "VM Memory Alarm",
"compartmentId": "<compartment_OCID>",
"metricCompartmentId": "<compartment_OCID>",
"namespace": "oci_computeagent",
"query": "MemoryUtilization[1m].max() > 90",
"severity": "CRITICAL",
"destinations":
[
   "<topic_OCID>
],
"isEnabled": true
}
```

For help with troubleshooting, see Troubleshooting Notifications on page 3385.

**Scenario B: Send Alarm Messages to Slack and SMS**

This topic explains how to set up automatic notifications to a Slack channel and an SMS phone number when alarms are triggered.

**Caution:**

Avoid entering confidential information when assigning descriptions, tags, or friendly names to your cloud resources through the Oracle Cloud Infrastructure Console, API, or CLI.

This scenario involves setting up a Slack endpoint for a channel and creating an alarm that sends a message to both that channel and an SMS phone number. When the alarm fires, the Notifications service sends the alarm message to the destination topic, which then fans out to the topic's subscriptions. In this scenario, the topic's subscriptions include the Slack channel and SMS phone number as well as your email address.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Monitoring and Notifications.

**Task 1: Set up your Slack endpoint**

Create an incoming webhook to your Slack app.

Example of an incoming webhook to a Slack app (equivalent to the Slack endpoint for your subscription): `https://hooks.slack.com/services/T00000000/B0000000/XXXXXXXXXXXXXXXXXXXXXXXX`

Once you set up your Slack endpoint, you can complete all other scenario steps in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.
**Task 2: Create the alarm, topic, and subscriptions**

You can create the alarm, topic, and subscriptions in the Console, CLI, or API.

*Using the Console*

This section walks through creating the alarm, topic, and subscriptions using the Console.

**Note:**

Another workflow for this scenario involves creating your topic and subscriptions first, then selecting this topic when you create your alarm.

For help with troubleshooting, see *Troubleshooting Notifications* on page 3385.

Create the alarm, topic, and Slack subscription

This example walks through using the Console to create an alarm that sends a message to Slack when a high CPU usage is detected. During this process, you'll create a topic that references your Slack channel (Slack endpoint, including the webhook token). You can add the SMS and email subscriptions later.

1. Open the navigation menu. Under *Solutions and Platform*, go to *Monitoring* and click *Alarm Definitions*.
2. Click *Create alarm*.
3. On the *Create Alarm* page, under *Define alarm*, set up your threshold:
   - **Metric description**:
     - **Compartment**: (select the *compartment* that contains your VM)
     - **Metric Namespace**: `oci_computeagent`
     - **Metric Name**: `CpuUtilization`
     - **Interval**: `1m`
     - **Statistic**: `Count`
   - **Trigger rule**:
     - **Operator**: `greater than`
     - **Value**: `90`
     - **Trigger Delay Minutes**: `1`
4. Add your Slack endpoint under *Notifications, Destinations*:
   - **Destination Service**: *Notifications Service*
   - **Compartment**: (select the *compartment* where you want to create the topic and associated subscriptions)
   - **Topic**: Click *Create a topic*
     **Note:**
     If you already created your topic and Slack subscription, you can select that topic here instead of creating a new one.
     - **Topic Name**: Alarm Topic
     - **Subscription Protocol**: Slack
     - **URL**: Your Slack endpoint, including the webhook token.
5. Click *Save alarm*.
6. Confirm your new Slack subscription: Navigate to the confirmation URL that is sent to the Slack channel. (Look for the message containing the phrase "To confirm the subscription".)

Add an SMS subscription

This example walks through using the Console to add an SMS subscription to the topic you created when you set up the alarm.

1. Open the navigation menu. Under *Solutions and Platform*, go to *Application Integration* and click *Notifications*.
2. Click the name of the topic that you want to add the subscription to.
   
   Example: "Alarm Topic" (assuming you used the suggested topic name when creating the topic in the alarm).

3. On the topic detail page, click Create Subscription.

4. In the Create Subscription dialog box, set up your SMS subscription:
   
   - **Protocol**: Select SMS.
   - **Country**: Select the country for the phone number.
   - **Phone Number**: Enter the phone number, using E.164 format.

   Example SMS endpoints:
   
   - Phone Number (E.164 format): +14255550100

5. Click Create.
   
   The SMS subscription has been created and a subscription confirmation message is sent to the specified phone number. The subscription remains in "Pending" status until it has been confirmed.

6. To confirm your new SMS subscription, follow the instructions in the received confirmation message. (Look for the message containing the phrase "REPLY CONFIRM" followed by your topic name.)

Add an email subscription (optional)

This example walks through using the Console to add an optional email subscription to the topic you created when you set up the alarm.

1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.

2. Click the name of the topic that you want to add the subscription to.

   Example: "Alarm Topic" (assuming you used the suggested topic name when creating the topic in the alarm).

3. On the topic detail page, click Create Subscription.

4. In the Create Subscription dialog box, set up your email subscription:

   - **Protocol**: Select Email.
   - **Email**: Type an email address.

5. Click Create.

   The email subscription has been created and a subscription confirmation URL is sent to the specified email address. The subscription remains in "Pending" status until it has been confirmed.

6. To confirm your new email subscription, open your email and navigate to the confirmation URL.

Using the CLI

This section walks through creating the topic, subscriptions, and alarm using the CLI.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

1. **Create the topic**

   Open a command prompt and run the oci ons topic create command:

   ```bash
   oci ons topic create --name "Alarm Topic" --compartment-id "<compartment-ocid>"
   ```
2. **Add the subscriptions**

To the topic you just created in the previous step, add subscriptions referencing your Slack endpoint (including the webhook token) and an optional email address and SMS phone number.

- **Create a Slack subscription:** Open a command prompt and run the `oci ons subscription create` command:

  ```bash
  oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "SLACK" --subscription-endpoint "<slack-endpoint>"
  ```

- **Create an SMS subscription:** Open a command prompt and run the `oci ons subscription create` command:

  ```bash
  oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "SMS" --subscription-endpoint "<sms-endpoint>"
  ```

- **Create an email subscription (optional):** Open a command prompt and run the `oci ons subscription create` command:

  ```bash
  oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "EMAIL" --subscription-endpoint "john.smith@example.com"
  ```

3. **Create the alarm**

Create an alarm that defines the CPU threshold and references this topic as the destination: Open a command prompt and run the `oci monitoring alarm create` command:

```bash
oci monitoring alarm create --display-name "VM Memory Alarm" --compartment-id "<compartment-ocid>" --metric-compartment-id "<compartment-ocid>" --namespace "oci_computeagent" --query-text "CPUUtilization[1m].count() > 90" --severity "CRITICAL" --destinations "<topic-ocid>" --is-enabled true
```

For help with troubleshooting, see Troubleshooting Notifications on page 3385.

**Using the API**

This section walks through creating the topic, subscriptions, and alarm using the API.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:

1. **CreateTopic:** Create a topic.

   **Example CreateTopic request**

   ```
   POST /20181201/topics
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
   "name": "Alarm Topic",
   "compartmentId": "<compartment_OCID>"
   }
   ```
2. **CreateSubscription**: To this topic, add subscriptions referencing your Slack channel and optionally your email address and SMS phone number.

**Example CreateSubscription request: Slack**

```plaintext
POST /20181201/subscriptions
Host: notification.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
  "topicId": "<topic_OCID>",
  "compartmentId": "<compartment_OCID>",
  "protocol": "SLACK",
  "endpoint": "<slack-endpoint>
}
```

**Example CreateSubscription request: SMS**

```plaintext
POST /20181201/subscriptions
Host: notification.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
  "topicId": "<topic_OCID>",
  "compartmentId": "<compartment_OCID>",
  "protocol": "SMS",
  "endpoint": "<sms-endpoint>
}
```

**Example CreateSubscription request: Email**

```plaintext
POST /20181201/subscriptions
Host: notification.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
  "topicId": "<topic_OCID>",
  "compartmentId": "<compartment_OCID>",
  "protocol": "EMAIL",
  "endpoint": "john.smith@example.com"
}
```

3. **CreateAlarm**: Create an alarm that defines the CPU threshold and references this topic.

**Example CreateAlarm request**

```plaintext
POST /20180401/alarms
Host: telemetry.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
  "displayName": "CPU Alarm",
  "compartmentId": "<compartment_OCID>",
  "metricCompartmentId": "<compartment_OCID>",
  "namespace": "oci_computeagent",
  "query": "CPUUtilization[1m].count() > 90",
  "severity": "CRITICAL",
  "destinations":
  ["<topic_OCID>"],
  "isEnabled": true
}
```

For help with troubleshooting, see [Troubleshooting Notifications](#) on page 3385.
Scenario C: File Jira Tickets for Reminders

This topic explains how to file automatic Jira tickets whenever maintenance reminder events occur. In this scenario, whenever a reminder for upcoming database maintenance comes from Oracle Cloud Infrastructure, a Jira ticket is created for your on-call engineer.

This scenario involves writing a function to file Jira tickets (and creating a secret to store your Jira credentials), adding that function and optional email as subscriptions to a topic, and creating a rule that sends messages to that topic when maintenance reminder events occur (see Database Service: Autonomous Container Database Event Types on page 1849). The message fans out to the topic's subscriptions, which includes a group email address in addition to the function. The function is invoked on receipt of the message.

Everything but the function can be set up in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

Note:
The Notifications service has no information about a function after it's invoked. For more details, see the troubleshooting information at Function not invoked or run on page 3387.

For more information about this scenario, see Automated Jira Ticketing using OCI Events, Notifications, and Functions and the associated GitHub repository.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Events, Notifications, and Functions. You must have FN_INVOCATION permission against the function to be able to add the function as a subscription to a topic. To access your Jira credentials, the function must be authorized to read secrets. This scenario walks through steps to provide this authorization.

Task 1: Store your Jira credentials in a secret

You can create a secret in the Console, CLI, or API. You'll reference this secret later, when creating your function.
**Using the Console**

**To create the secret for your Jira credentials**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment where you want to create a secret.
3. From the list of vaults in the compartment, do one of the following:
   - Click the name of the vault where you want to create a secret.
   - Create a new vault for the secret by following the instructions in **To create a new vault**, and then click the name of the vault.
4. Click **Secrets**, and then click **Create Secret**.
5. In the **Create Secret** dialog box, choose a compartment from the **Create in Compartment** list. (Secrets can exist outside the compartment the vault is in.)
6. Click **Name**, and then enter a name to identify the secret. Avoid entering confidential information.
   
   Example name: `jira_auth_plain_text`

7. Click **Description**, and then enter a brief description of the secret to help identify it. Avoid entering any confidential information in this field.
   
   Example description: `jira_auth_plain_text`

8. Choose the master encryption key that you want to use to encrypt the secret contents while they're imported to the vault. (The key must belong to the same vault.)
9. For **Secret Type Template**, select **Plain-Text**.
10. Click **Secret Contents**, and then enter your Jira credentials in the following format, with a colon separating your login email from your auth token:

    `<your-jira-cloud-login-email>:<your-jira-cloud-auth-token>`

11. Click **Create Secret**.
12. Note the secret **OCID** for use in your function code to securely fetch the secret.

For more information about creating secrets using the Vault service, see **To create a new secret** on page 4008.

**Using the CLI**

**To create the secret using the CLI**

Create a secret storing your Jira credentials: Open a command prompt and run the `oci vault secret create-base64` command:

```
oci vault secret create-base64 --compartment-id <compartment_OCID>  
--secret-name <secret_name> --vault-id <vault_OCID> --  
description <secret_description_text> --key-id <encryption_key_OCID> --  
secret-content-content <base64_encoded_secret_content> --secret-content-  
name <unique_content_name>
```

Avoid entering confidential information.

For more information about managing secrets using the CLI, see **Using the Command Line Interface (CLI)** on page 4013.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the **CreateSecret** operation.

**Example CreateSecret request**

```
POST /20180608/secrets
Host: <managementEndpoint>
<authorization and other headers>
```
Notifications

{ "vaultId": "<vault_OCID>",
"compartmentId": "<compartment_OCID>",
"secretName": "jira_auth_plain_text",
"description": "jira_auth_plain_text",
"keyId": "<key_OCID>",
"secretContent": {
   "content": "<base64_encoded_secret_contents>",
   "contentType": "BASE64"
}
}

For more information about managing secrets using the API, see Using the API on page 4018.

**Task 2: Create the function**

This section provides the code sample for creating your function and covers steps to authorize the function to access your Jira credentials in the secret created using the Vault service.

**Function code sample**

The following code sample is for a function to file Jira tickets.

Add your secret OCID in the line that includes `getSecretForOcid`.

For instructions on creating and deploying functions, see Creating and Deploying Functions on page 2063.

```java
public String handleRequest(CloudEvent cloudEvent) {
   // Json body of Cloud event from Oracle Event Service in serialized into
   // cloudEvent object by Fn SDK implicitly
   System.err.println("Inside Java jira function with input as " +
   cloudEvent.getEventType() + " +
   cloudEvent.getData().getResourceName());

   String response = jiraCreateTicket(cloudEvent);
   if (response != null) return response;
   return null;
}

private String jiraCreateTicket(CloudEvent cloudEvent) {
   try {
      //create jira ticket body as per CloudEvent
      String jsonBodyJira = getJiraApiBody(cloudEvent);

      String jiraCloudEndpoint = System.getenv().get("JIRA_CLOUD_URL");
      String ocidForSecretForJiraAuthToken =
      System.getenv().get("JIRA_CLOUD_SECRET_OCID");
      String jiraAuthToken =
      getSecretForOcid(ocidForSecretForJiraAuthToken); // base64 encoded form of
      <YourJiraUsername:YourJiraAuthToken>

      // actual REST call to JIRA cloud
      OkHttpClient client = new OkHttpClient().newBuilder()
         .build();
      MediaType mediaType = MediaType.parse("application/json");
      RequestBody body = RequestBody.create(mediaType, jsonBodyJira);
      Request request = new Request.Builder()
         .url(jiraCloudEndpoint)
         .method("POST", body)
         .addHeader("Accept", "application/json")
         .addHeader("Content-Type", "application/json")
      
   } catch (

```
.addHeader("Authorization", "Basic " + jiraAuthToken)
    .build();
    Response response = client.newCall(request).execute();
    return response.body().string();
}

return null;

**Authorize your function to access secrets**

Use a dynamic group to grant your function the ability to read secrets. Your function must have this authorization to access your Jira credentials, which are stored in the secret you created earlier.

**To authorize your function to access secrets (Console)**

1. Find and note your function **OCID** (format is ocid1.fnfunc.ocl.iad.exampleuniqueID).
2. Include your function in a dynamic group: In the relevant **dynamic group**, specify the following rule:

   ```
   resource.id = '<function-ocid>'
   ```

   Alternatively, you can create a dynamic group that includes all functions:

   ```
   ALL{resource.type='fnfunc', resource.compartment.id='<compartment_OCID>'}
   ```

3. Grant the dynamic group access to secrets: Add the following **policy**:

   ```
   allow dynamic-group <dynamic-group-name> to read secret-family in tenancy
   ```

To authorize your function for access to other Oracle Cloud Infrastructure resources, such as Compute instances, include the function in a dynamic group and create a policy to grant the dynamic group access to those resources. For more information, see [Accessing Other Oracle Cloud Infrastructure Resources from Running Functions](#).

For more information about dynamic groups, see [Managing Dynamic Groups](#).

**Task 3: Create the topic, subscriptions, and rule**

This section walks through creating a topic, adding your function and optional email as subscriptions, and creating the rule that sends a message whenever the Database service emits an event for a database maintenance reminder. Your function must be deployed.

Everything can be set up in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

For more information about managing topics and subscriptions, see [Managing Topics and Subscriptions](#). For more information about managing rules, see [Managing Rules for Events](#).

**Using the Console**

To create the topic

This section walks through creating the topic you'll use for the subscriptions and rule.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.
2. Click **Create Topic** at the top of the topic list.
3. In the **Create Topic** dialog box, configure your topic.

   • **Name**: Required. Specify a friendly name for the topic. It must be unique across the tenancy; validation is case-sensitive. Avoid entering confidential information.
     
     Example: Maintenance Topic
   
   • **Description**: Optional. Enter a description for the topic. Avoid entering confidential information.

4. Click **Create**.

   For help with troubleshooting, see *Troubleshooting Notifications* on page 3385.

**To create the function subscription**

This section walks through adding your function as a subscription to the topic. Your function must be deployed.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.

2. Click the name of the topic that you want to add the subscription to.

   Example: "Maintenance Topic" (assuming you used the suggested topic name when creating the topic).

3. On the topic detail page, click **Create Subscription**.

4. In the **Create Subscription** dialog box, configure your function subscription:

   **Note:**

   The function must be deployed. You must have **FN_INVOCATION** permission against the function to be able to add the function as a subscription to a topic.

   The Notifications service has no information about a function after it's invoked. For more details, see the troubleshooting information at *Function not invoked or run* on page 3387.

   Confirmation is not required for function subscriptions.

   • **Subscription Protocol**: Select **Function**.

   • **Function Compartment**: Select the compartment containing your function.

   • **Function Application**: Select the application containing your function.

   • **Function**: Select your function.

5. Click **Create**.

   The subscription has been created.

   For help with troubleshooting, see *Troubleshooting Notifications* on page 3385.

**To create an email subscription**

This section walks through adding an optional email subscription to your topic.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.

2. Click the name of the topic that you want to add the subscription to.

   Example: "Maintenance Topic" (assuming you used the suggested topic name when creating the topic).

3. On the topic detail page, click **Create Subscription**.

4. In the **Create Subscription** dialog box, set up your email subscription:

   • **Protocol**: Select **Email**.

   • **Email**: Type an email address.

5. Click **Create**.

   The email subscription has been created and a subscription confirmation URL is sent to the specified email address. The subscription remains in "Pending" status until it has been confirmed.
6. To confirm your new email subscription, open your email and navigate to the confirmation URL.
   For more information, see To confirm a subscription on page 3362.

   For help with troubleshooting, see Troubleshooting Notifications on page 3385.

To create the rule

This section walks through creating the rule that sends a message to the topic whenever the Database service emits an event for a database maintenance reminder.

1. Open the navigation menu. Under the Solutions and Platform group, go to Application Integration and click Events Service.
2. Choose a Compartment you have permission to work in, and then click Create Rule.

   Events compares the rules you create in this compartment to event messages emitted from resources in this compartment and any child compartments.
3. Enter the following.
   • Display Name: Specify a friendly name for the rule. You can change this name later. Avoid entering confidential information.
     Example: Maintenance Reminder
   • Description: Specify a description of what the rule does. You can change this description later. Avoid entering confidential information.
     Example: Sends messages to Maintenance Topic
4. In Rule Conditions, create a filter for database reminder events:
   • For Service Name, select Database.
   • In Event type, select Autonomous Container Database – Maintenance Reminder.
5. In Actions, select the topic you previously created:
   a. Select Notifications.
   b. Select the Notifications Compartment.
   c. Select the Topic that you previously created.
6. Click Create Rule.

Using the CLI

This section walks through creating the topic, subscriptions, and rule using the CLI. Your function must be deployed.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

1. Create the topic

   Open a command prompt and run the oci ons topic create command:

   ```bash
   oci ons topic create --name "Maintenance Topic" --compartment-id "<compartment-ocid>"
   ```
2. **Add the subscriptions**

To the topic you just created in the previous step, add subscriptions referencing your function **OCID** and an optional email address.

- Create a function subscription: Open a command prompt and run the `oci ons subscription create` command:

  ```bash
  oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "ORACLE_FUNCTIONS" --subscription-endpoint "<function-ocid>
  ```

- Create an email subscription: Open a command prompt and run the `oci ons subscription create` command:

  ```bash
  oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "EMAIL" --subscription-endpoint "maintenance.team@example.com"
  ```

3. **Create the rule**

Create a rule that is triggered by maintenance reminders and references this topic as the destination:

- Create a file, **action.json**, that contains the following, referencing your topic created previously:

  ```json
  {
  "actions": [
  {
  "actionType": "ONS",
  "description": "string",
  "isEnabled": true,
  "topicId": "<topic_OCID>"
  }
  ]
  }
  ```

- Open a command prompt and run the `oci events rule create` command:

  ```bash
  oci events rule create --display-name <friendly_name> --is-enabled true --condition "{"eventType": ["com.oraclecloud.databaseservice.autonomous.container.database.maintenance.reminder"]}" --compartment-id <compartment_OCID> --actions file://action.json
  ```

For more information about creating rules using the CLI, see To create a rule on page 1811.

For help with troubleshooting, see Troubleshooting Notifications on page 3385.

**Using the API**

This section walks through creating the topic, subscriptions, and rule using the API. Your function must be deployed.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:

1. **CreateTopic**: Create a topic.

   **Example CreateTopic request**

   ```
   POST /20181201/topics
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
   "name": "Maintenance Topic",
   "compartmentId": "<compartment_OCID>"
   }
   ```
2. **CreateSubscription**: To this topic, add subscriptions referencing your function OCID and an optional email address.

**Example CreateSubscription request: Function**

```
POST /20181201/subscriptions
Host: notification.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
    "topicId": "<topic_OCID>",
    "compartmentId": "<compartment_OCID>",
    "protocol": "ORACLE_FUNCTIONS",
    "endpoint": "<function_OCID>"
}
```

**Example CreateSubscription request: Email**

```
POST /20181201/subscriptions
Host: notification.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
    "topicId": "<topic_OCID>",
    "compartmentId": "<compartment_OCID>",
    "protocol": "EMAIL",
    "endpoint": "maintenance.team@example.com"
}
```

3. **CreateRule**: Create a rule that is triggered by maintenance reminders and references this topic as the destination.

**Example CreateRule request**

```
POST /20181201/rules
Host: events.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
    "displayName": "Maintenance Reminder",
    "condition": {
        "eventType": "com.oraclecloud.databaseservice.autonomous.container.database.maintenance.reminder",
        "compartmentId": "<compartment_OCID>",
        "isEnabled": true,
        "actions": [
            {
                "actionType": "ONS",
                "topicId": "<topic_OCID>",
                "isEnabled": true
            }
        ]
    }
}
```

For help with troubleshooting, see [Troubleshooting Notifications](#) on page 3385.

**Troubleshooting Notifications**

This topic covers troubleshooting techniques for Notifications.
Message not received

Tip:
Assess alarms and messages using their unique identifiers. See Prevent Processing of Duplicate Items on page 3356. To view the format used by alarm messages, see Message format and examples on page 2661.

Check these items:

• **Alarm firing transition:** If the message is a result of a firing alarm, then view the history of the alarm. Note times for any transition to a firing state. You'll use noted times for comparison to metrics for your topic ("Publication and delivery").

To view history for your alarm
1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Alarm Definitions.
2. On the Alarm Definitions page, click the alarm that you want to view history for.
3. Adjust the time range by selecting from Quick Selects or changing the Start Time and End Time.

• **Publication and delivery:** Note times for messages published to your topic as well as messages delivered to your topic. Compare to times of the firing alarm or other inciting incident.

To view timing of published and delivered messages for your topic
1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Choose the Compartment that contains your topic, and then click the topic's name.
3. In the Resources menu, click Metrics.
   
   The Metrics page displays a chart for each metric that is emitted by the metric namespace for Notifications. For more information about the emitted metrics, see Available Metrics: oci_notification on page 3389.
4. Adjust the time range by selecting from Quick Selects or changing the Start Time and End Time.
5. Review the following metric charts:
   - Published Messages Total Count
   - Delivered Messages Count

• **Service permissions (alarm messages):** If your topic is in an Oracle Platform Services managed compartments (named "ManagedCompartmentForPaas"), then the Monitoring service may not have permissions to use it, and alarm messages sent to that topic may not be received. For more details, including steps for resolution, see Alarm Messages are not Received in Oracle Platform Services Managed Compartments.

• **Unsupported method used to send messages:** Confirm that the method you used to send messages is supported for the subscription protocols used by the topic. Messages sent by unsupported methods are dropped, as indicated by data points in the Failed Messages Count metric chart.

   The value of the metric dimension endpointType corresponds to the subscription protocol. For example, if you attempt to send an SMS message through an unsupported method, then the message is dropped and the counter of this metric chart is increased, with the corresponding data point showing an endpointType value of SMS.

To view dropped messages for your topic
1. Open the navigation menu. Under Solutions and Platform, go to Application Integration and click Notifications.
2. Choose the Compartment that contains your topic, and then click the topic's name.
3. In the Resources menu, click Metrics.
   
   The Metrics page displays a chart for each metric that is emitted by the metric namespace for Notifications. For more information about the emitted metrics, see Available Metrics: oci_notification on page 3389.
4. Adjust the time range by selecting from Quick Selects or changing the Start Time and End Time.
5. Review the Failed Messages Count metric chart.
Function not invoked or run

This section provides troubleshooting information for function subscriptions. For an example function subscription, see Scenario A: Automatically Resize VMs on page 3366.

**Note:**
The Notifications service has no information about a function after it's invoked.

**Tip:**
Assess alarms and messages using their unique identifiers. See Prevent Processing of Duplicate Items on page 3356. To view the format used by alarm messages, see Message format and examples on page 2661.

Check these items:

- **Message receipt:** See Message not received on page 3386.
• **Function invocation:** Note times for invocations of your function. Compare to times of the firing alarm or other inciting incident.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this is the first invocation, response may be delayed.</td>
</tr>
</tbody>
</table>

**To view timing of invocations for your function**

1. Open the detail page for your function by doing one of the following.
   - Find your function on the related subscription page:
     a. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.
     b. Choose the **Compartment** that contains your function subscription.
     c. Click **Subscriptions**.
     d. Under **Endpoint**, in the row for your function subscription, click the name of your function.
   - Find your function on a Functions page:
     a. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**.
     b. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. **Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure** on page 2053).
     c. Select the compartment containing the application that contains your function.
        
        The **Applications** page shows all the applications in the compartment you selected.
        
        d. Click the name of the application containing your function.
        
        e. Click the name of your function.

        The function detail page is displayed.

2. Under **Resources**, click **Metrics**.
   
   The Metrics page displays a chart for each metric that is emitted by the metric namespace for Oracle Functions. For more information about the emitted metrics, see **Available Metrics: oci_faas** on page 2107.

3. Adjust the time range by selecting from **Quick Selects** or changing the **Start Time** and **End Time**.

4. Review the **Invocations** chart.

• **Function run:** Note times for runs of your function. Compare to times of the firing alarm or other inciting incident.

**To view timing of runs of your function (logs)**

See **Storing and Viewing Function Logs** on page 2078.

**To view timing of runs of your function (metrics)**

1. Open the detail page for your function by doing one of the following.
   - Find your function on a subscription page:
     a. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.
     b. Choose the **Compartment** that contains your function subscription.
     c. Click **Subscriptions**.
     d. Under **Endpoint**, in the row for your function subscription, click the name of your function.
   - Find your function on a Functions page:
     a. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Functions**. 
b. Select the region you are using with Oracle Functions. Oracle recommends that you use the same region as the Docker registry that's specified in the Fn Project CLI context (see 6. Create an Fn Project CLI Context to Connect to Oracle Cloud Infrastructure on page 2053).

c. Select the compartment containing the application that contains your function.

   The Applications page shows all the applications in the compartment you selected.

d. Click the name of the application containing your function.

e. Click the name of your function.

   The function detail page is displayed.

2. Under Resources, click Metrics.

   The Metrics page displays a chart for each metric that is emitted by the metric namespace for Oracle Functions. For more information about the emitted metrics, see Available Metrics: oci_faas on page 2107.

3. Adjust the time range by selecting from Quick Selects or changing the Start Time and End Time.

4. Review the Duration chart.

Notifications Metrics

You can monitor the health, capacity, and performance of your messages by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace oci_notification (the Notifications service).

Resources: Not applicable. Measures data for messages, which are not resources.

Overview of the Notifications Service Metrics

The Notifications service metrics help you measure the number and size of messages that are in initial requests, are delivered, and are not delivered.

Prerequisites

- IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Available Metrics: oci_notification

The metrics listed in the following table are automatically available for messages you publish to topics. You do not need to enable monitoring on any resources to get these metrics.

Each metric includes a subset of the following dimensions:

- AVAILABILITYDOMAIN
  The availability domain in which the associated topic resides.

- ENDPOINTTYPE
  The subscription protocol of the endpoint used for the delivery attempt.

- REGION
  The region in which the associated topic resides.

- RESOURCEID
  The OCID of the resource to which the metric applies.
### TOPICDISPLAYNAME

The friendly name of the associated *topic*.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublishedMessagesSize</td>
<td>Published Messages Size (Bytes)</td>
<td>bytes</td>
<td>Size of messages in request.</td>
<td>availabilityDomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>region</td>
</tr>
<tr>
<td>PublishedMessagesCount</td>
<td>Published Messages Count</td>
<td>count</td>
<td>Count of messages in request.</td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>topicDisplayName</td>
</tr>
<tr>
<td>DeliveredMessagesSize</td>
<td>Delivered Messages Size (Bytes)</td>
<td>bytes</td>
<td>Size of messages successfully delivered to endpoints.</td>
<td>availabilityDomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>endpointType</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>topicDisplayName</td>
</tr>
<tr>
<td>FailedMessagesSizes</td>
<td>Failed Messages Sizes (Bytes)</td>
<td>bytes</td>
<td>Size of messages that did not get delivered to endpoints.</td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>topicDisplayName</td>
</tr>
<tr>
<td>DeliveredMessagesCount</td>
<td>Delivered Messages Count</td>
<td>count</td>
<td>Count of messages successfully delivered to endpoints.</td>
<td>availabilityDomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>topicDisplayName</td>
</tr>
<tr>
<td>FailedMessagesCount</td>
<td>Failed Messages Count</td>
<td>count</td>
<td>Count of messages that did not get delivered to endpoints.</td>
<td>availabilityDomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>topicDisplayName</td>
</tr>
</tbody>
</table>

### Using the Console

**To view default metric charts for a single topic**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Application Integration** and click **Notifications**.
2. Choose the **Compartment** that contains the topic you want to view, and then click the topic's name.
3. In the **Resources** menu, click **Metrics** (if necessary).

   The **Metrics** page displays a default set of charts for the current topic.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**To view default metric charts for multiple topics**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Service Metrics**.
2. For **Metric Namespace**, select **oci_notification**.

   The **Service Metrics** page displays a default set of charts for the selected metric namespace. For more information about the emitted metrics, see the foregoing table. You can also use the Monitoring service to create custom queries.

**Tip:**

- Filter metrics by dimension, such as a selected topic, by clicking **Add** above the charts (to the right of **Dimensions**).
For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

**Using the API**

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)
Chapter 28

Object Storage

This chapter explains how to upload, manage, and access data using Object Storage.

Overview of Object Storage

The Oracle Cloud Infrastructure Object Storage service is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability. The Object Storage service can store an unlimited amount of unstructured data of any content type, including analytic data and rich content, like images and videos.

With Object Storage, you can safely and securely store or retrieve data directly from the internet or from within the cloud platform. Object Storage offers multiple management interfaces that let you easily manage storage at scale. The elasticity of the platform lets you start small and scale seamlessly, without experiencing any degradation in performance or service reliability.

Object Storage is a regional service and is not tied to any specific compute instance. You can access data from anywhere inside or outside the context of the Oracle Cloud Infrastructure, as long you have internet connectivity and can access one of the Object Storage endpoints. Authorization and resource limits are discussed later in this topic.

Oracle Cloud Infrastructure supports multiple storage tiers that offer cost and performance flexibility. Standard is the default storage tier for Object Storage buckets.

Object Storage also supports private access from Oracle Cloud Infrastructure resources in a VCN through a service gateway. A service gateway allows connectivity to the Object Storage public endpoints from private IP addresses in private subnets. For example, you can back up DB systems to an Object Storage bucket over the Oracle Cloud Infrastructure backbone instead of over the internet. You can optionally use IAM policies to control which VCNs or ranges of IP addresses can access Object Storage. See Access to Oracle Services: Service Gateway on page 3256 for details.

Object Storage is Always Free eligible. For more information about Always Free resources, including capabilities and limitations, see Oracle Cloud Infrastructure Free Tier on page 140.

Object Storage Resources

Use the following Object Storage resources to store and manage data. Authorization and resource limits are discussed later in this topic.

**Buckets**

Buckets are logical containers for storing objects. Users or systems create buckets as needed within a region. A bucket is associated with a single compartment that has policies that determine what actions a user can perform on a bucket and on all the objects in the bucket.

**Objects**

Any type of data, regardless of content type, is stored as an object. An object is composed of the object itself and metadata about the object. Each object is stored in a bucket.
Namespace

A namespace serves as the top-level container for all buckets and objects. At account creation time, each tenant is assigned one unique system-generated and immutable namespace name. The namespace spans all compartments within a region. You control bucket names, but those bucket names must be unique within a namespace. While the namespace is region-specific, the namespace name itself is the same in all regions. See Understanding Object Storage Namespaces on page 3395 for more details, including information about older tenancy names, illustrative examples of namespaces, and how to obtain your namespace string.

Compartment

A compartment is the primary building block used to organize your cloud resources. When your tenancy is provisioned, a root compartment is created for you. You can then create compartments under your root compartment to organize your resources. You control access by creating policies that specify what actions groups of users can take on the resources in those compartments. An Object Storage bucket can only exist in one compartment.

Object Storage Features

Object Storage provides the following features:

**STRONG CONSISTENCY**

When a read request is made, Object Storage always serves the most recent copy of the data that was written to the system.

**DURABILITY**

Object Storage is a regional service. Data is stored redundantly across multiple storage servers. Object Storage actively monitors data integrity using checksums and automatically detects and repairs corrupt data. Object Storage actively monitors and ensures data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies. For more details about Object Storage durability, see the Object Storage FAQ.

**custom metadata**

You can define your own extensive metadata as key-value pairs for any purpose. For example, you can create descriptive tags for objects, retrieve those tags, and sort through the data. You can assign custom metadata to objects and buckets using the Oracle Cloud Infrastructure CLI or SDK. See Software Development Kits and Command Line Interface on page 4225 for details.

**ENCRYPTION**

Object Storage employs 256-bit Advanced Encryption Standard (AES-256) to encrypt object data on the server. Each object is encrypted with its own data encryption key. Data encryption keys are always encrypted with a master encryption key that is assigned to the bucket. Encryption is enabled by default and cannot be turned off. By default, Oracle manages the master encryption key.

In addition to this default encryption, you can employ these other strategies to encrypt data:

- You can optionally configure a bucket so that it's assigned an Oracle Cloud Infrastructure Vault master encryption key that you control and rotate on your own schedule. See Overview of Vault on page 3952 for details.
- You can optionally encrypt each Object Storage object using your own encryption key. See Using Your Own Keys for Server-Side Encryption on page 3491 for details.

Ways to Access Object Storage

You can access Object Storage using any of the following options, based on your preference and its suitability for the task you want to complete:
• The Console is an easy-to-use, browser-based interface.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

• Google Chrome 69 or later
• Safari 12.1 or later
• Firefox 62 or later

You are prompted to enter your cloud tenant, your user name, and your password.

• The command line interface (CLI) provides both quick access and full functionality without the need for programming. For more information, see Using the CLI on page 4207.

• The REST API provides the most functionality, but requires programming expertise. API Reference and Endpoints provides endpoint details and links to the available API reference documents. For general information about using the API, see REST APIs on page 4368. Object Storage is accessible with the following APIs:
  • Object Storage Service
  • Amazon S3 Compatibility API
  • Swift API (for use with Oracle RMAN)
  • Oracle Cloud Infrastructure provides SDKs that interact with Object Storage without you having to create a framework. For general information about using the SDKs, see Software Development Kits and Command Line Interface on page 4225.

Using Object Storage

If you are ready to use Object Storage, you can find more information in the following topics:

• For instructions on how to create a bucket and store an object in the bucket, see "Putting Data into Object Storage" in the Oracle Cloud Infrastructure Getting Started Guide.

• For task documentation related to buckets, see Managing Buckets on page 3398, Using Replication on page 3440, and Using Retention Rules to Preserve Data on page 3458.

• For task documentation related to objects, see Managing Objects on page 3419, Using Object Versioning on page 3446, and Copying Objects on page 3487.

• For task documentation related to lifecycle management, see Using Object Lifecycle Management on page 3466.

• For API reference documentation, see Object Storage Service API.

• For SDK and CLI information, see Software Development Kits and Command Line Interface on page 4225.

• For more information about using Archive Storage, see Overview of Archive Storage on page 484.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API). IAM also manages user credentials for things like API signing keys, auth tokens, and customer secret keys for Amazon S3 Compatibility API. See User Credentials on page 2360 for details.

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create users and groups, create buckets, download objects, and manage Object Storage-related policies and rules. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see the Policy Reference on page 2167. For specific details about writing policies for Object Storage, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.
Blocking Access to Object Storage Resources from Unauthorized IP Addresses

You can enhance the security of your Object Storage policies by restricting access only to requests that originate from an allowed IP address. First, you create a network source to specify the allowed IP addresses, then you add a condition to your policy to restrict access to the IP addresses in the network source. An example of a policy that restricts access to only IP addresses in a network source is:

```
    allow group CorporateUsers to manage object-family in tenancy where
    request.networkSource.name='corpnet'
```

For information on creating network sources and using them in a policy, see Managing Network Sources on page 2427.

Object Storage IP Addresses

The Oracle Cloud Infrastructure Object Storage service uses the CIDR block IP range 134.70.0.0/17 for all regions.

Limits on Object Storage Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

To set tenancy or compartment-specific storage limits, administrators can use Object Storage Quotas on page 256.

Other limits include:

- Number of Object Storage namespaces per root compartment: 1
- Maximum object size: 10 TiB
- Maximum object part size in a multipart upload: 50 GiB
- Maximum number of parts in a multipart upload: 10,000
- Maximum object size allowed by PutObject API: 50 GiB
- Maximum size of object metadata: 2 K

Understanding Object Storage Namespaces

, namespace serves as the top-level container for all buckets and objects. At account creation time, each tenant is assigned one unique system-generated and immutable namespace name. The namespace spans all compartments within a region. You control bucket names, but those bucket names must be unique within a namespace. While the namespace is region-specific, the namespace name itself is the same in all regions.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot customize, change, or request a namespace name change.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For some older tenancies, the namespace name string might be based on your tenancy name instead of being machine generated. If your namespace was created based on your tenancy name, your namespace uses all lowercase letters (regardless of the presence of capital letters in your tenancy name). When using the API, CLI, or SDKs, do not use capital letters in your namespace name string.</td>
</tr>
</tbody>
</table>

If your tenancy is assigned a namespace name of axaxncorw5, that is your namespace name in all regions. You can create a bucket named MyBucket in US West (Phoenix). You cannot create another bucket named MyBucket in US West (Phoenix). You can, however, create a bucket named MyBucket in Germany Central (Frankfurt).

Because the namespace name is unique to a tenant, other customers can create buckets named MyBucket in their own namespaces.

Within a namespace, buckets and objects exist in flat hierarchy, but you can simulate a directory structure to help navigate a large set of objects. See Object Naming Using Prefixes and Hierarchies on page 3420 for details.
The namespace metadata stores the default compartment assignments for the Amazon S3 Compatibility API and the Swift API. For more information, see Viewing and Specifying Designated Compartments.

Using the Console

To view your Object Storage namespace string:

Open the Profile menu and click Tenancy: <your_tenancy_name>.

Your namespace string is listed under Object Storage Settings.

Note:

While the Object Storage namespace string is displayed under Object Storage Settings, you cannot edit the namespace string. The namespace string appears here for information only.

Using the Command Line Interface (CLI)

Run the following command get your Object Storage namespace:

```sh
oci os ns get
```

Your Object Storage namespace is returned:

```json
{
  "data": "MyNamespace"
}
```

Tip:

You can use -ns, --namespace, or --namespace-name for CLI commands that require you to specify the Object Storage namespace string.

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the GetNamespace operation to get your Object Storage namespace. If you have the OBJECTSTORAGE_NAMESPACE_READ permission and supply the compartment or tenancy OCID in the optional compartmentId parameter, you can also get the namespace of a different tenancy's Object Storage namespace.

Understanding Storage Tiers

Oracle Cloud Infrastructure offers distinct storage class tiers to address the need for both performant, frequently accessed "hot" storage, less frequently accessed "cool" storage, and rarely accessed "cold" storage. Storage tiers help you maximize access performance where appropriate and minimize storage costs where possible.

You interact with the data stored in any of the storage tiers using the same resources and management interfaces that you use for Object Storage. In addition, each storage tier supports the full range of Object Storage features. Specific storage tier details or interactions that you need to be aware of are covered in the Scope and Constraints section for the feature.
**Standard Tier**

The **Standard** tier is the primary, default storage tier used for Object Storage service data. The Standard storage tier is "hot" storage used for data that you need to access quickly, immediately, and frequently. Data accessibility and performance justifies a higher price to store data in the Standard tier.

You choose a default storage tier (Standard or Archive) when you create a bucket. Once set at bucket creation, you cannot change the default storage tier for a bucket. When you upload objects to a bucket, the default storage tier is selected by default. You can, however, change the storage tier when uploading objects to either the Infrequent Access or Archive tier. Standard buckets can therefore contain a mix of objects residing in all storage tiers.

The following list summarizes some of the use cases for the Standard tier.

- Primary content repository for accessible scalable data, images, logs, and video
- Primary data repository for Hadoop/big data. Provides a scalable storage platform to store large datasets and operate seamlessly on those datasets. The HDFS Connector for Object Storage on page 4347 provides connectivity to various big data analytic engines like Apache Spark and MapReduce. This connectivity enables the analytics engines to work directly with data stored in Object Storage. For more information, see Hadoop Support on page 3505.

**Infrequent Access**

The **Infrequent Access** tier is "cool" storage used for data that you access infrequently, but that must be available immediately when needed. Storage costs are lower than **Standard**.

The use cases for the Infrequent Access tier include the following:

- Backups of on-premises data
- Storage for data replicated or copied from another region

The Infrequent Access tier has a minimum storage retention period and data retrieval fees:

- The minimum storage retention period for the Infrequent Access tier is 31 days. If you delete objects from the Infrequent Access tier before the minimum retention requirements are met, you are charged the prorated cost of storing the data for the full 31 days.
- When you need to access objects stored in this tier, you are charged a per GiB data retrieval fee.

**Archive**

The **Archive** tier is the primary, default storage tier used for Archive Storage service data. The Archive storage tier is "cold" storage used for data seldom or rarely access, but that must be retained and preserved for long periods of time.

You can choose a default storage tier (Standard or Archive) when you create a bucket. When you upload objects to a bucket in an Archive tier, the objects are automatically uploaded to the Archive tier. You cannot upload objects in an Archive bucket to any other storage tier. Archive buckets can only contain objects in the Archive storage tier.

The use cases for the Archive tier include the following:

- Compliance and audit mandates
- Retroactive log data analysis to determine usage pattern or to debug problems
- Historical or rarely accessed content repository data
- Application-generated data requiring archival for future analysis or legal purposes

Objects in the Archive tier must be restored before they are available for access. The cost efficiency of the Archive tier offsets the lead time required to access the data. However, the Archive tier has a minimum storage retention period and some additional storage fees:

- The minimum storage retention period for the Archive tier is 90 days. If you delete objects from the Archive tier before the minimum retention requirements are met, you are charged the prorated cost of storing the data for the full 90 days.
- When you restore objects, you are returning those objects to the Standard tier for access. You are billed for the Standard class tier while the restored objects reside in that tier.
Managing Buckets

In the Oracle Cloud Infrastructure Object Storage service, a bucket is a container for storing objects in a compartment within an Object Storage namespace. A bucket is associated with a single compartment. The compartment has policies that indicate what actions you can perform on a bucket and all the objects in the bucket.

You cannot nest buckets—a bucket cannot contain other buckets.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you are new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For administrators:

- The policy Let Object Storage admins manage buckets and objects on page 2149 lets the specified group do everything with buckets and the associated objects.
- If you must write more restrictive policies for buckets, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

Security Zones

Security Zones ensure that your cloud resources comply with Oracle security principles. If any operation on a resource in a security zone compartment violates a policy for that security zone, then the operation is denied.

The following security zone policies affect your ability to manage buckets:

- You can't move a bucket from a security zone to a standard compartment because it might be less secure. For details, see Restrict Resource Movement.
- Buckets in a security zone must be private.
- Buckets in a security zone must use customer-managed master encryption keys in the Vault service.

Pre-Authenticated Requests

Pre-authenticated requests provide a way to let you access a bucket or an object without having your own credentials. For example, you can create a request that lets you upload backups to a bucket without owning API keys. See Using Pre-Authenticated Requests on page 3482 for details.

Object Versioning

You can enable object versioning to retain previous versions of objects. Object versioning lets you view, retrieve, and recovery previous versions of objects and provides protection against accidental or malicious object overwrite or deletion. For information about this feature, see Using Object Versioning on page 3446.

Object Lifecycle Policies

Using object lifecycle policies applied at the bucket level, you can automatically manage the archiving and deletion of objects according to a pre-defined schedule. For information about this feature, see Using Object Lifecycle Management on page 3466.

Retention Rules

You can apply retention rules at the bucket level to provide immutable object storage options for data written to Object Storage for governance, regulatory compliance, and legal requirements. For information about this feature, see Using Retention Rules to Preserve Data on page 3458.
Replication Policy

Using a replication policy for a bucket, you can automatically replicate the objects in one Object Storage bucket to another bucket in the same region or a different region. For information about this feature, see Using Replication on page 3440.

Tagging Resources

You can add tags to your resources to help you organize them according to your business needs. You can add tags at the time you create a resource, or you can update the resource later with the desired tags. For general information about applying tags, see Resource Tags on page 211.

Object Storage currently supports adding tags to buckets.

Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring buckets, see Object Storage Metrics on page 3499.

Usage Reports

A usage report is a comma-separated value (CSV) file that can be used to get a detailed breakdown of resources in Oracle Cloud Infrastructure for audit or invoice reconciliation. A usage report is generated daily and stored in an Object Storage bucket. For more information, see Cost and Usage Reports Overview on page 278 and Accessing Cost and Usage Reports on page 281.

Creating Automation for Buckets and Objects Using the Events Service

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

Buckets emit events for bucket state changes by default. Events for objects are handled differently than other resources. Objects do not emit events by default. Use the Console, CLI, or API to enable a bucket to emit events for object state changes. You can enable events for object state changes during or after bucket creation.

Bucket Names

Bucket names are system generated by default, but you can overwrite the default with a name you specify.

System-Generated Bucket Names

When a bucket is created, the system generates a default name for that bucket, for example bucket-20190306-1359. This bucket name identifies the current year, month, and day that the bucket was created. You can use that system-generated name for your new bucket or you can specify a different name.

User-Specified Bucket Names

If you change this default bucket name or the name of any bucket, observe the following:

- Make the name unique within your tenancy's Object Storage namespace.
- Use from 1 to 256 characters.
- Valid characters are letters (upper or lower case), numbers, hyphens, underscores, and periods.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket names and object names are case-sensitive. Object Storage handles accounts-payable and Accounts-Payable as separate buckets.</td>
</tr>
</tbody>
</table>

- Avoid entering confidential information.
**Default Storage Tiers**

When you create a bucket, you decide which default storage tier is appropriate for storing objects:

- Use the **Standard** tier for data to which you need fast, immediate, and frequent access.
- Use the **Archive** tier for data to which you seldom or rarely access, but that must be retained and preserved for long periods of time.

For more information, see Understanding Storage Tiers on page 3396.

**Important:**

You cannot change the storage tier in which a bucket resides.

**Public Buckets**

When you create a bucket, the bucket is considered a private bucket and the access to the bucket and bucket contents requires authentication and authorization. However, Object Storage supports anonymous, unauthenticated access to a bucket that is not in a security zone. You make a bucket public by enabling read access to the bucket.

**Important:**

Carefully assess the business requirement for public access to a bucket. When you enable anonymous access to a bucket, any user can obtain object metadata, download bucket objects, and optionally list bucket contents.

**Required Permissions**

The following permissions are required to configure a public bucket:

- To enable public access when creating a bucket, use permission `BUCKET_CREATE`.
- To enable public access for an existing bucket, use permission `BUCKET_UPDATE`.

**Options**

When creating a public bucket, you have the following options:

- You can configure the access to allow listing and downloading objects. List and download access is the default.
- You can configure the access to allow downloading objects only. A user would not be able to list bucket contents.

**Scope and Constraints**

Understand the following scope and constraints regarding public access:

- Buckets in a security zone can't be public.
- Changing the type of access is bi-directional. You can change a bucket's access from public to private or from private to public.
- Changing the type of access doesn't affect existing pre-authenticated requests. Existing pre-authenticated requests still work.

You can enable anonymous public access for new or existing buckets using the Console, CLI, or an SDK to access the API.

**Using the Console**

**To get a list of buckets**

Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).
To create a bucket

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Select a compartment from the Compartment list on the left side of the page.

A list of existing buckets is displayed.
3. Click Create Bucket.
4. In the Create Bucket dialog box, specify the attributes of the bucket:
   - **Bucket Name:** The system generates a default bucket name that reflects the current year, month, day, and time, for example bucket-20190306-1359. If you change this default to any other bucket name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
   - **Default Storage Tier:** Select the default tier in which you want to store your data. When you upload objects, the objects are uploaded to this tier by default. Available default tiers include:
     - **Standard** is the primary, default storage tier used for Object Storage service data. Use the Standard tier for storing data that requires fast and immediate access.
     - **Archive** is the default storage tier used for Archive Storage service data. Use the Archive tier for storing data that does not require immediate access, but requires long retention periods. Access to data in the Archive tier is not immediate. Archived data must be restored before the data is accessible.
   - **Object Events:** Select Emit Object Events if you want to enable the bucket to emit events for object state changes. For more information about events, see Overview of Events on page 1784.
   - **Object Versioning:** Select Enable Object Versioning if you want Object Storage to create an object version each time the content changes or the object is deleted. For more information, see Using Object Versioning on page 3446.
   - **Encryption:** Buckets are encrypted with keys managed by Oracle by default, but you can optionally encrypt the data in this bucket using your own Vault encryption key. To use Vault for your encryption needs, select Encrypt Using Customer-Managed Keys. Then, select the Vault Compartment and Vault that contain the master encryption key you want to use. Also select the Master Encryption Key Compartment and Master Encryption Key. For more information about encryption, see Overview of Vault on page 3952. For details on how to create a vault, see Managing Vaults on page 3957.
   - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click Create Bucket.

The bucket is created immediately and you can start uploading objects. Objects added to archive buckets are immediately archived and must be restored before they are available for download.

To view bucket details

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment that contains your buckets.

A list of buckets is displayed.
3. Click the Actions icon (three dots) to the right of the bucket name, and then click View Bucket Details.

To change the visibility of a bucket

A bucket is either private (the default) or public. See Public Buckets on page 3400 for more information.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can't change the visibility of a bucket from private to public if that bucket is in a security zone.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.

A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).
2. Click the bucket name to see the bucket details.
   - **Visibility**: shows the current bucket setting, which is **Private** by default.
3. Click **Edit Visibility**.
4. In the **Edit Visibility** dialog box, edit the visibility settings:
   - **Visibility**
     - **Public**
     - **Private**
   - If you select **Public** to enable public access, decide whether you want to let users list the bucket contents. To set the visibility of bucket object lists, click **Allow users to list objects from this bucket**.
5. Click **Save Changes**.

**To move a bucket to a different compartment**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can't move a bucket from a security zone to a standard compartment. You also need to ensure that the resource users have sufficient access permissions for the compartment to which the resource is being moved.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. In the **Scope** section, select a compartment.
3. Find the bucket in the list, click the Actions icon (three dots), and then click **Move Resource**.
   - Alternatively, you can choose a bucket, and then click **Move Resource** on the bucket details page.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**To manage tags for a bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).
3. Click the bucket name.
4. You can manage tags in the following ways:
   - To view the tags associated with the bucket, click the **Tags** tab, located to the right of the **Bucket Information** tab.
   - To add one or more tags, click **Add Tags**.
   - To rename a tag, click the pencil icon to the left of a tag name, edit the name, and save.
   - To delete a tag, click the pencil icon to the left of a tag name and click **Remove Tag**.

For more information, see **Resource Tags** on page 211.

**To delete a bucket**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot recover a deleted bucket.</td>
</tr>
</tbody>
</table>

You can permanently delete an *empty* bucket. You cannot delete a bucket that contains any of the following:
- Any objects
- Previous versions of an object
- A multipart upload in progress
- A pre-authenticated request
Tip:

When you delete an object in a version-enabled bucket, a previous version of that object is created. Select Show Deleted Objects to display the object versions that might prevent you from deleting the bucket. For more information, see Using Object Versioning on page 3446.

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.

   A list of the buckets in the compartment you're viewing is displayed. If you don't see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. Find the bucket that you want to delete.

3. Click the Actions icon (three dots), and then click Delete.

   Alternatively, you can choose a bucket, click More Actions on the bucket details page, and then click Delete.

4. Confirm deletion when prompted.

To assign a Vault master encryption key to a bucket

Buckets are encrypted with keys managed by Oracle by default. Optionally, you can encrypt the data encryption keys that encrypt the objects in a bucket using your own Vault master encryption key.

Important:

Buckets in a security zone can't use the default encryption key managed by Oracle. You must use your own Vault master encryption key.

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.

   A list of the buckets in the compartment you're viewing is displayed. If you don't see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. Click the name of the bucket that you want to encrypt.

3. Next to Encryption Key, do one of the following:

   • If the bucket is encrypted with a key managed by Oracle, click the Assign link.
   • If the bucket already has a Vault master encryption key assigned, to assign a different key, click the Edit link.

4. In the dialog box, provide or edit the following information:

   • Vault Compartment and Vault that contain the master encryption key you want to use. The current compartment is displayed by default.
   • Master Encryption Key Compartment and Master Encryption Key. The current compartment is displayed by default.

5. When you are finished, click Assign or Edit.

See Overview of Vault on page 3952 for more details.

To remove a Vault master encryption key from a bucket

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.

   A list of the buckets in the compartment you're viewing is displayed. If you don't see the one you're looking for, verify that you're viewing the correct compartment (select from the list on the left side of the page).

2. Click the name of the bucket for which you want to remove a Vault key assignment.

3. Next to Encryption Key, click the Unassign link.

4. In the Confirm dialog box, click OK to remove the key assignment from the bucket.

To re-encrypt a bucket's data encryption keys

If you've rotated a master encryption key since the time you assigned it to a bucket, you might want to re-encrypt the bucket. Until you explicitly re-encrypt a bucket, the key version associated with the bucket when an object was inserted into the bucket continues to decrypt all data encryption keys. To encrypt and decrypt all data encryption keys with the same, most recent version of the assigned master encryption key, re-encrypt the bucket.
1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. Click the name of the bucket for which you want to re-encrypt all data encryption keys.

3. Click **Re-encrypt**. (If the button is not enabled, that's because the bucket is using a master encryption key managed by Oracle rather than a Vault master encryption. Or, the bucket does not contain any objects.)

4. In the confirmation dialog box, click **Re-encrypt** to generate a work request to re-encrypt all data encryption keys associated with the bucket.

The **Work Requests Details** dialog box that displays tells you about the work request, including the percentage completed and the work request ID. You can copy the work request ID to monitor the request status later.

**To view the approximate bucket size and number of objects in the bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

2. Choose the compartment that contains your buckets.

A list of buckets is displayed.

3. Click the Actions icon (three dots) to the right of the bucket name, and then click **View Bucket Details**.

- **Approximate Count** is the approximate number of objects in the bucket. Count statistics are reported periodically. A lag can occur between what is displayed and the actual object count.

- **Approximate Size** is the approximate total size of all objects in the bucket. Size statistics are reported periodically. A lag can occur between what is displayed and the actual size of the bucket.

**To enable or disable emitting events for object state changes**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see **Overview of Events** on page 1784.

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

2. Choose the compartment that contains your buckets.

A list of buckets is displayed.

3. Click the Actions icon (three dots) to the right of the bucket name, and then click **View Bucket Details**.

4. Next to **Emit Object Events**, click **Edit**.

5. In the dialog box, select (to enable) or deselect (to disable) **Emit Object Events**.

6. Click **Save Changes**.

**To view or copy the Oracle Cloud Identifier (OCID) for a bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

2. Choose the compartment that contains your buckets.

A list of buckets is displayed.

3. Click the Actions icon (three dots) to the right of the bucket name, and then click **View Bucket Details**.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see **Command Line Interface (CLI)**. For a complete list of flags and options available for CLI commands, see the **Command Line Reference**.

**Note:**

The examples in this section use the full syntax for all parameters, for example `--namespace` and `--compartment-id`. For some parameters, there are shortened versions that you can use instead, like `-ns` and `-c`. See the CLI online help for instances of a shortened parameter associated with a command.
To get a list of buckets

```bash
oci os bucket list --namespace <object_storage_namespace> --compartment-id <target_compartment_id>
```

For example:

```bash
oci os bucket list --namespace MyNamespace --compartment-id ocid.compartment.oc1..exampleuniqueID
```

```json
{
  "data": [
    {
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "created-by": "ocid1.user.oc1..exampleuniqueID",
      "defined-tags": null,
      "etag": "c8889cd1-8414-41fb-84b7-3738c39e62c5",
      "freeform-tags": null,
      "name": "MyBucket1",
      "namespace": "MyNamespace",
      "time-created": "2020-05-22T19:22:25.032000+00:00"
    },
    {
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "created-by": "ocid1.user.oc1..exampleuniqueID",
      "defined-tags": null,
      "etag": "7b7c3dc1-713f-4996-b176-a938345cae8e",
      "freeform-tags": null,
      "name": "MyBucket2",
      "namespace": "MyNamespace",
      "time-created": "2020-06-22T13:04:05.879000+00:00"
    }
  ]
}
```

By default, getting a list of buckets returns up to the first 1,000 buckets in the compartment.

**Note:**

If you do not specify the `--fields tags` option when listing buckets, null is returned as the value for both freeform and defined tags.

For example:

To include resource tag data, use the `--fields tags` option:

```bash
oci os bucket list --namespace <object_storage_namespace> --compartment-id <target_compartment_id> --fields tags
```

For example:

```bash
oci os bucket list --namespace MyNamespace --compartment-id ocid.compartment.oc1..exampleuniqueID --fields tags
```

```json
{
  "data": [
    {
      "compartment-id": "ocid1.compartment.oc1..exampleuniqueID",
      "created-by": "ocid1.user.oc1..exampleuniqueID",
      "defined-tags": {
        "example_tag_namespace_Financials": {

```
To create a Standard tier bucket

```bash
oci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id>
```

For example:

```bash
oci os bucket create --namespace MyNamespace --name MyBucket --compartment-id ocid.compartment.oc1..exampleuniqueID
```

By default, a bucket is created in the standard Object Storage tier. You do not need to explicitly set `--storage-tier`.

A Standard tier bucket is created immediately and you can start uploading objects.
To create an Archive tier bucket

To create an Archive tier bucket, you must explicitly set --storage-tier Archive.

```bash
oci os bucket create --namespace <object_storage_namespace> --name <archivebucket_name> --compartment-id <target_compartment_id> --storage-tier Archive
```

For example:

```bash
oci os bucket create --namespace MyNamespace --name MyArchiveBucket --compartment-id ocid.compartment.oc1..exampleuniqueID
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "c8889cd1-8414-41fb-84b7-3738c39e62c5",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": null,
    "metadata": {},
    "name": "MyArchiveBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policyetag": null,
    "public-access-type": "NoPublicAccess",
    "replication-enabled": false,
    "storage-tier": "Archive",
    "time-created": "2020-06-12T19:04:05.879000+00:00",
    "versioning": "Disabled"
  },
  "etag": "c8889cd1-8414-41fb-84b7-3738c39e62c5"
}
```

An Archive Storage bucket is created and you can start uploading objects. Objects uploaded to Archive Storage buckets are immediately archived and must be restored before they are available for download.

To create a public bucket that allows listing and downloading bucket objects

To create a public bucket that allows listing and downloading bucket objects, you must explicitly set --public-access-type ObjectRead.

```bash
oci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --public-access-type ObjectRead
```

For example:

```bash
oci os bucket create --namespace MyNamespace --name MyBucket --compartment-id ocid.compartment.oc1..exampleuniqueID
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "01096e0b-659a-4d9d-a806-d57568cf1b22",
    "freeform-tags": {}
  }
```

Oracle Cloud Infrastructure User Guide
To create a public bucket that allows downloading bucket objects only

```bash
oci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --public-access-type ObjectReadWithoutList
```

For example:

```bash
oci os bucket create --namespace MyNamespace --name MyPublicObjectReadBucket --compartment-id ocid.compartment.oc1..exampleuniqueID --public-access-type ObjectReadWithoutList
```

```json
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "ec20c59a-f5ba-4a6d-8a7e-b69bb9bb76ad",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": null,
    "metadata": {},
    "name": "MyPublicObjectReadWithoutListBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "ObjectReadWithoutList",
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-22T19:04:05.879000+00:00",
    "versioning": "Disabled"
  },
  "etag": "01096e0b-659a-4d9d-a806-d57568cf1b22"
}
```

To create a bucket with resource tags

You can create standard Object Storage tier or Archive tier buckets with resource tags.

To add resource tags when creating a bucket, set one or both of the `--defined-tags` and `--freeform-tags` options.
Tip:
The `--defined-tags` and `--freeform-tags` options require that the input to be a complex type formatted in valid JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

The following example syntax creates a standard Object Storage tier bucket with a defined tag:

```
ooci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --defined-tags '{<JSON_formatted_defined_tag>}'
```

Examples of defined tag formatting:

```
'{"Operations": {"CostCenter": "42"}}

'{"Logistics": {"Procurement": "Madrid Center"}},"Financials":{"Production": "Unit 5"}}
```

Note:
If you are running the CLI on a Windows computer, you might need to use the backslash (\) character to escape the strings containing the tag values. For example, a single defined tag is formatted '{"Logistics": \"Procurement\": \"Madrid Center\"}''

For example:

```
ooci os bucket create --namespace MyNamespace --name MyBucketDefined --compartment-id ocid.compartment.oc1..exampleuniqueID --defined-tags '{"Operations": {"CostCenter": "42"}}
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {
      "operations": {
        "costcenter": "42"
      }
    },
    "etag": "ea88f444-842c-462d-965e-d3540b3b54f6",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": null,
    "metadata": {},
    "name": "MyBucketDefined",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess",
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-23T19:47:51.362000+00:00",
    "versioning": "Disabled"
  },
  "etag": "ea88f444-842c-462d-965e-d3540b3b54f6"
}
```
The following example syntax creates a Standard tier bucket with a free-form tag:

```bash
oci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --freeform-tags <JSON_formated_free-form_tag>
```

Examples of free-form tag formatting:

```json
'{"Chicago_Team": "marketing_videos"}'

'{"Project": "prototype 3","Manager": "Meadows"}'
```

**Note:**
If you are running the CLI on a Windows computer, you might need to use the backslash (\) character to escape the strings containing the tag values. For example, a single free-form tag is formatted as `{"Chicago_Team": {"marketing_videos"}}`

For example:

```bash
oci os bucket create --namespace MyNamespace --name MyBucketFreeform --compartment-id ocid.compartment.oc1..exampleuniqueID --freeform-tags '{"Chicago_Team": "marketing_videos"}'
```

To view bucket details

```bash
oci os bucket get --name <bucket_name>
```

For example:

```bash
oci os bucket get --name MyBucket
```

```json
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "6f4bda10-fc8b-462e-8563-875639fd7294",
    "freeform-tags": {
      "Chicago_Team": "marketing_videos"
    },
    "is-read-only": false,
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "kms-key-id": null,
    "metadata": {},
    "name": "MyBucketFreeform",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess",
    "storage-tier": "Standard",
    "time-created": "2020-06-23T20:51:16.260000+00:00"
  },
  "etag": "6f4bda10-fc8b-462e-8563-875639fd7294"
}
```
To add custom key-value metadata pairs to a bucket

```bash
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --metadata <JSON-formatted_key-value_pair>
```

<JSON-formatted_key-value_pair> is a key-value pair input as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

For example:

```bash
oci os bucket update --namespace MyNamespace --name MyBucket --metadata '{"Department": "Finance"}'
```

```json
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "4b09d7b9-a8bf-42f6-8d67-bb357694f92d",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": null,
    "metadata": {
      "department": "Finance"
    },
    "name": "MyBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess",
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-22T19:04:05.879000+00:00",
    "versioning": "Disabled"
  },
  "etag": "4b09d7b9-a8bf-42f6-8d67-bb357694f92d"
}
```
To make a bucket private or public

```plaintext
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --public-access-type [NoPublicAccess|ObjectReadWithoutList|ObjectRead]
```

- **NoPublicAccess**: Allows only an authenticated caller to access the bucket and bucket contents. NoPublicAccess is the default value.
- **ObjectReadWithoutList**: Allows public access for the GetObject, HeadObject, and ListObjects operations.
- **ObjectRead**: Allows public access for the GetObject and HeadObject operations.

For example:

```plaintext
oci os bucket update --namespace MyNamespace --name MyBucket --public-access-type ObjectRead
```

```
{  
  "data": {  
    "approximate-count": null,  
    "approximate-size": null,  
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",  
    "created-by": "ocid1.user.oc1..exampleuniqueID",  
    "defined-tags": {},  
    "etag": "09ab3193-a441-43cc-a8e2-e468e94c7c60",  
    "freeform-tags": {},  
    "id": "ocid1.bucket.oc1..exampleuniqueID",  
    "is-read-only": false,  
    "kms-key-id": null,  
    "metadata": {  
      "department": "Finance"  
    },  
    "name": "MyBucket",  
    "namespace": "MyNamespace",  
    "object-events-enabled": false,  
    "object-lifecycle-policy-etag": null,  
    "public-access-type": "ObjectRead",  
    "replication-enabled": false,  
    "storage-tier": "Standard",  
    "time-created": "2020-06-22T19:04:05.879000+00:00",  
    "versioning": "Disabled"  
  },  
  "etag": "09ab3193-a441-43cc-a8e2-e468e94c7c60"
}
```

To move a bucket to a different compartment

```plaintext
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <new_target_compartment_id>
```

*<new_target_compartment_id>* is the compartment ID associated with the compartment to which you are moving the bucket.

For example:

```plaintext
oci os bucket update --namespace MyNamespace --name MyBucket --compartment-id ocid.compartment.oc1..exampleuniqueID
```

```
{  
  "data": {  
    "approximate-count": null,  
    "approximate-size": null,  
    "compartment-id": "new_ocid.compartment.oc1..exampleuniqueID",  
    "created-by": "ocid1.user.oc1..exampleuniqueID",  
    "defined-tags": {}  
  }
```
To add resource tags to a bucket

To add defined resource tags to a bucket:

```
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --defined-tags <JSON_formatted_defined_tag>
```

For example:

```
oci os bucket update --namespace MyNamespace --name MyBucket --defined-tags '{"Operations": {"CostCenter": "42"}}'
```

```json
{
   "data": {
      "approximate-count": null,
      "approximate-size": null,
      "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "created-by": "ocid1.user.oc1..exampleuniqueID",
      "defined-tags": {
         "operations": {
            "costcenter": "42"
         }
      },
      "etag": "0a26b47d-c43f-4ef8-9c26-02bb8d69fa34",
      "freeform-tags": {},
      "id": "ocid1.bucket.oc1..exampleuniqueID",
      "is-read-only": false,
      "kms-key-id": null,
      "metadata": {
         "department": "Finance"
      },
      "name": "MyBucket",
      "namespace": "MyNamespace",
      "object-events-enabled": false,
      "object-lifecycle-policy-etag": null,
      "public-access-type": "NoPublicAccess",
      "replication-enabled": false,
      "storage-tier": "Standard",
      "time-created": "2020-06-22T19:04:05.879000+00:00",
      "versioning": "Disabled"
   },
   "etag": "0a26b47d-c43f-4ef8-9c26-02bb8d69fa34"
}
```
To add free-form resource tags to a bucket:

```
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --freeform-tags <JSON_formatted_free-form_tag>
```

For example:

```
oci os bucket update --namespace MyNamespace --name MyBucket --freeform-tags '{"Chicago_Team": "marketing_videos"}'
```

```
"data": {
  "approximate-count": null,
  "approximate-size": null,
  "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
  "created-by": "ocid1.user.oc1..exampleuniqueID",
  "defined-tags": {
    "operations": {
      "costcenter": "42"
    }
  },
  "etag": "856a3c73-0194-4c02-8c6b-1b20be3c9a48",
  "freeform-tags": {
    "Chicago_Team": "marketing_videos"
  },
  "id": "ocid1.bucket.oc1..exampleuniqueID",
  "is-read-only": false,
  "kms-key-id": null,
  "metadata": {
    "department": "Finance"
  },
  "name": "MyBucket",
  "namespace": "MyNamespace",
  "object-events-enabled": false,
  "object-lifecycle-policyetag": null,
  "public-access-type": "NoPublicAccess",
  "replication-enabled": false,
  "storage-tier": "Standard",
  "time-created": "2020-06-22T19:04:05.879000+00:00",
  "versioning": "Disabled"
},
"etag": "856a3c73-0194-4c02-8c6b-1b20be3c9a48"
```

**Tip:**

Provide key-value pair input for `--defined-tags` and `--freeform-tags` as valid formatted JSON. For examples of JSON-formatted resource tags, see To create a Standard or Archive tier bucket with resource tags. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

To delete a bucket

**Caution:**

You cannot recover a deleted bucket.

You can permanently delete an *empty* bucket. You cannot delete a bucket that contains any of the following:

- Any objects
- Previous versions of an object
Object Storage

- A multipart upload in progress
- A pre-authenticated request

```bash
oci os bucket delete --namespace <object_storage_namespace> --name <bucket_name>
```

For example:

```bash
oci os bucket delete --namespace MyNamespace --name MyDeletedBucket
Are you sure you want to delete this resource? [y/N]:
```

Select y and press Enter. The bucket is deleted with no further prompting.

**To assign a Vault key to a bucket**

```bash
oci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --kms-key-id <target_key_id>
```

<target_key_id> is the ID of the key versions that contain the cryptographic material used to encrypt and decrypt data, protecting the data where the data is stored.

For example:

```bash
oci os bucket create --namespace MyNamespace --name MyKeyBucket --compartment-id ocid.compartment.oc1..exampleuniqueID --kms-key-id ocid1.key.region1.sea..exampleuniqueID
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "e7f29fdd-b5f5-42e5-a98b-80883f9f2f32",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": "ocid1.key.region1.sea..exampleuniqueID",
    "metadata": {},
    "name": "MyKeyBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess"
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-29T23:00:35.490000+00:00",
    "versioning": "Disabled"
  },
  "etag": "e7f29fdd-b5f5-42e5-a98b-80883f9f2f32"
}
```

See Overview of Vault on page 3952 for more details.

**To update the Vault key assigned to a bucket**

```bash
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --kms-key-id <target_key_id>
```
<target_key_id> is the ID of the key versions that contain the cryptographic material used to encrypt and decrypt data, protecting the data where the data is stored.

For example:

```bash
oci os bucket update --namespace MyNamespace --name MyKeyBucket --kms-key-id ocid1.key.region1.sea.exampleuniqueID_updated
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "e7f29fdd-b5f5-42e5-a98b-80883f9f2f32",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": "ocid1.key.region1.sea..exampleuniqueID_updated",
    "metadata": {},
    "name": "MyKeyBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess",
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-29T23:00:35.490000+00:00",
    "versioning": "Disabled"
  },
  "etag": "e7f29fdd-b5f5-42e5-a98b-80883f9f2f32"
}
```

To remove the Vault key assigned to a bucket

```bash
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --kms-key-id ""
```

For example:

```bash
oci os bucket update --namespace MyNamespace --name MyKeyBucket --kms-key-id ""
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1.user.oc1..exampleuniqueID",
    "defined-tags": {},
    "etag": "10a50818-e495-45a9-b1ce-cc815f7b39ad",
    "freeform-tags": {},
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": null,
    "metadata": {},
    "name": "MyKeyBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": false,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess",
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-29T23:00:35.490000+00:00",
    "versioning": "Disabled"
  }
}
To re-encrypt a bucket's data encryption keys

If you've rotated a master encryption key since the time you assigned it to a bucket, you might want to re-encrypt the bucket. Until you explicitly re-encrypt a bucket, the key version associated with the bucket when an object was inserted into the bucket continues to decrypt all data encryption keys. To encrypt and decrypt all data encryption keys with the same, most recent version of the assigned master encryption key, re-encrypt the bucket.

`oci os bucket reencrypt --name <bucket_name>`

For example:

`oci os bucket reencrypt --name MyBucket`

To view the approximate bucket size and number of objects in the bucket

`oci os bucket get --name <bucket_name> --fields approximateCount --fields approximateSize`

- `approximateCount` is the approximate number of objects in the bucket. Count statistics are reported periodically. You might see a lag between what is displayed and the actual object count.
- `approximateSize` is the approximate total size of all objects in the bucket. Size statistics are reported periodically. You might see a lag between what is displayed and the actual size of the bucket.

For example:

`oci os bucket get --name MyBucket --fields approximateCount --fields approximateSize`

```json
{  "data": {    "approximate-count": 25,    "approximate-size": 8075918,    "compartment-id": "ocid1.compartment.oc1..exampleuniqueID",    "created-by": "ocid1:user:oc1:phx:1458751937789:exampleuniqueID",    "defined-tags": {},    "etag": "218f201f-28a4-434d-9591-f05b6223c67a",    "freeform-tags": {},    "id": "ocid1.bucket.oc1..exampleuniqueID",    "is-read-only": false,    "kms-key-id": null,    "metadata": {},    "name": "MyBucket",    "namespace": "MyNamespace",    "object-events-enabled": false,    "object-level-audit-mode": "Disabled",    "object-lifecycle-policy-etag": null,    "public-access-type": "NoPublicAccess",    "replication-enabled": false,    "storage-tier": "Standard",    "time-created": "2017-10-19T04:11:32.040000+00:00",    "versioning": "Disabled"  },  "etag": "218f201f-28a4-434d-9591-f05b6223c67a"}
```
To enable or disable emitting events for object state changes

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

```
oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --object-events-enabled [true|false]
```

For example, to enable emitting events for all objects in the bucket named MyBucket:

```
oci os bucket update --namespace MyNamespace --name MyBucket --object-events-enabled true
{
  "data": {
    "approximate-count": null,
    "approximate-size": null,
    "compartment-id": "ocid1.compartment.oc1..exampleuniqueID",
    "created-by": "ocid1:user:oc1:phx:1458751937789:exampleuniqueID",
    "defined-tags": {
      "operations": {
        "costcenter": "42"
      }
    },
    "etag": "39d1db02-27d0-4263-b3ff-5e6450495457",
    "freeform-tags": {
      "Chicago_Team": "marketing_videos"
    },
    "id": "ocid1.bucket.oc1..exampleuniqueID",
    "is-read-only": false,
    "kms-key-id": null,
    "metadata": {
      "department": "Finance"
    },
    "name": "MyBucket",
    "namespace": "MyNamespace",
    "object-events-enabled": true,
    "object-lifecycle-policy-etag": null,
    "public-access-type": "NoPublicAccess",
    "replication-enabled": false,
    "storage-tier": "Standard",
    "time-created": "2020-06-22T19:04:05.879000+00:00",
    "versioning": "Disabled"
  },
  "etag": "39d1db02-27d0-4263-b3ff-5e6450495457"
}
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

When accessing the Object Storage API, the bucket name is used with the Object Storage namespace name to form the request URL:

```
n/<object_storage_namespace>/b/<bucket>
```

Use the following API operations to manage buckets:

- CreateBucket
- DeleteBucket
- GetBucket
Managing Objects

In the Oracle Cloud Infrastructure Object Storage service, an object is a file or unstructured data you upload to a bucket within a compartment within an Object Storage namespace. The object can be any type of data, for example, multimedia files, data backups, static web content, or logs. You can store objects that are up to 10 TiB. Objects are processed as a single entity. You can't edit or append data to an object, but you can replace the entire object.

This topic describes how to manage objects within a single bucket. For information on copying an object to another bucket, see Copying Objects.

You might also be interested in exploring an Object Storage feature that retains previous versions of objects. Among other things, object versioning protects objects from accidental or malicious overwrite or deletion. For more information, see Using Object Versioning on page 3446.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For administrators:

- The policy Let Object Storage admins manage buckets and objects on page 2149 lets the specified group do everything with buckets and objects. Objects always reside in the same compartment as the bucket.
- If you need to write a more restrictive policy for objects, the inspect objects lets you list all the objects in a bucket and do a HEAD operation for a particular object. In comparison, read objects lets you download the object itself.
- If you create more restrictive policies that grant individual permissions:
  - OBJECT_VERSION_DELETE is required to delete previous object versions on your behalf using lifecycle policies.
  - OBJECT_UPDATE_TIER is required to change the storage tier of an object.

See Details for Object Storage, Archive Storage, and Data Transfer on page 2324 for more information on Object Storage user permissions.

Pre-Authenticated Requests

Pre-authenticated requests provide a way to let users access a bucket or object without having their own credentials. For example, you can create a request that lets a user upload backups to a bucket without owning API keys. See Using Pre-Authenticated Requests on page 3482 for details.
Object Names

Unlike other resources, objects do not have Oracle Cloud Identifiers (OCIDs). Instead, users define an object name when they upload an object.

Use the following guidelines when naming an object:

- Use from 1 to 1024 characters.
- Valid characters are letters (upper or lower case), numbers, and characters other than line feed, carriage return, and NULL.

  **Important:**

  Bucket names and object names are case-sensitive. Object Storage handles q3-field-assets.xlsx and Q3-Field-Assets.XSLX as separate objects.

- Use only Unicode characters for which the UTF-8 encoding does not exceed 1024 bytes. Clients are responsible for URL-encoding characters.
- Avoid entering confidential information.
- Make the name unique within the bucket. Do not use the name of an existing object within the bucket when naming an object unless you intend to overwrite the existing object with the contents of the new or renamed object.

  **Tip:**

  Object names can include one or more forward slash (/) characters in the name. See **Object Naming Using Prefixes and Hierarchies** for more information on using the forward slash in object names to create hierarchies.

Object Naming Using Prefixes and Hierarchies

Within an Object Storage namespace, buckets and objects exist in a flat structure, but you can simulate a directory structure using a prefix string that includes the forward slash (/) to add hierarchy to an object name. Doing so lets you list one directory at a time, which is helpful when navigating a large set of objects.

For example:

```
marathon/finish_line.jpg
marathon/participants/p_21.jpg
```

If you added prefixes to object names, you can:

- Use the Console to display a hierarchical view of your objects in virtual folders. In the previous example, marathon would be displayed as a folder containing an object named finish_line.jpg and participants would be a subfolder of marathon, containing an object named p_21.jpg. You can bulk upload objects to any level of the hierarchy and perform bulk deletes of all the objects in a bucket or folder.
- Use the CLI or API to perform bulk downloads and bulk deletes of all objects at a specified level of the hierarchy.

Bulk operations at a specified level of the hierarchy do not affect objects in any level above.

When naming objects, you can also use prefix strings without a delimiter. No delimiters would allow search operations in the Console and certain bulk operations in the CL or API to match on the prefix portion of the object name. For example, in the object names below, the string gloves_27_ can serve as a prefix for matching purposes when performing bulk operations:

```
gloves_27_dark_green.jpg
gloves_27_light_blue.jpg
```

When you perform bulk uploads with the Console, CLI, or API, you can prepend a prefix string to the names of the files you are uploading.
For hierarchy and prefix string details for a particular management interface, see the individual tasks in Using the Console on page 3400, Using the Command Line Interface (CLI) on page 3404, and Using the API on page 3439.

Optional Response Headers and Metadata

When you upload objects, you can provide optional response headers and user-defined metadata. Response headers are HTTP headers sent from Object Storage to Object Storage clients when objects are downloaded. User-defined metadata are name-value pairs stored with an object. You can use the Console, REST API, or CLI to provide these optional attributes.

**Important:**

No validation is performed on the response headers or metadata you provide.

You can specify values for the following response headers:

- **Content-Disposition**
  
  Defines presentation only information for the object. Specifying values for this header has no effect on Object Storage behavior. Programs that read the object determine what to do based on the value provided. For example, you could use this header to let users download objects with custom file names in a browser:

  
  ```
  attachment; filename="fname.ext"
  ```

  See https://tools.ietf.org/html/rfc2616#section-19.5.1 for more information.

- **Cache-Control**
  
  Defines the caching behavior for the object. Specifying values for this header has no effect on Object Storage behavior. Programs that read the object determine what to do based on the value provided. For example, you could use this header to identify objects that require caching restrictions:

  ```
  no-cache, no-store
  ```


You specify user-defined metadata in the form of name-value pairs. User-defined metadata names are stored and returned to Object Storage clients with the mandatory prefix of **opc-meta-**.

Object Lifecycle Management

Object Lifecycle Management lets you automatically manage the deletion of uncommitted multipart uploads, the movement of objects to a different storage tier, and the deletion of supported resources on your behalf within a given bucket. These automated actions are based on rules that you define and manage. See Using Object Lifecycle Management on page 3466 for more information about this feature.

Multipart Uploading and Downloading

The Oracle Cloud Infrastructure Object Storage service supports multipart uploading and downloading for objects.

- For information about the API and CLI multipart uploading functionality, see Using Multipart Uploads on page 3477.
- For CLI information on multipart downloading, see downloading an object using multipart download.
- For API documentation related to multipart downloading, see the GetObject API call and its range parameter.

Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.
For more information about monitoring objects, see Object Storage Metrics on page 3499.

**Creating Automation for Objects Using the Events Service**

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

Events for objects are handled differently than other resources. Objects do not emit events by default. Use the Console, CLI, or API to enable a bucket to emit events for object state changes. You can enable events for object state changes during or after bucket creation.

**Using Storage Gateway to Upload and Download Objects**

Storage Gateway is another way you can upload objects to and download objects from Oracle Cloud Infrastructure Object Storage.

Storage Gateway is installed in an Oracle Cloud Infrastructure compute instance or as a Linux Docker instance on one or more hosts in your on-premises data center. Applications store and retrieve objects from Oracle Cloud Infrastructure Object Storage through file systems that you create in Storage Gateway. Storage Gateway exposes an NFS mount point that can be mounted to any host that supports an NFSv4 client. The Storage Gateway mount point maps to an Object Storage bucket to upload and download objects.

See Overview of Storage Gateway on page 3790 for details.

**Using the Console**

**To upload objects to a bucket or folder**

The Console uses multipart uploads to upload objects larger than 64 MiB.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your objects are larger than 64 MiB and will be uploaded using multipart uploads, you need OBJECT_CREATE and OBJECT_OVERWRITE permissions.</td>
</tr>
</tbody>
</table>

See Using Multipart Uploads on page 3477 and Details for Object Storage, Archive Storage, and Data Transfer on page 2324 for details.

1. From the Object Storage Buckets screen, click the bucket name to view its details.
2. Click Objects under Resources.
3. To upload objects to the bucket, click Upload. To upload objects to a folder in the bucket, click the Actions icon (three dots) to the right of the folder that you want to upload objects to, then click Upload.
4. Optionally, specify an Object Name Prefix. If provided, this prefix is prepended to each one of the files you upload. You can specify the following prefix strings:
   - Prefix strings with a forward slash (/) delimiter to simulate hierarchy and create folders or subfolders
   - Prefix strings without a delimiter for matching purposes to perform allowed bulk operations

   See Object Naming Using Prefixes and Hierarchies on page 3420 for more details.
5. If the Storage Tier field displays Standard, you can optionally change the tier to upload objects to:
   - Infrequent Access
   - Archive
6. Select the object or objects that you want to upload in one of two ways:
   • Drag and drop one or more files from your computer.
   • Click the select files link to display a file selection dialog box.

   The files you select to upload are displayed in a list. If you decide that you do not want to upload a particular file, click the X to the right of the file name.

   If the files you select to upload are already stored in the bucket or folder with the same name, the Console displays messages warning you of an overwrite.

7. To specify values for optional response headers and metadata to be displayed in Object Details, click Show Optional Response Headers and Metadata.
   a. Select the attribute Type that you are adding.
   b. To add a Response Header, select the Name and enter a Value.
   c. To add Metadata, enter the Name and Value.
   d. To add attributes, click + Add More Headers or Metadata.

8. Click Upload.

   The selected objects are uploaded and displayed in the list of objects in the bucket or folder.

**To download an object from a bucket or folder**

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment that contains the bucket that contains your object.
   
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click Objects under Resources.
   
   A list of folders and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object that you want to download.
6. For the object you want to download, click the Actions icon (three dots), and then click Download.

**To create a folder or subfolder**

If the Virtual Folders view is enabled, you can create a folder in a bucket or you can create a subfolder in an existing folder or subfolder.

1. From the Object Storage Details screen, click the bucket name to view its details.
2. Click Objects under Resources.
3. To create a folder in a bucket, click More Actions above the Objects table, then click Create New Folder. To create a subfolder in a folder or subfolder, click the Actions icon (three dots) to the right of the folder that you want to create a folder or subfolder, then click Create New Folder.
4. Enter a Name for the folder or subfolder. Avoid entering confidential information.
5. Click Create.
   
   The folder or subfolder is created and displayed in the Objects table.

**To view object details**

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment that contains the bucket that contains your object.
   
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click Objects under Resources.
   
   A list of folders and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object for which you want details.
6. Choose the object for which you want details.
7. Click the Actions icon (three dots), and then click **View Object Details**. Object details include:
   - Basic Information
   - Response Headers
   - Metadata
8. Optionally, click **Download** to download the selected object.

**To rename an object**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment that contains the bucket that contains your object.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click **Objects** under **Resources**.
   A list of folders and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object that you want to rename.
6. For the object you want to rename, click the Actions icon (three dots), and then click **Rename**.
7. In the **Rename Object** dialog box, provide the new name for the object and an optional delimited directory structure prefix. For example, `p_94.jpg` or `/marathon/participants/p_94.jpg`.

   Avoid entering confidential information.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets cannot store two objects that use identical names (case-sensitive). If you choose to rename an object using the name of another object in the same bucket, the object that originally used the name is overwritten.</td>
</tr>
</tbody>
</table>

8. Click **Save Changes**.

**To determine which storage tier an object resides**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment that contains the bucket that contains your object.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click **Objects** under **Resources**.
   A list of folders and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object for which you want details.
6. The **Storage Tier** column identifies the storage tier in which each object resides.

**To update the storage tier of an object**

You can only update the storage tier for objects that reside in the **Standard** and **Infrequent Access** tiers. You cannot update the storage tier for objects that reside in the **Archive** tier.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You also need to understand the ramifications of updating the storage tier for an object. Objects in the Archive and Infrequent Access tiers have a minimum storage retention period and data retrieval fees. For more information, see <strong>Understanding Storage Tiers</strong> on page 3396.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You need OBJECT_UPDATE_TIER permissions to update the storage tier of an object.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment that contains the bucket that contains your object.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click **Objects** under **Resources**.
   A list of folders and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object for which you want to update the storage tier.
6. Choose the object for which you want to update the storage tier.
7. Click the Actions icon (three dots), and then click **Update Storage Tier**.
8. In the **Update Storage Tier** dialog, select from the available storage tiers.
9. Click **Save Changes**.

**To restore objects from Archive Storage**

Depending on the size of the object, it can take at most an hour to restore an object from Archive Storage. You cannot download an item until the item is fully restored.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You need OBJECT_RESTORE permissions to restore Archive Storage objects.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment your bucket is in.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click **Objects** under **Resources**.
   A list of folders (if enabled) and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object that you want to restore.
6. To restore a single object, click the Actions icon (three dots) to the right of the object you want to restore, and then click **Restore**. To restore multiple objects, select the check boxes to the left of each object you want to restore, then click **Restore**.
7. Optionally, specify the **Time Available for Download in Hours**.
   By default, you have 24 hours to download an object after restoration. However you can alternatively specify a download time of from 1 to 240 hours. You can find out how much download time is remaining by looking at **Available for Download** in object **Details** or by looking at the Actions icon (three dots) menu to the right of **Download**. Refresh the browser to obtain up-to-date remaining download time information.
   After the allotted download time expires, the object returns to Archive Storage.
8. Click **Restore Objects**.
   Error messages are generated if there is a problem with restoring the selected objects. You can optionally click **Retry failed restore option**.

**To check the status of an Archive Storage object restoration**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment your bucket is in.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click **Objects** under **Resources**.
   A list of folders and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object for which you want to check the restoration status.
6. Check the **Status** field in the **Object** table.

   **Status** displays one of the following:
   
   • Archived
   • Restoring
   • Restored

**To re-encrypt an object**

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You need OBJECT_READ and OBJECT_OVERWRITE permissions to re-encrypt an object.</td>
</tr>
</tbody>
</table>

To encrypt and decrypt an object's data encryption keys with a different master encryption key, you can re-encrypt the object. When re-encrypting an object, you can choose either a different key from the one assigned to the bucket or the most recent version of the key assigned to the bucket. Until you explicitly re-encrypt an object, the key version associated with the bucket (when the object was inserted into the bucket) continues to decrypt all the object's data encryption keys.

You can re-encrypt an object's data encryption keys with a key managed by Oracle, a key that you created and control through a vault that you manage, or a customer-provided encryption key (SSE-C).

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use server-side encryption with customer-provided keys (SSE-C), you must use the CLI to provide the SSE-C key during the encryption or re-encryption process. Using the CLI, you can re-encrypt an object with a different SSE-C key, a key managed by Oracle, or a key that you manage through the Vault service. In the Console, you can only re-encrypt an object to use the latest version of the Oracle-managed key assigned to the bucket or the latest version of a Vault key. It does not matter whether the chosen key version is the one assigned to the bucket.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

   A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. Click the name of the bucket that has the object for which you want to re-encrypt data encryption keys.

3. Under **Objects**, find the object that you want to re-encrypt. Click the Actions icon (three dots), and then click **Re-encrypt**.

4. Do one of the following, depending on whether the key assigned to the bucket is an Oracle-managed key or a key in a vault that you manage:
   
   • For buckets encrypted with an Oracle-managed key, you can re-encrypt the object with the latest version of that key by clicking **Use the key assigned to the bucket**. Or, you can re-encrypt the object with a key in a vault by clicking **Use a customer-managed key** and then choosing a key from a compartment and vault that you have access to.
   
   • For buckets encrypted with a customer-managed key, you can re-encrypt the object with the latest version of that key by clicking **Use the key assigned to the bucket**. Or, you can re-encrypt the object with a different Vault key by clicking **Use a different customer-managed key** and then choosing another key from a compartment and vault that you have access to.

5. When you are ready, click **Re-encrypt** to re-encrypt all data encryption keys associated with the object.

If you receive an error, verify that you have the correct permissions. If you have access to the object, confirm that the object exists and has not recently been deleted. If you have permissions and the object exists, also confirm whether the object is encrypted with an SSE-C key. To re-encrypt an object that you encrypted with an SSE-C key, you need to use the CLI to provide the SSE-C key to the Object Storage service for use during decryption and subsequent re-encryption, as appropriate. For more information, see the **To re-encrypt an object** on page 3436 CLI topic.
To delete objects from a bucket or a folder

You can permanently delete an object from a bucket or folder. You cannot, however, recover a deleted object unless you have object versioning enabled. See Using Object Versioning on page 3446 for details.

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment that contains the bucket that contains the object or objects you want to delete. A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click Objects under Resources. A list of folders and objects in the bucket are displayed.
5. Expand the folders and subfolders as needed to locate the object or objects that you want to delete.
6. To delete a single object, click the Actions icon (three dots) to the right of the object you want to delete, and then click Delete. To delete multiple objects, select the check boxes to the left of each object you want to delete, and then click Delete.
7. Confirm when prompted.

Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

Note:
The examples in this section use the full syntax for parameters, for example --namespace and --bucket-name. Sometimes, there are shortened parameter terms that you can use instead of the full ones, for example -ns for --namespace and -bn for --bucket-name. The CLI online --help for a particular command displays the shortened parameters that you can use.

To list the objects in a bucket

oci os object list --namespace <object_storage_namespace> --bucket-name <bucket_name>

By default, a minimal number of fields are returned for each object. For example:

oci os object list --namespace MyNamespace --bucket-name MyBucket

```json
{
  "data": [
    {
      "etag": "7588e71f-433f-4518-ba2d-90082208bd5d",
      "md5": "As+3syaEbVhPnm8fM+DSAw==",
      "name": "eventslogreference.htm",
      "size": 13515,
      "storage-tier": "InfrequentAccess",
      "time-created": "2021-01-11T15:47:44.427000+00:00",
      "time-modified": "2021-01-11T15:44.441000+00:00"
    },
    {
      "etag": "833c7099-f74e-4ce5-a7c8-ffa29a12d88",
      "md5": "J19Yxzog5HsbPSANkTVyG==",
      "name": "flowlogreference.htm",
      "size": 16601,
      "storage-tier": "Archive",
      "time-created": "2021-01-11T15:44.617000+00:00",
      "time-modified": "2021-01-11T15:44.638000+00:00"
    }
  ]
}``
To get object details

```bash
oci os object head --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name>
```

For example:

```bash
oci os object head --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt
```

If the object resides in an Archive tier bucket, the output also includes `archival-state`.

To upload an object to a bucket

```bash
oci os object put --namespace <object_storage_namespace> --bucket-name <bucket_name> --file <file_location> --storage-tier <object_storage_tier> --name <object_name> --no-multipart
```

`<file_location>` is the source directory path of the object being uploaded, such as `C:\workspace\Uploads\MyFile.txt` or `/home/user/Documents/Uploads/MyFile.txt`.

If you are uploading to a Standard tier bucket, you can optionally specify the `<object_storage_tier>` to upload the object to:

- InfrequentAccess
- Archive

If you do not specify --storage-tier option, the object is uploaded to the default storage tier of the bucket.
Object Storage

<object_name> is the name of the uploaded object excluding the path. This parameter is required if the object is being read from STDIN. If you want to use the filename as the uploaded object’s name (if not being read from STDIN), omit the --name option. The resulting object name does not include the path information (for example, C:\workspace\Uploads\, just the actual file name by itself (MyFile.txt).

An object can be uploaded as a single part or as multiple parts. Use the --no-multipart option to upload as a single part. For detailed information on multipart uploads, see Using Multipart Uploads on page 3477.

For example, to upload an object to the default storage tier of the bucket:

```bash
oci os object put --namespace MyNamespace --bucket-name MyBucket --file C:\workspace\Uploads\MyFile.txt --name MyFile.txt --no-multipart
{
"etag": "cadb9f8a-3292-45e6-a1e8-f075699fb619",
"last-modified": "Fri, 11 Dec 2020 14:04:19 GMT",
"opc-content-md5": "9P610SaYe4fXXaeK8siuDw=="
}
```

For example, to upload an object using the original filename, omit the --name option:

```bash
oci os object put --namespace MyNamespace --bucket-name MyBucket --file C:\workspace\Uploads\MyFile.txt --no-multipart
{
"etag": "cadb9f8a-3292-45e6-a1e8-f075699fb619",
"last-modified": "Fri, 11 Dec 2020 14:04:19 GMT",
"opc-content-md5": "9P610SaYe4fXXaeK8siuDw=="
}
```

For example, to upload an object to the Infrequent Access tier:

```bash
oci os object put --namespace MyNamespace --bucket-name MyBucket --file C:\workspace\Uploads\MyDocument.txt --storage-tier InfrequentAccess --no-multipart
{
"etag": "6b292cla-b01b-4f36-97c8-4567fb43d071",
"last-modified": "Sat, 12 Dec 2020 12:58:01 GMT",
"opc-content-md5": "9P610SaYe4fXXaeK8siuDw=="
}
```

For example, to upload an object to the Archive tier:

```bash
oci os object put --namespace MyNamespace --bucket-name MyBucket --file C:\workspace\Uploads\MyDocument.txt --storage-tier Archive --no-multipart
{
"etag": "6b292cla-b01b-4f36-97c8-4567fb43d071",
"last-modified": "Sat, 12 Dec 2020 12:58:01 GMT",
"opc-content-md5": "9P610SaYe4fXXaeK8siuDw=="
}
```

To add optional response headers, use one or more of the following options:

- --cache-control
- --content-disposition
- --content-encoding
- --content-language
- --content-disposition
- --content-type

For more information about attributes that you can add when you upload an object, see Optional Response Headers and Metadata on page 3421. For more details about these headers, see the Command Line Reference.
For example:

```
oci os object put --namespace MyNamespace --bucket-name MyBucket --file C:\workspace\MyFile --cache-control no-cache --no-multipart
```

To add custom metadata key-value pairs, use the `--metadata` option:

```
oci os object put --namespace <object_storage_namespace> --bucket-name <bucket_name> --file <file_location> --name <object_name> --metadata <json_formatted_key-value_pairs> --no-multipart
```

`<JSON-formatted_key-value_pair>` is a key-value pair input as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for more information about JSON formatting.

For example:

```
oci os object put --namespace MyNamespace --bucket-name MyBucket --file C:\workspace\MyFile.txt --metadata '{"Department": "Finance"}' --no-multipart
```

To bulk upload objects to a bucket

```
oci os object bulk-upload --namespace <object_storage_namespace> --bucket-name <bucket_name> --src-dir <source_directory_location>
```

`<source_directory_location>` is the upload directory path, such as `C:\workspace\Upload\` or `/home/user/Documents/Upload`. If your source directory has subdirectories, the subdirectory names are prepended to the names of the files stored in those subdirectories, delimited with a forward slash (/) character. For example, if a file named `maple.jpg` is stored in the subdirectory `trees`, when the file is uploaded, Object Storage assigns the name `trees/maple.jpg` to the resulting object.

If you are uploading to a Standard tier bucket, you can optionally specify the `<object_storage_tier>` to upload the object to:

- InfrequentAccess
- Archive

If you do not specify `--storage-tier` option, the object is uploaded to the default storage tier of the bucket.

For example, to upload objects to the default storage tier of the bucket:

```
oci os object bulk-upload --namespace MyNamespace --bucket-name MyBucket --src-dir C:\workspace\Files
```

Uploaded logFile.log [########################################] 100%
Uploaded MyFile.txt [########################################] 100%

```
For example, to upload objects to the Infrequent Access storage tier:

```bash
oci os object bulk-upload --namespace MyNamespace --bucket-name MyBucket --src-dir C:\workspace\Files --storage-tier InfrequentAccess
```

Uploaded logFile.log [########################################] 100%
Uploaded MyFile.txt [########################################] 100%

```
{
  "skipped-objects": [],
  "upload-failures": {},
  "uploaded-objects": {
    "MyFile.txt": {
      "etag": "e25f95e6-a2bd-435c-83d6-785f838134d5",
      "last-modified": "Sat, 12 Dec 2020 11:31:36 GMT",
      "opc-content-md5": "vqglL/ToD0FxnuqE83wBycw=="
    },
    "logFile.log": {
      "etag": "bbcf33dd-a177-4406-bed1-a4f7125da800",
      "last-modified": "Sat, 12 Dec 2020 11:31:36 GMT",
      "opc-content-md5": "K8vB8NVAS1vtL2BE5ksUjw=="
    }
  }
}
```

For example, to upload objects to the Archive tier:

```bash
oci os object bulk-upload --namespace MyNamespace --bucket-name MyBucket --src-dir C:\workspace\Files --storage-tier Archive
```

Uploaded logFile.log [########################################] 100%
Uploaded MyFile.txt [########################################] 100%

```
{
  "skipped-objects": [],
  "upload-failures": {},
  "uploaded-objects": {
    "MyFile.txt": {
      "etag": "e25f95e6-a2bd-435c-83d6-785f838134d5",
      "last-modified": "Sat, 12 Dec 2020 11:31:36 GMT",
      "opc-content-md5": "vqglL/ToD0FxnuqE83wBycw=="
    },
    "logFile.log": {
      "etag": "bbcf33dd-a177-4406-bed1-a4f7125da800",
      "last-modified": "Sat, 12 Dec 2020 11:31:36 GMT",
      "opc-content-md5": "K8vB8NVAS1vtL2BE5ksUjw=="
    }
  }
}
```

To append a prefix string to the object names created by your uploads, use the `--object-prefix` option. For example:

```bash
oci os object bulk-upload --namespace MyNamespace --bucket-name MyBucket --src-dir C:\workspace\Files --object-prefix /bicycling/gloves/
```

Uploaded /bicycling/gloves/gloves_27_A.jpg [########################################] 100%
Uploaded `/bicycling/gloves/gloves_31_A.jpg`
[########################################] 100%
{
    "skipped-objects": [],
    "upload-failures": {},
    "uploaded-objects": {
        "/bicycling/gloves/gloves_27_A.jpg": {
            "etag": "7ba793ce-a341-4c56-9baf-61ca2c56ad50",
            "last-modified": "Sat, 12 Dec 2020 18:35:09 GMT",
            "opc-content-md5": "1B2M2Y8AsgTpgAmY7PhCfg="
        },
        "/bicycling/gloves/gloves_31_A.jpg": {
            "etag": "6efa58a6-a723-4696-a31f-3c5099adbec4",
            "last-modified": "Sat, 12 Dec 2020 18:35:09 GMT",
            "opc-content-md5": "6GxlLP9fa71HvnpLNJ+DQ=="
        }
    }
}

To add custom metadata key-value pairs, use the `--metadata <JSON_formatted_key-value_pairs>` option.

*<JSON-formatted_key-value_pairs>* is a key-value pair input as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

**To download an object from a bucket**

```bash
oci os object get --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --file <file_location>
```

*<file_location>* is the destination path for the file being downloaded, such as `C:\workspace\Downloads\MyFile.txt` or `/home/user/Documents/Downloads/MyFile.txt`.

The `--name <object_name>` parameter is required.

For example:

```bash
oci os object get --namespace MyNamespace --bucket-name MyBucket --file c:\workspace\Downloads\MyFile.txt --name MyFile.txt
```

No information is returned when you run the command. The file is downloaded to the specified destination.

**To download an object using multipart download**

Multipart object downloading is available using the byte-range request standard defined in [RFC 7233, section 2.1](https://tools.ietf.org/html/rfc7233).

```bash
oci os object get --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --file <file_location> --range bytes=<byte_range>
```

For example:

```bash
oci os object get --namespace MyNamespace --bucket-name MyBucket --name MyObject.mp4 --file c:\workspace\Downloads\MyObject.mp4 --range bytes=0-499
```

**To bulk download all objects within a bucket**

```bash
oci os object bulk-download --namespace <object_storage_namespace> --bucket-name <bucket_name> --download-dir <download_directory_location>
```
<download_directory_location> is the destination path for the objects being downloaded, such as C:\workspace \Downloads\ or /home/user/Documents/Downloads/. If the directory does not exist, Object Storage creates the directory when the command is run.

For example:

```
oci os object bulk-download --namespace MyNamespace --bucket-name MyBucket --download-dir c:\workspace\Downloads
```

Downloaded MyFile.txt [############################] 100%
Downloaded logFile.log [############################] 100%

```
{
  "download-failures": {},
  "skipped-objects": []
}
```

For a complete list of object bulk download options, see the Command Line Reference.

**To bulk download objects by object name prefix string**

If you have named your objects with prefix strings, you can bulk download objects in a bucket that match a specified prefix string.

```
oci os object bulk-download --namespace <object_storage_namespace> --bucket-name <bucket_name> --download-dir <download_directory_location> --prefix <prefix_string>
```

<download_directory_location> is the destination path for the objects being downloaded, such as C:\workspace \Downloads\ or /home/user/Documents/Downloads/. If the directory does not exist, Object Storage creates the directory when the command is run.

For example:

```
oci os object bulk-download --namespace MyNamespace --bucket-name MyBucket --download-dir c:\workspace\Downloads --prefix gloves_27
```

In the example above, an object named gloves_27_A.jpg is downloaded, while an object named gloves_31_A.jpg is not downloaded.

If you named your objects so that they exist in Object Storage in a hierarchy, you can download objects at a specified level and below. Specify the prefix that matches the level of your choosing:

```
oci os object bulk-download --namespace <object_storage_namespace> --bucket-name <bucket_name> --download-dir <download_directory_location> --prefix <level_1/level_2/>
```

The preceding command downloads the following objects:

- <level_1/level_2/object_name>
- <level_1/level_2/level_3/object_name>
- <level_1/level_2/level_3/level_4/object_name>

To download only those objects at a given hierarchy level (and not objects in levels above or below), see To bulk download objects at a specified hierarchy level.
To bulk download objects at a specified hierarchy level

If you named your objects so that they exist in Object Storage in a hierarchy, you can bulk download all objects at a specified hierarchy level.

```
oci os object bulk-download --namespace <object_storage_namespace> --bucket-name <bucket_name> --download-dir <download_directory_location> --prefix <level_1/level_2/> --delimiter /
```

`<download_directory_location>` is the destination path for the objects being downloaded, such as `C:\workspace\Downloads\` or `/home/user/Documents/Downloads/`. If the directory does not exist, Object Storage creates the directory when the command is run.

**Note:**
Currently, only the forward slash (`/`) is the supported delimiter for the `--delimiter` option.

The preceding command downloads objects only at `<level_2>` of the hierarchy. For example, the following object is downloaded:

`<level_1/level_2/object_name>`

The preceding command does not download objects in levels above or below `<level_2>`. For example, the preceding command does not download the following objects:

- `<level_1/object_name>`
- `<level_1/level_2/level_3/object_name>`
- `<level_1/level_2/level_3/level_4/object_name>`

To download objects at a given hierarchy level along with all objects in the hierarchy sublevels, see To bulk download objects by object name prefix string.

To rename an object

```
oci os object rename --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_original_name> --new-name <object_new_name>
```

For example:

```
oci os object rename --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --new-name MyRenamedFile.txt

{
  "etag": "3504606b-8412-4b5d-924a-aeeacfd1df1e"
}
```

To make the rename operation dependent on the object having a specific entity tag, use the `--src-obj-if-match-e-tag` option.

For example:

```
oci os object rename rename --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --new-name MyRenamedFile.txt --src-obj-if-match-e-tag 6672BECB67CCFFBCE0530292F20ZBACE
```

For rename operations where you intend to overwrite one object in a bucket with another, you can make the renaming dependent on having a specific entity tag. To do so, use the `--new-obj-if-match-e-tag` option.
For example:

```
oci os object rename rename --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --new-name MyRenamedFile.txt --new-obj-if-match-e-tag 6672BECB67CCFDBCE0530292F20ZBACE
```

When renaming an object, you can prevent the system from overwriting another object in the same bucket by using the `--new-obj-if-none-match-e-tag *` option. This option prevents the renaming operation from completing if an object exists with the `--new-name` value specified and the same entity tag of the source object.

For example:

```
oci os object rename rename --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --new-name MyRenamedFile.txt --new-obj-if-none-match-e-tag *
```

To determine which storage tier an object resides

```
oci os object head --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name>
```

For example:

```
oci os object head --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt
{
  "accept-ranges": "bytes",
  "access-control-allow-credentials": "true",
  "access-control-allow-methods": "POST,PUT,GET,HEAD,DELETE,OPTIONS",
  "access-control-allow-origin": "*",
  "access-control-expose-headers": "accept-ranges,access-control-allow-credentials,access-control-allow-methods,access-control-allow-origin,content-length,content-md5,content-type,etag,last-modified,opc-client-info,opc-client-request-id,opc-request-id,x-api-id",
  "content-length": "823",
  "content-md5": "9P61OsaYe4fXxaeK8siu Dw==",
  "content-type": "application/octet-stream",
  "date": "Fri, 11 Dec 2020 14:22:51 GMT",
  "etag": "cadb9f8a-3292-45e6-a1e8-f075699fb619",
  "last-modified": "Fri, 11 Dec 2020 14:04:19 GMT",
  "opc-client-request-id": "C732DB8E25BC406FB35974D18C78D4",
  "opc-request-id": "phx-1:EzxtLDJJxPwDluQ30AEyB8R6X_CEYrxKK2rEYq23k8EQD749g2YtK01hx4jJdVwah3",
  "storage-tier": "InfrequentAccess",
  "version-id": "82d3a264-08c4-4732-a9b1-e246ee0e4fa1",
  "x-api-id": "native"
}
```

If the object resides in an Archive tier bucket, the output also includes `archival-state`.

You can also determine which storage tier an object resides by listing the objects or object versions for a bucket. See To list the objects in a bucket.

To update the storage tier of an object

```
oci os object update-storage-tier --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --storage-tier <object_storage_tier>
```
For example:

```
oci os object update-storage-tier --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --storage-tier Archive
```

**To restore an Archive Storage tier object**

**Tip:**
You need OBJECT_RESTORE permissions to restore Archive Storage objects.

```
oci os object restore --namespace <object_storage_namespace> --bucket-name <archive_bucket_name> --name <archived_object_name> [--hours <#_of_hours>]
```

By default, you have 24 hours to download an object after restoration. However, you can optionally specify --hours with an integer value of download time of from 1 to 240 hours.

**To check the status of an Archive Storage object restoration**

```
oci os object restore-status --namespace <object_storage_namespace> --bucket-name <archive_bucket_name> --name <archived_object_name>
```

**To re-encrypt an object**

**Tip:**
You need OBJECT_READ and OBJECT_OVERWRITE permissions to re-encrypt an object.

You can re-encrypt the data encryption keys that encrypt an object. You can do so by re-encrypting the object's data encryption keys with the latest version of the master encryption key assigned to the bucket, whether it's an Oracle managed key or a key in a vault that you manage. You can also re-encrypt the object's data encryption keys with a different key in a vault or a different SSE-C key. If you use SSE-C keys, you must provide the SSE-C key during the object decryption and subsequent re-encryption process, as appropriate.

You can re-encrypt an object's data encryption keys with the latest key version of the key assigned to the bucket.

```
oci os object reencrypt --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name>
```

For example:

```
oci os object reencrypt --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt
```

The object's data encryption keys are re-encrypted with no further information returned.

If the object's data encryption keys are currently encrypted with an SSE-C key, you must also provide the name of the file that contains the base64-encoded string of the AES-256 source encryption key to first decrypt the object.

```
oci os object reencrypt --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --source-encryption-key-file <name_of_file_containing_base64-encoded_AES-256_key>
```

For example:

```
oci os object reencrypt --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --source-encryption-key-file MySSE-CKey
```
You can re-encrypt an object's data encryption keys with a specific Vault key.

```bash
oci os object reencrypt --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --kms-key-id <key_OCID>
```

For example:

```bash
oci os object reencrypt --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --kms-key-id ocid1.key.region1.sea.exampleaaacu2.examplestpsuqmoyp4m5cvblugizcoeu2nfc6b3zfaux2lmqz245gezevsq
```

Again, if the key is currently encrypted with an SSE-C key, you must also provide the name of the file that contains the base64-encoded string of the AES-256 source encryption key to first decrypt the object.

```bash
oci os object reencrypt --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --source-encryption-key-file <name_of_file_containing_base64-encoded_AES-256_key> --kms-key-id <key_OCID>
```

For example:

```bash
oci os object reencrypt --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --source-encryption-key-file MySSE-CKey --kms-key-id ocid1.key.region1.sea.exampleaaacu2.examplestpsuqmoyp4m5cvblugizcoeu2nfc6b3zfaux2lmqz245gezevsq
```

You can re-encrypt an object's data encryption keys with an SSE-C key.

```bash
oci os object reencrypt --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --encryption-key-file <name_of_file_containing_base64-encoded_AES-256_key>
```

For example:

```bash
oci os object reencrypt --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --encryption-key-file MySSE-CKey
```

If the object is currently encrypted with an SSE-C key, and you want to encrypt the object's data encryption keys with a different SSE-C key, provide the file name of each key.

```bash
oci os object reencrypt --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name> --source-encryption-key-file <name_of_file_containing_base64-encoded_AES-256_key_currently_assigned> --encryption-key-file <name_of_file_containing_base64-encoded_AES-256_key_desired>
```

For example:

```bash
oci os object reencrypt --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt --source-encryption-key-file MySSE-CKey --encryption-key-file MyNewSSE-CKey
```

**To delete an object**

If object versioning is disabled or suspended, you can permanently delete an object.

```bash
oci os object delete --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <object_name>
```
For example:

```
oci os object delete --namespace MyNamespace --bucket-name MyBucket --name MyFile.txt

Are you sure you want to delete this resource? [y/N]: y
```

The object is deleted with no further information returned.

**To bulk delete all objects within a bucket**

```
oci os object bulk-delete --namespace <object_storage_namespace> --bucket-name <bucket_name>
```

For example:

```
oci os object bulk-delete --namespace MyNamespace --bucket-name MyBucket

WARNING: This command will delete 2 objects. Are you sure you wish to continue? [y/N]:

Deleted MyRenamedFile.txt [####################################] 100%
Deleted logFile.log [####################################] 100%

{
  "delete-failures": {},
  "deleted-objects": [
    "MyRenamedFile.txt",
    "logFile.log"
  ]
}
```

To see a list of the files impacted by a bulk delete command without actually deleting the files, use the `--dry-run` option.

For example:

```
oci os object bulk-delete --namespace MyNamespace --bucket-name MyBucket --dry-run
{
  "delete-failures": {},
  "deleted-objects": [
    "MyFile.txt",
    "logFile.log"
  ]
}
```

**To bulk delete objects by object name prefix string**

If you named your objects with prefix strings, you can bulk delete objects in a given bucket by providing a prefix to match.

```
oci os object bulk-delete --namespace <object_storage_namespace> --bucket-name <bucket_name> --prefix <prefix_string>
```

For example:

```
oci os object bulk-delete --namespace MyNamespace --bucket-name MyBucket --prefix gloves_A
```

The preceding command deletes the objects `gloves_27_A.jpg` and `gloves_31_A.jpg`, but does not delete the object `shoes_1.jpg`. 
If you named your objects so that they exist in a hierarchy, specify a prefix to match to bulk delete objects at a given level and below.

```bash
oci os object bulk-delete --namespace <object_storage_namespace> --bucket-name <bucket_name> --prefix <level_1/level_2/>
```

The preceding command deletes the following files:

- `<level_1/level_2/object_name>`
- `<level_1/level_2/level_3/object_name>`
- `<level_1/level_2/level_3/level_4/object_name>`

To delete only those objects at a given hierarchy level (and not objects in levels above or below), see **To bulk delete objects at a specified hierarchy level**.

To see a list of the files impacted by a bulk delete command without actually deleting the files, use the `--dry-run` option.

**To bulk delete objects at a specified hierarchy level**

If you named your objects so that they exist in a hierarchy, you can bulk delete only those objects at a given hierarchy level (and not objects in levels above or below).

```bash
oci os object bulk-delete --namespace <object_storage_namespace> --bucket-name <bucket_name> --prefix <level_1/level_2/> --delimiter /
```

**Note:**
Currently, only the forward slash (/) is the supported delimiter for the `--delimiter` option.

The preceding bulk delete command deletes the following object:

`<level_1/level_2/>object_name`

The preceding command does not bulk delete objects in levels above or below `<level_2>`. For example, the command would not delete the following objects:

- `<level_2/object_name>`
- `<level_1/level_2/level_3/object_name>`
- `<level_1/level_2/level_3/level_4/object_name>`

To delete objects at a given hierarchy level along with all objects in the hierarchy sublevels, see **To bulk delete objects by object name prefix string**.

To see a list of the files impacted by a bulk delete command without actually deleting the files, use the `--dry-run` option.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Object Storage prepends the Object Storage namespace string and bucket name to the object name when constructing a URL for use with the API:

```
/n/<object_storage_namespace>/b/<bucket>/o/<object_name>
```

The object name is everything after the `/o/`, which could include hierarchy levels and prefix strings.

Use the following API operations to manage objects:

- **DeleteObject**
Object Storage

- GetObject
- HeadObject
- ListObjects
- PutObject (see Special Instructions for Object Storage PUT for signing request requirements)
- RenameObject
- ReencryptObject
- RestoreObjects

Using Replication

Replication provides protection from regional outages, aids in disaster recovery efforts, and addresses data redundancy compliance requirements. Maintaining multiple copies of data in regional locations closer to user access can also reduce latency.

This topic describes Object Storage replication and provides details on how to replicate the objects in one bucket to another bucket in the same region or a different region.

About Object Storage Replication

Enabling Object Storage replication is as simple as creating a replication policy on the source bucket that identifies the region and the bucket to replicate to. After the replication policy is created, the destination bucket is read-only and updated only by replication from the source bucket. Objects uploaded to a source bucket after policy creation are asynchronously replicated to the destination bucket. Objects deleted from the source bucket after policy creation are automatically deleted from the destination bucket. Objects uploaded to a source bucket before policy creation are not replicated.

Replication overwrites any object in the destination bucket that has the same name as an object in the source bucket. A replicated object has the same name, metadata, ETag, and MD5 value as the object in the source bucket. The creation timestamp, modified timestamp, and archival state can be different, so these attributes are not replicated from the source.

Required IAM Policies

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Caution:

Replication does not work if you do not authorize the Object Storage service to replicate objects on your behalf. See Service Permissions on page 3441 for more information.

User Permissions

You must have the required access to both the source and destination buckets when configuring replication. You must also have permissions to manage objects in the source and destination buckets.

For administrators:

- You can create a policy that lets the specified IAM group manage Object Storage namespaces, buckets, and their associated objects in all compartments in the tenancy. For example, here is a simple user access policy that lets a StorageAdmins group do anything with the Object Storage service resources in the tenancy:

  Allow group StorageAdmins to manage object-family in tenancy
• Alternatively, you can create policies that reduce the scope of access. For example, you can create the policies to let the StorageAdmins group manage buckets and objects in a compartment called ObjectStore in the tenancy:

| Allow group StorageAdmins to manage buckets in compartment ObjectStore |
| Allow group StorageAdmins to manage objects in compartment ObjectStore |

For more information about other alternatives for writing policies, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

**Service Permissions**

Because Object Storage is a regional service, you must authorize the Object Storage service for each region carrying out replication on your behalf. For example, you might authorize the Object Storage service in region US East (Ashburn) to manage objects on your behalf. After you authorize the Object Storage service, you can replicate the objects in a bucket in US East (Ashburn) to a bucket in another region.

To determine the region identifier value of an Oracle Cloud Infrastructure region, see Regions and Availability Domains on page 180.

For administrators:

To enable replication, you must authorize the service to manage objects on your behalf:

• For example, here is a service access policy that lets the Object Storage service do anything with the resources in the tenancy in the US West (Phoenix) region:

| Allow service objectstorage-us-phoenix-1 to manage object-family in tenancy |

• Alternatively, you can create policies that reduce the scope of access. For example, you can create a policy that lets the Object Storage service do anything with the resources in a compartment called ObjectStore in the US West (Phoenix) region:

| Allow service objectstorage-us-phoenix-1 to manage object-family in compartment ObjectStore |

• You can also create more restrictive policies that grant the individual permissions required for replication. For example:

| Allow service objectstorage-us-phoenix-1 to manage object-family in compartment ObjectStore where any {request.permission='BUCKET_READ', request.permission='BUCKET_UPDATE', request.permission='OBJECT_READ', request.permission='OBJECT_INSPECT', request.permission='OBJECT_CREATE', request.permission='OBJECT_OVERWRITE', request.permission='OBJECT_RESTORE', request.permission='OBJECT_DELETE'} |

**Scope and Constraints**

• Replication policy creation does not automatically create a destination bucket. Create the destination bucket before creating the replication policy on the source bucket.

• A source or destination bucket can be in the Standard (Object Storage) or Archive Storage tier.

• Maximum of one replication policy per bucket.

• Maximum of one destination for each replication source bucket.

• A destination bucket cannot also be a replication source. Chained replication is not supported.

• After the replication policy is created, the destination bucket is read-only and updated only by replication from the source bucket. Objects uploaded to the source bucket are automatically replicated to the destination bucket. Objects deleted from the source bucket are automatically deleted from the destination bucket.
Interaction Between Replication and Other Object Storage Features

This section describes some key things you need to know about the interaction between replication and other Object Storage features.

Lifecycle Management

You can combine replication with Lifecycle Management policies that manage the archiving and deletion of objects. Lifecycle policies must, however, honor the read-only properties of the replication destination bucket. A lifecycle policy that deletes objects from the replication destination bucket does not work. Carefully review and test any combination replication and lifecycle policies that you implement.

Here are examples of combination policies that might benefit you:

- You can create a lifecycle policy on the source that deletes objects with certain file extensions after a specified number of days. The result of that deletion would also be reflected in the replication destination.
- You can create a lifecycle policy on the destination that archives objects after a specified number of days. If you do not need immediate access to those objects, you could benefit from reduced storage costs.

Server-Side Encryption Using Your Own Keys

Replication cannot replicate objects that have been encrypted with an SSE-C key. For more information, see Using Your Own Keys for Server-Side Encryption on page 3491.

Stopping Replication

Stopping replication can be initiated from either the replication source or the destination.

- To stop replication from the source, delete the replication policy. Deleting a replication policy is permanent. You cannot recover a deleted policy. If you want to replicate to that target destination again, create a new policy.
- To stop replication from the destination, make the destination bucket writable again. When you make the bucket writable, the destination bucket no longer accepts replication requests from the source. Replication status on the source changes from active to a client error state. If you want this destination to again be the target replication destination, delete the policy on the source bucket and create a new policy.

Troubleshooting Replication

This topic provides troubleshooting solutions for issues you might encounter using replication.

Unable to create a replication policy on the source bucket

If creating a replication policy fails, the most likely cause is missing or incomplete IAM permissions. Policy creation requires:

- User permissions that let you access both the source and destination buckets and let you manage the objects in those buckets.
- Service permissions that authorize Object Storage itself to access both the source and destination bucket and their objects.

Review the existing policies that grant user and service permissions. For more information, see Required IAM Policies on page 3440.

Policy is in error on the source bucket

If the policy status changes from active to error, check these items:

- You intentionally or unintentionally stopped replication on the destination bucket. To once again replicate to this target bucket, delete the existing policy on the source bucket and create a new policy.
- Ensure that your user permissions are still in place.
- Ensure that the policies that authorize Object Storage access to the source and destination buckets and their objects are still in place.
• You might have exceeded your storage limits on the destination bucket. If you are a Free Trial or Always Free customer, your storage is limited. Upgrade to paid account or delete your replication policy.

Unable to stop replication on the destination bucket and make the bucket writable

If stopping a replication policy fails, the most likely cause is missing or incomplete IAM permissions. Policy creation requires:

• User permissions that let you access both the source and destination buckets and let you manage the objects in those buckets.
• Service permissions that authorize Object Storage itself to access both the source and destination bucket and their objects.

Review the existing policies that grant user and service permissions. For more information, see Required IAM Policies on page 3440.

Using the Console

To create a replication policy

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. Choose the compartment that contains the bucket you want to replicate from.
4. Click the bucket name.
5. Click Replication Policy under Resources to access the replication policy list.
6. Click Create Policy.
7. In the Create Policy dialog, enter the following:
   • Name: Required. The system generates a default policy name that reflects the current year, month, day, and time, for example replication-policy-20200129-2230. If you change this default to a different policy name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
   • Destination Region: Required. The Oracle Cloud Infrastructure region containing the destination bucket that you want to replicate to. Your tenancy must be subscribed to a region for you to replicate to that region.
   • Destination Bucket: The name of the destination bucket for replication. Specify an existing target bucket. Replication cannot automatically create the bucket.
8. Click Create.

After the policy is created, Replication: Source is added to Bucket Information. Objects uploaded to the source bucket after policy creation are asynchronously replicated to the destination bucket.

To view the source replication policy details

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the List Scope section, select the compartment that contains the source replication bucket.
4. Click the source replication bucket name.
5. Click Replication Policy under Resources to access the replication policy list.

To view the destination replication policy details

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the List Scope section, select the compartment that contains the destination replication bucket.
4. Click the destination replication bucket name.
5. Click Replication Policy under Resources to access the replication policy list.

To stop replication on the destination bucket and make the bucket writable

If you stop replication, the policy is removed from this destination bucket and cannot be recovered. The bucket reverts to a standard read/write bucket and is no longer a replication target.

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct replication destination region is selected from the regions menu (shown at the top of the
Console).
3. In the List Scope section, select the compartment that contains the destination replication bucket.
4. Click the destination replication bucket name.
5. Click Replication Policy under Resources to access the replication policy list.
6. Click Stop Replication.

To delete the replication policy on the source bucket
1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the List Scope section, select the compartment that contains the destination replication bucket.
4. Click the replication destination bucket name.
5. Click Replication Policy under Resources to access the replication policy list.

Using the Command Line Interface (CLI)
For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags
and options available for CLI commands, see the Command Line Reference.

To create a replication policy

```
oci os replication create-replication-policy --namespace <object_storage_namespace> --bucket-name <source_bucket_name> --destination-region <destination_region_identifier> --destination-bucket <destination_bucket_name>
```

For example:

```
oci os replication create-replication-policy --namespace MyNamespace --bucket-name MySourceBucket --destination-region us-ashburn-1 --destination-bucket MyDestinationBucket --name MyReplicationPolicy
```

```
{
    "data": {
        "destination-bucket": "MyDestinationBucket",
        "destination-region": "us-ashburn-1",
        "id": "bacb8334-b191-4026-aa65-5e4f5165ae3e",
        "name": "MyReplicationPolicy",
        "status": "ACTIVE",
        "status-message": "The policy is active.",
        "time-created": "2020-02-06T16:44:10+00:00",
        "time-last-sync": "2020-02-06T16:44:20+00:00"
    }
}
```

Objects uploaded to the source bucket after policy creation are asynchronously replicated to the destination bucket.

To view the replication policy details

```
oci os replication get-replication-policy --namespace <object_storage_namespace> --bucket-name <source_bucket_name> --replication-id <replication_policy_identifier>
```

For example:

```bash
oci os replication get-replication-policy --namespace MyNamespace --bucket-name MySourceBucket --replication-id bacb8334-b191-4026-aa65-5e4f5165ae3e
```

```
{
  "data": {
    "destination-bucket": "MyDestinationBucket",
    "destination-region": "us-ashburn-1",
    "id": "bacb8334-b191-4026-aa65-5e4f5165ae3e",
    "name": "MyReplicationPolicy",
    "status": "ACTIVE",
    "status-message": "The policy is active.",
    "time-created": "2020-02-06T16:44:10+00:00",
    "time-last-sync": "2020-02-06T16:49:40+00:00"
  }
}
```

**To list replication policies**

**Note:**

There is currently a maximum of one replication policy per bucket.

```bash
oci os replication list-replication-policies --namespace <object_storage_namespace> --bucket-name <destination_bucket_name>
```

For example:

```bash
oci os replication list-replication-policies --namespace MyNamespace --bucket-name MySourceBucket
```

```
{
  "data": [
    {
      "destination-bucket": "MyDestinationBucket",
      "destination-region": "us-ashburn-1",
      "id": "bacb8334-b191-4026-aa65-5e4f5165ae3e",
      "name": "MyReplicationPolicy",
      "status": "ACTIVE",
      "status-message": "The policy is active.",
      "time-created": "2020-02-06T16:44:10+00:00",
      "time-last-sync": "2020-02-06T16:49:40+00:00"
    }
  ]
}
```

**To list the replication source for a destination bucket**

```bash
oci os replication list-replication-sources --namespace <object_storage_namespace> --bucket-name <destination_bucket_name> --region <destination_region_identifier>
```

For example:

```bash
oci os replication list-replication-sources --namespace MyNamespace --bucket-name MyDestinationBucket --region us-ashburn-1
```

```
{
  "data": [
```
To stop replication on the destination bucket and make the bucket writable

```bash
oci os replication make-bucket-writable --namespace <object_storage_namespace> --bucket-name <destination_bucket_name> --region <destination_region_identifier>
```

For example:

```bash
oci os replication make-bucket-writable --namespace MyNamespace --bucket-name MyDestinationBucket --region us-ashburn-1
```

If the command is successful, you are returned to the prompt.

To delete the replication policy on the source bucket

```bash
oci os replication delete-replication-policy --namespace <object_storage_namespace> --bucket-name <source_bucket_name> --replication-id <replication_policy_identifier>
```

For example:

```bash
oci os replication delete-replication-policy --namespace MyNamespace --bucket-name MySourceBucket --replication-id bacb8334-b191-4026-aa65-5e4f5165ae3e
```

Are you sure you want to delete this resource? [y/N]: y

If the command is successful, you are returned to the prompt.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to use and manage replication:

- CreateReplicationPolicy
- GetReplicationPolicy
- ListReplicationPolicies
- ListReplicationSources
- MakeBucketWritable (Stops replication)

Using Object Versioning

Object versioning provides data protection against accidental or malicious object update, overwrite, or deletion.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Oracle Cloud Infrastructure pricing applies to each bucket that is enabled for versioning. You are charged for all latest object versions and...</td>
</tr>
</tbody>
</table>
This topic describes Object Storage versioning and provides details on how to create and manage object versions.

**About Object Versioning**

Object versioning is enabled at the bucket level. Versioning directs Object Storage to automatically create an object version each time a new object is uploaded, an existing object is overwritten, or when an object is deleted. You can enable object versioning at bucket creation time or later.

A bucket that is versioning-enabled can have many versions of an object. There is always one latest version of the object and zero or more previous versions.

**Understanding Object Versioning Status**

Each Object Storage bucket has object versioning status of disabled, enabled, or suspended. By default, object versioning is disabled on a bucket. It's important to understand the behavior associated with each object versioning status.

**Disabled**

If object versioning is disabled on a bucket:

- Object versioning has never been enabled on the bucket.
- When you upload an object with the same name as an existing object, the object is overwritten and the overwritten object is not retained or recoverable.
- When you delete an object, the deletion is permanent and objects are not recoverable.

**Enabled**

If object versioning is enabled on a bucket:

- When you upload an object with the same name as an existing object, the existing object becomes a previous version and the newly uploaded object becomes the latest version.
- Each uploaded object is assigned a unique version identifier. The identifier lets you direct Object Storage actions to a specific version.
- When you delete an object, Object Storage retains a version of the deleted object. For more information about object deletion, see Understanding Object Version Deletion on page 3447.
- You cannot disable object versioning. You can, however, suspend versioning.

**Suspended**

If object versioning is suspended on a bucket:

- Upload and delete behavior is the same as a bucket that has versioning disabled.
- Object versions created before versioning suspension are retained, unless you take explicit action to delete them.
- You can re-enable object versioning at any time.

**Understanding Object Version Deletion**

No object is physically deleted from a bucket that has versioning enabled until you take explicit action to do so. When you delete an object without targeting a specific version, the latest object version becomes a previous object version and a special delete marker is created that marks the deletion point. A delete marker contains only minimal metadata. If you delete a folder, a delete marker is created for each object in the folder. You can simply delete the delete marker to make that deleted version become the latest object version.
When you upload an object with the same name as the delete marker, the uploaded object becomes the latest version of the object. The delete marker remains. There can be multiple delete markers for an object and you can recover any of the previous object versions.

Object version deletion is different. When you delete an object version, the version is permanently deleted. **Permanent deletion also happens if you explicitly delete the latest version by version ID.** All delete operations that target a specific object version ID permanently deletes the data.

**Required IAM Policies**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142.

For administrators:

- You can create a policy that lets the specified IAM group manage Object Storage namespaces, buckets, and their associated objects in all compartments in the tenancy. For example, to let the IAM group StorageAdmins do everything in the tenancy:

  ```
  Allow group StorageAdmins to manage object-family in tenancy
  ```

- Alternatively, you can create policies that reduce the scope of access. For example, you can create the policies to let the StorageAdmins group manage only buckets and objects in a compartment called ObjectStore in the tenancy:

  ```
  Allow group StorageAdmins to manage buckets in compartment ObjectStore
  Allow group StorageAdmins to manage objects in compartment ObjectStore
  ```

- If you create more restrictive policies that grant individual permissions, BUCKET_UPDATE is required to enable versioning. Uploading objects, overwriting existing objects, or deleting objects require the regular permissions necessary for those operations. OBJECT_VERSION_DELETE is required to delete object versions. For example, to allow a group called StorageSupport to manage Object Storage resources, but prevent that group from permanently removing object versions:

  ```
  Allow group StorageSupport to manage object-family in tenancy where request.operation != 'DeleteObjectVersion'
  ```

For more information about other alternatives for writing policies, see [Details for Object Storage, Archive Storage, and Data Transfer](#) on page 2324.

**Scope and Constraints**

- Versioning can be enabled on a bucket in the Standard (Object Storage) or Archive Storage tier.
- Restoring an archived object is an in-place operation and does not create an object version.
- You can rename the latest version of an object, but you cannot rename a previous object version. Renaming an object creates a new object.

**Interaction Between Versioning and Other Object Storage Features**

This section describes some key things you need to know about the interaction between object versioning and other Object Storage features.

**Bucket Re-Encryption**

Bucket re-encryption (using either Oracle or your own master encryption key) also re-encrypts any existing object versions.
Lifecycle Management

Lifecycle policies can archive the latest version or previous versions of an object. When Lifecycle policies delete the latest version of an object, that object becomes a previous version and a delete marker is created. When Lifecycle policies delete a previous version of an object, that deletion is permanent.

Copying Objects

If you copy the latest version of an object to a different bucket, only the object is copied. None of the object's previous versions are copied. You can copy a previous version of an object to another bucket, but that action creates either the latest version of a new object or a new object version in the destination bucket.

Replication

- Replication cannot replicate previous object versions.
- You cannot enable versioning on a replication destination bucket. A destination bucket is read-only.

Retention Rules

- You cannot add retention rules to a bucket that has versioning enabled.
- You cannot enable versioning on a bucket with active retention rules.
- You can add retention rules to bucket that has versioning suspended. However, you cannot resume versioning with active retention rules.

Troubleshooting Versioning

This topic provides troubleshooting solutions for issues you might encounter using versioning.

Unable to enable versioning

If enabling versioning fails, the most likely cause is missing or incomplete IAM permissions. Enabling versioning requires:

- User permissions that let you use the bucket and manage the objects in that bucket.
- Minimally, BUCKET_UPDATE permissions.

Review the existing policies that grant user permissions. For more information, see Required IAM Policies on page 3448.

Unable to delete a bucket

If deleting a bucket fails, the most likely cause is that the bucket is not empty.

Caution:

You cannot recover a deleted bucket.

You can permanently delete an empty bucket. You cannot delete a bucket that contains any of the following:

- Any objects
- Previous versions of an object
- A multipart upload in progress
- A pre-authenticated request

Tip:

When you delete an object in a version-enabled bucket, a previous version of that object is created. Select Show Deleted Objects to display the object versions that might prevent you from deleting the bucket.
Unable to delete a previous object version

If deleting a previous object version fails, the most likely cause is missing or incomplete IAM permissions. Object version deletion requires:

- User permissions that let you use the bucket and manage the objects in that bucket.
- Minimally, OBJECT_VERSION_DELETE permissions.

Using the Console

To enable versioning during bucket creation

1. Follow the steps for creating a bucket.
2. Select Enable Object Versioning to direct Object Storage to create an object version each time the content changes or the object is deleted.

To enable object versioning after bucket creation

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the List Scope section, select the compartment that contains the bucket that you want to enable object versioning.
4. Click the bucket name.
5. In Bucket Information, locate Object Versioning.

   Object Versioning indicates the current versioning status. Versioning is disabled by default. If you did not enable object versioning during bucket creation, Object Versioning is Disabled.
6. Click Edit.
7. Click Enable Versioning.

To suspend object versioning

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the List Scope section, select the compartment that contains the bucket that you want to suspend object versioning.
4. Click the bucket name.
5. In Bucket Information, locate Object Versioning.

   Object Versioning indicates the current versioning status. Versioning is Enabled.
6. Click Edit.
7. Click Suspend Versioning.

To re-enable object versioning from suspension

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the List Scope section, select the compartment that contains the bucket that you want to re-enable object versioning.
4. Click the bucket name.
5. In Bucket Information, locate Object Versioning.

   Object Versioning indicates the current versioning status. Versioning is Suspended.
6. Click Edit.
7. Click Enable Versioning.

To view the latest version of an object

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the bucket that you want to see the list of object versions.

4. Click the bucket name.

5. Click **Objects** under **Resources**.

6. Expand any folders and subfolders as needed to find the object for which you want to display previous versions.

   The latest version of each object is displayed.

**To view the previous versions of an object**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).

3. In the **List Scope** section, select the compartment that contains the bucket that you want to see the list of object versions.

4. Click the bucket name.

5. Click **Objects** under **Resources**.

6. Expand any folders and subfolders as needed to find the object for which you want to display previous versions.

   The latest version of each object is displayed.

7. Locate the object for which you want to display previous versions.

8. Click the file expander, located to the left of the the Actions icon (three dots).

   The list of all previous versions of the object is displayed.

**To view the details of an object version**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).

3. In the **List Scope** section, select the compartment that contains the bucket that has the object version that you want to delete.

4. Click the bucket name.

5. Click **Objects** under **Resources**.

   A list of folders and the latest versions of objects in the bucket are displayed.

6. Expand any folders and subfolders as needed to locate the object for which you want to view details.
7. To display the details for the latest version of an object, click the Actions icon (three dots) to the right of the object, and then click **View Object Details**.

8. To display the details for a previous version of an object, click the file expander, located to the left of the the Actions icon (three dots).

The list of all previous versions of the object is displayed.

9. Click the Actions icon (three dots) to the right of the object version, and then click **View Object Details**.

**To delete an object**

When versioning is enabled, deleting an object without targeting a specific version creates a delete marker and a previous version of the object that can be recovered.

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the bucket that has the object that you want to delete.
4. Click the bucket name.
5. Click **Objects** under **Resources**.

A list of folders and objects in the bucket are displayed.

6. Expand any folders and subfolders as needed to locate the object that you want to delete.
7. Click the Actions icon (three dots) to the right of the object, and then click **Delete**.
8. Confirm the deletion when prompted.

**To delete the previous version of an object**

When versioning is enabled, deleting an object without targeting a specific version creates a delete marker and previous version of the object that can be recovered. However, **deleting a previous version of an object is a permanent deletion.**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the bucket that has the object version that you want to delete.
4. Click the bucket name.
5. Click **Objects** under **Resources**.

   A list of folders and objects in the bucket are displayed.

6. Expand any folders and subfolders as needed to locate the object for which you want to delete a previous version.

7. Click the file expander, located to the left of the the Actions icon (three dots).

   ![Objects](image)

   The list of all previous versions of the object is displayed.

8. Locate the previous version of the object that you want to delete.

9. Click the Actions icon (three dots) to the right of the object version, and then click **Delete**.

10. Confirm the deletion when prompted.

**To recover a deleted object version**

   Recovering a deleted object version is as simple as deleting the delete marker that was created when you deleted the latest version of an object. The previous version of the object listed just below the delete marker is recovered and becomes the latest version of the object.

   1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
   2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
   3. In the **List Scope** section, select the compartment that contains the bucket that has the object version that you want to recover.
   4. Click the bucket name.
   5. Click **Objects** under **Resources**.

      A list of folders and objects in the bucket are displayed.

   6. Select **Show Deleted Objects**.
   7. Expand any folders and subfolders as needed to locate the object that you want to recover.
   8. Click the file expander, located to the located to the left of the the Actions icon (three dots) of the deleted object to display the versions that you can recover.
   9. Click the Actions icon (three dots) to the right of the delete marker of the object, and then click **Delete**.
   10. Confirm deletion when prompted.

**Using the Command Line Interface (CLI)**

   For information about using the CLI, see [Command Line Interface (CLI)](CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the [Command Line Reference](Reference).
To determine the object versioning status for a bucket

```
oci os bucket get --namespace <object_storage_namespace> --name <bucket_name>
```

For example:

```
oci os bucket get --namespace MyNamespace --name MyBucket
{
   "approximate-count": null,
   "approximate-size": null,
   "compartment-id": "ocid1.compartment.oc1..aaaaaaaamnk2ilreg5fkgu7rarfbbhdv3a5j4e1xxgk14uprbqk6aefv5sq",
   "created-by": "ocid1.user.oc1..aaaaaaaah46lg3ueuftovn3urjgst1g4laxnre3djelu5jxy5uaqhgy7acgq",
   "defined-tags": {
      "Financials": {
         "key1": "nondefault"
      }
   },
   "etag": "79833b3f-89bd-41ac-bf86-0fbe331f3071",
   "freeform-tags": {},
   "id": "ocid1.bucket.oc1.phx.aaaaaaaa4feuzkcdagy77lxujdneuvoiza7rh2unbpzmywytinbxymy5zku6q",
   "is-read-only": false,
   "kms-key-id": null,
   "metadata": {},
   "name": "MyBucket",
   "namespace": "MyNamespace",
   "object-events-enabled": false,
   "object-level-audit-mode": "Disabled",
   "object-lifecycle-policy-etag": null,
   "public-access-type": "NoPublicAccess",
   "replication-enabled": false,
   "storage-tier": "Standard",
   "time-created": "2020-04-14T14:25:32.465000+00:00",
   "versioning": "Disabled"
},
"etag": "79833b3f-89bd-41ac-bf86-0fbe331f3071"
}
```

To enable versioning during bucket creation

To enable versioning in a Standard tier bucket, you do not need to explicitly set `--storage-tier` because a bucket is created in the standard Object Storage tier by default:

```
oci os bucket create --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --versioning enabled
```

For example:

```
oci os bucket create --namespace MyNamespace --name MyStandardBucket --compartment-id ocid.compartment.oc1..exampleuniqueID --versioning enabled
{
   "data": {
      "approximate-count": null,
      "approximate-size": null,
      "compartment-id": "ocid1.compartment.oc1..aaaaaaaamnk2ilreg5fkgu7rarfbbhdv3a5j4e1xxgk14uprbqk6aefv5sq",
```
To enable versioning in an Archive tier bucket, you must explicitly set --storage-tier Archive:

```
oci os bucket create --namespace <object_storage_namespace> --name <archivebucket_name> --compartment-id <target_compartment_id> --storage-tier Archive
```

For example:

```
oci os bucket create --namespace MyNamespace --name MyArchiveBucket --compartment-id ocid.compartment.oc1..exampleuniqueID --storage-tier Archive --versioning enabled
```

```json

"created-by":
"ocid1.user.oc1..aaaaaaaah46lg3ueuftovn3urjgst1g41axnre3djelu5jxy5uaqgy7acgq",
"defined-tags": {
  "Financials": {
    "key1": "nondefault"
  }
},
"etag": "a91fd091-e112-483e-8e23-2b5d11e3dc2d",
"freeform-tags": {},
"id":
"ocid1.bucket.oc1.phx.aaaaaaaqagwnd5foe23xhpqk6ts754igpww5t7qrapbmr5tjiugvjoicq",
"is-read-only": false,
"kms-key-id": null,
"metadata": {},
"name": "MyStandardBucket",
"namespace": "MyNamespace",
"object-events-enabled": false,
"object-level-audit-mode": "Disabled",
"object-lifecycle-policy-etag": null,
"public-access-type": "NoPublicAccess",
"replication-enabled": false,
"storage-tier": "Standard",
"time-created": "2020-04-14T14:08:421000+00:00",
"versioning": "Enabled"
},
"etag": "a91fd091-e112-483e-8e23-2b5d11e3dc2d"
}
```
To enable object versioning after bucket creation

oci os bucket update --namespace <object_storage_namespace> --name <bucket_name> --compartment-id <target_compartment_id> --versioning Enabled

For example:

oci os bucket update --namespace MyNamespace --name MyBucket --versioning Enabled

To list object versions

oci os object list-object-versions --namespace <object_storage_namespace> --bucket-name <bucket_name>

For example:
oci os object list-object-versions --namespace MyNamespace --bucket-name MyStandardBucket
{
  "data": {
    "items": [
      {
      "etag": null,
      "is-delete-marker": false,
      "md5": null,
      "name": "MyTextDocument.txt",
      "size": null,
      "time-created": null,
      "time-modified": "2020-04-14T22:18:08.777000+00:00",
      "version-id": "2d528a44-5b15-40dc-b303-20993d1ade66"
      },
      {
      "etag": null,
      "is-delete-marker": false,
      "md5": null,
      "name": "MyTextDocument.txt",
      "size": null,
      "time-created": null,
      "time-modified": "2020-04-14T22:17:10.371000+00:00",
      "version-id": "a175ddc0-cc86-425f-bc2e-9b9bcb9b9f92"
      },
      {
      "etag": null,
      "is-delete-marker": false,
      "md5": null,
      "name": "MyTextDocument.txt",
      "size": null,
      "time-created": null,
      "time-modified": "2020-04-14T22:14:47.675000+00:00",
      "version-id": "8d8f06ef-e0c2-4435-bea6-f7c3ec80a444"
      }
    ],
    "prefixes": null
  }
}

To get the contents of an object version

oci os object get --name <object_name> --file path/to/file/name --version-id <version_identifier> --namespace <object_storage_namespace> --bucket-name <bucket_name>

For example, to retrieve the contents of an object version into a file called TextDocument.txt:


To delete an object version

oci os object delete --name <object_name> --version-id <version_identifier> --namespace <object_storage_namespace> --bucket-name <bucket_name>

For example:

oci os object delete --name MyTextDocument.txt delete --version-id 8d8f06ef-e0c2-4435-bea6-f7c3ec80a444 --namespace MyNamespace --bucket-name MyStandardBucket
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following API operations to enable object versioning:

- **CreateBucket** (enable versioning during bucket creation)
- **UpdateBucket** (enable versioning after bucket creation)

Use the following API operation to list object versions:

- **ListObjectVersions**

To perform version-specific operations, use the following APIs with a version identifier query parameter:

- **CopyObject**
- **DeleteObject**
- **GetObject**
- **HeadObject**
- **RestoreObjects**

Object-related APIs that do not take a version identifier query parameter operate only on an object, not object versions.

Using Retention Rules to Preserve Data

Retention rules provide immutable, WORM-compliant storage options for data written to Object Storage and Archive Storage for data governance, regulatory compliance, and legal hold requirements. Retention rules can also protect your data from accidental or malicious update, overwrite, or deletion. Retention rules can be locked to prevent rule modification and data deletion or modification even by administrators.

This topic describes Object Storage rule-based retention and provides details on how to create and manage these rules.

About Object Storage Data Retention

Retention rules are configured at the bucket level and are applied to all individual objects in the bucket. Object Storage provides a flexible approach to data retention that supports the following use cases.

**REGULATORY COMPLIANCE**

Your industry might require you to retain a certain class of data for a defined length of time. Your data retention regulations might also require that you lock the retention settings. If you lock the settings, the only change you can make is to increase the retention duration.

For Object Storage regulatory compliance, you create a time-bound retention rule and specify a duration. Object modification and deletion are prevented for the duration specified. Duration is applied to each object individually, and is based on the object's Last Modified timestamp. Lock the rule as required.

**DATA GOVERNANCE**

You might need to protect certain data sets as a part of internal business process requirements. While retaining the data for a defined length of time is necessary, that time period could change.

For Object Storage data governance, you create a time-bound retention rule and specify a duration. Object modification and deletion are prevented for the duration specified. Duration is applied to each object individually, and is based on the object's Last Modified timestamp. To be able to delete the rule and allow changes to the duration as required, do not lock the rule.
LEGAL HOLD

You might need to preserve certain business data in response to potential or on-going lawsuits. A legal hold does not have a defined retention period and remains in effect until removed.

For Object Storage legal holds, you create an indefinite retention rule. Object modification and deletion are prevented until you delete the rule. You cannot lock an indefinite retention rule because the rule has no duration.

It's important to understand retention duration for time-bound rules. Even though you are creating retention rules for a bucket, the duration of a rule is applied to each object in the bucket individually, and is based on the object's Last Modified timestamp. Let's say you have two objects in the bucket, ObjectX and ObjectY. ObjectX was last modified 14 months ago and ObjectY was last modified 3 months ago. You create a retention rule with a duration of 1 year. This rule prevents the modification or deletion of ObjectY for the next 9 months. The rule allows the modification or deletion of ObjectX because the retention rule duration (1 year) is less that the object's Last Modified timestamp (14 months). If ObjectX is overwritten some time in the coming year, modification and deletion would be prevented for the rule duration time remaining.

Locking a retention rule is an irreversible operation. Not even a tenancy administrator can delete a locked rule. There is a mandatory 14-day delay before a rule is locked. This delay lets you thoroughly test, modify, or delete the rule or the rule lock before the rule is permanently locked. A rule is active at the time of creation. The lock only controls whether the rule itself can be modified. After a rule is locked, only increases in the duration are allowed. Object modification is prevented and the rule can only be deleted by deleting the bucket. A bucket must be empty before it can be deleted.

Required IAM Policies

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For administrators:

- You can create a rule that lets the specified IAM group manage Object Storage namespaces, buckets, and their associated objects in all compartments in the tenancy. For example, to let the IAM group StorageAdmins do everything in the tenancy:

  Allow group StorageAdmins to manage object-family in tenancy

- Alternatively, you can create policies that reduce the scope of access. For example, you can create the policies to let the StorageAdmins group manage only buckets and objects in a compartment called ObjectStore in the tenancy:

  Allow group StorageAdmins to manage buckets in compartment ObjectStore
  Allow group StorageAdmins to manage objects in compartment ObjectStore

- If you create more restrictive policies that grant individual permissions, BUCKET_UPDATE and RETENTION_RULE_MANAGE is required to create, edit, and delete retention rules. BUCKET_UPDATE, RETENTION_RULE_MANAGE, and RETENTION_RULE_LOCK is required to lock retention rules.

For more information about other alternatives for writing policies, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

Scope and Constraints

- Retention rules can be applied to a bucket in the Standard (Object Storage) or Archive Storage tier.
- The actions that you can perform on a bucket with active retention rules are limited. You cannot update, overwrite, or delete objects or object metadata until the retention rule is deleted (indefinite rule) or for the duration
specified (time-bound rules). The duration for time-bound rules is applied to each object individually, and is based on the object's Last Modified timestamp.

- You can create multiple retention rules for a bucket. Indefinite retention rule is applied before any time-bound rule is considered.
- When a retention rule is locked, the rule can only be deleted by deleting the bucket. A bucket must be empty before it can be deleted.

**Interaction Between Retention and Other Object Storage Features**

Carefully review the policies and rules that you have in place for the other Object Storage features that you are using. Some of these policies and rules may no longer make sense with retention rules. This section describes some key things you need to know about the interaction between retention rules and other Object Storage features.

**Bucket Re-Encryption**

Retention rules do not block bucket re-encryption using either Oracle or your own Vault master encryption keys.

**Multipart Uploads**

Uncommitted (unfinished or failed) multipart uploads are not protected by retention rules and can be deleted at any time.

**Lifecycle Management**

- Lifecycle policies can archive objects with retention rules.
- Lifecycle Management cannot remove objects protected by active retention rules.

**Replication**

- You can create retention rules on a replication source bucket.
- You cannot create retention rules on a replication destination bucket.
- You cannot enable replication on a destination bucket that has retention rules.

**Versioning**

- You cannot add retention rules to a bucket that has versioning enabled.
- You cannot enable versioning on a bucket with active retention rules.
- You can add retention rules to bucket that has versioning suspended. However, you cannot resume versioning with active retention rules.

**Troubleshooting Retention Rules**

This topic provides troubleshooting solutions for issues you might encounter using retention rules.

**Unable to create a retention rule**

If creating a retention rule fails, the most likely cause is missing or incomplete IAM permissions. Rule creation requires:

- User permissions that let you access the bucket and manage the objects in those buckets.
- Minimally, BUCKET_UPDATE and RETENTION_RULE_MANAGE permissions.

Review the existing policies that grant user permissions. For more information, see [Required IAM Policies](#) on page 3459.

**Unable to lock a retention rule**

If locking a retention rule fails, the most likely cause is missing or incomplete IAM permissions. Minimally, BUCKET_UPDATE, RETENTION_RULE_MANAGE, and RETENTION_RULE_LOCK permissions are required to lock retention rules.
Review the existing policies that grant user permissions. For more information, see Required IAM Policies on page 3459.

**Unable to delete a retention rule**

You cannot delete a time-bound retention rule that is locked. When a retention rule is locked, the rule can only be deleted by deleting the bucket. A bucket must be empty before it can be deleted.

If deleting an indefinite retention rule fails, the most likely cause is missing or incomplete IAM permissions. Rule deletion requires:
- User permissions that let you access the bucket and manage the objects in those buckets.
- Minimally, BUCKET_UPDATE and RETENTION_RULE_MANAGE permissions.

**Using the Console**

To create a retention rule

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. Choose the compartment that contains the bucket where you want to create a retention rule.
4. Click the bucket name.
5. Click **Retention Rules** under **Resources** to access the retention rule list.
6. Click **Create Rule**.
7. In the Create Retention Rule dialog, enter the required rule **Name**. The system generates a default rule name that reflects the current year, month, day, and time, for example retention-rule-20200229-1002. If you change this default to a different rule name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
8. Choose the retention rule type that you want to create:
   - **Time-Bound** rules have a user-defined duration. Object modification is prevented for the duration specified. Duration is applied to each object individually, and is based on the object's Last Modified timestamp.
   - **Indefinite** rules have no duration or expiration. Object modification is prevented until an indefinite rule is deleted.
9. If you are creating a time **Time-Bound** rule, enter the retention rule duration attributes:
   - **Retention Time Amount**
   - **Retention Time Unit**
10. Optionally, select **Enable Retention Rule Lock** if you want to lock the rule.
11. Click **Create**.

The rule is displayed in the **Retention Rules** list.

To lock a time-bound retention rule

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the retention rule.
4. Click the bucket name.
5. Click **Retention Rule** under **Resources** to access the rule list.
   - If you are creating a retention rule, click **Create Retention Rule**. Specify the duration amount and unit, then select **Enable Retention Rule Lock**. Click **Create**.
   - If you are editing a retention rule, click the Actions icon (three dots) to the right of the rule name, and then click **Edit**. Select **Enable Retention Rule Lock**. Click **Save Changes**.

To view retention rule details

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the retention rule.
4. Click the bucket name.
5. Click **Retention Rule** under **Resources** to access the rule list.
6. Click the Actions icon (three dots) to the right of the rule name, and then click **View Details**.

### To edit a retention rule

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the retention rule.
4. Click the bucket name.
5. Click **Retention Rule** under **Resources** to access the rule list.
6. Click the Actions icon (three dots) to the right of the rule name, and then click **Edit**.
   - If you are editing an indefinite retention rule, you can only edit the name of the rule.
   - If you are editing a time-bound retention rule, you can edit multiple attributes. You can edit the name, the duration time amount and time unit, and optionally select whether to lock the rule.
   - If you are removing a retention rule lock during the delay period, deselect **Enable Retention Rule Lock**. For more information about retention rule locking, see [About Object Storage Data Retention](#) on page 3458.
7. If you are enabling a retention rule lock, confirm the rule lock details by selecting **Update the Retention Rule with a Scheduled Lock Time of <date and time>**.
8. Click **Save Changes**.

### To delete a retention rule

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Ensure that the correct region is selected from the regions menu (shown at the top of the Console).
3. In the **List Scope** section, select the compartment that contains the bucket.
4. Click the bucket name.
5. Click **Retention Rule** under **Resources** to access the rule list.
6. Click the Actions icon (three dots) to the right of the rule name, and then click **Delete**.
7. Confirm deletion when prompted.

### Using the Command Line Interface (CLI)

For information about using the CLI, see [Command Line Interface (CLI)](#) on page 4192. For a complete list of flags and options available for CLI commands, see the [Command Line Reference](#).

#### To create an indefinite retention rule

```
oci os retention-rule create --namespace <object_storage_namespace> --bucket-name <bucket_name> --display-name <display_name>
```

For example:

```
oci os retention-rule create --namespace MyNamespace --bucket-name MyBucket --display-name LegalHold
{
  "data": {
    "display-name": "LegalHold",
    "duration": null,
    "etag": "7f51ef6c-3fca-48f7-9060-c129911c1a50",
    "id": "5772c87f-6723-4ecc-b44c-bef86643be92",
    "time-created": "2020-03-25T14:53:20.792000+00:00",
    "time-modified": "2020-03-25T14:53:20.792000+00:00",
    "time-rule-locked": null
  },
  "etag": "7f51ef6c-3fca-48f7-9060-c129911c1a50"
}
```
To create a time-bound, unlocked retention rule

```
oci os retention-rule create --namespace <object_storage_namespace> --bucket-name <bucket_name> --display-name <display_name> --time-amount <time_integer> --time-unit <days|years>
```

For example:

```
oci os retention-rule create --namespace MyNamespace --bucket-name MyBucket --display-name DataGovernance --time-amount 5 --time-unit days
```

```
{  
  "data": {  
    "display-name": "DataGovernance",
    "duration": {  
      "time-amount": 5,
      "time-unit": "DAYS"
    },
    "etag": "efb9178f-4213-49f7-878d-7bbe57decc0b",
    "id": "89f4ca0c-4ad9-4fa5-8005-95e7741c531c",
    "time-created": "2020-03-25T15:08:01.601000+00:00",
    "time-modified": "2020-03-25T15:08:01.601000+00:00",
    "time-rule-locked": null
  },
  "etag": "efb9178f-4213-49f7-878d-7bbe57decc0b"
}
```

To create a time-bound, locked retention rule

See the Command Line Interface (CLI) on page 4192 or the Command Line Reference for supported date and time formats for --time-rule-locked.

```
oci os retention-rule create --namespace <object_storage_namespace> --bucket-name <bucket_name> --display-name <display_name> --time-amount <time_integer> --time-unit <days|years> --time-rule-locked <date and time>
```

For example:

```
oci os retention-rule create --namespace MyNamespace --bucket-name MyBucket --display-name RegulatoryCompliance --time-amount 5 --time-unit years --time-rule-locked "2020-04-28 00:00"
```

```
{  
  "data": {  
    "display-name": "RegulatoryCompliance",
    "duration": {  
      "time-amount": 5,
      "time-unit": "YEARS"
    },
    "etag": "c05f02d3-d2b5-4378-9fcb-3a92ba0e018f",
    "id": "b1a6c84c-57c4-416c-b006-f864b0904e9e",
    "time-created": "2020-03-25T15:11:44.423000+00:00",
    "time-modified": "2020-03-25T15:11:44.423000+00:00",
    "time-rule-locked": "2020-04-28T00:00:00+00:00"
  },
  "etag": "c05f02d3-d2b5-4378-9fcb-3a92ba0e018f"
}
```

To list retention rules
oci os retention-rule list --namespace <object_storage_namespace> --bucket-name <bucket_name>

For example:

oci os retention-rule list --namespace MyNamespace --bucket-name MyBucket
{
    "data": {
        "items": [
            {
                "display-name": "RegulatoryCompliance",
                "duration": {
                    "time-amount": 5,
                    "time-unit": "YEARS"
                },
                "etag": "c05f02d3-d2b5-4378-9fcb-3a92ba0e018f",
                "id": "b1a6c84c-57c4-416c-b006-f864b0904c9e",
                "time-created": "2020-03-25T15:11:44.423000+00:00",
                "time-modified": "2020-03-25T15:11:44.423000+00:00",
                "time-rule-locked": "2020-04-28T00:00:00+00:00"
            },
            {
                "display-name": "DataGovernance",
                "duration": {
                    "time-amount": 5,
                    "time-unit": "DAYS"
                },
                "etag": "efb9178f-4213-49f7-878d-7bbee57dec0b",
                "id": "89f4ca0c-4ad9-4fa5-8005-95e7741c531c",
                "time-created": "2020-03-25T15:08:01.601000+00:00",
                "time-modified": "2020-03-25T15:08:01.601000+00:00",
                "time-rule-locked": null
            },
            {
                "display-name": "LegalHold",
                "duration": null,
                "etag": "7f51ef6c-3fca-48f7-9060-c129911c1a50",
                "id": "5772c87f-6723-4ecc-b44c-bef86643be92",
                "time-created": "2020-03-25T14:53:20.792000+00:00",
                "time-modified": "2020-03-25T14:53:20.792000+00:00",
                "time-rule-locked": null
            }
        ]
    }
}

To view retention rule details

oci os retention-rule get --namespace <object_storage_namespace> --bucket-name <bucket_name> --retention-rule-id <retention_rule_identifier>

For example:

oci os retention-rule get --namespace MyNamespace --bucket-name MyBucket --retention-rule-id b1a6c84c-57c4-416c-b006-f864b0904c9e
{
    "data": {
        "display-name": "RegulatoryCompliance",
        "duration": {
            "time-amount": 5,
            "time-unit": "YEARS"
        }
    }
}
To update a time-bound retention rule after creation

```shell
oci os retention-rule update --namespace <object_storage_namespace> --bucket-name <bucket_name> --retention-rule-id --display-name <display_name> --time-amount <time_integer> --time-unit <days|years> --time-rule-locked <date and time>
```

For example, to increase the duration of and change the date a retention rule is locked:

```shell
oci os retention-rule update --namespace MyNamespace --bucket-name MyBucket --retention-rule-id bla6c84c-57c4-416c-b006-f864b0904c9e --time-amount 6 --time-unit years --time-rule-locked "2020-03-25T15:11:44.423000+00:00"
```

```json
{
  "data": {
    "display-name": "RegulatoryCompliance",
    "duration": {
      "time-amount": 6,
      "time-unit": "YEARS"
    },
    "etag": "700ada5c-6a2a-4c6c-acb6-4ebb173e0f8f",
    "id": "bla6c84c-57c4-416c-b006-f864b0904c9e",
    "time-created": "2020-03-25T15:11:44.423000+00:00",
    "time-modified": "2020-03-25T15:11:44.423000+00:00",
    "time-rule-locked": "2020-04-28T00:00:00+00:00"
  },
  "etag": "700ada5c-6a2a-4c6c-acb6-4ebb173e0f8f"
}
```

To remove a retention rule lock during the delay period

```shell
oci os retention-rule update --namespace <object_storage_namespace> --bucket-name <bucket_name> --retention-rule-id --display-name <display_name> --time-rule-locked ""
```

```shell
oci os retention-rule update --namespace MyNamespace --bucket-name MyBucket --retention-rule-id bla6c84c-57c4-416c-b006-f864b0904c9e --time-rule-locked ""
```

```json
{
  "data": {
    "display-name": "RegulatoryCompliance",
    "duration": {
      "time-amount": 6,
      "time-unit": "YEARS"
    },
    "etag": "5b4fa526-faec-47d4-9162-4acdf1813ee0",
    "id": "bla6c84c-57c4-416c-b006-f864b0904c9e",
    "time-created": "2020-03-25T15:11:44.423000+00:00",
    "time-modified": "2020-03-25T15:11:44.423000+00:00",
    "time-rule-locked": null
  },
  "etag": "5b4fa526-faec-47d4-9162-4acdf1813ee0"
}
```
To delete a retention rule

```bash
oci os retention-rule delete --namespace <object_storage_namespace> --bucket-name <bucket_name> --retention-rule-id <retention_rule_identifier>
```

For example:

```bash
oci os retention-rule delete --namespace MyNamespace --bucket-name MyBucket --retention-rule-id 4ed833b1-fb27-4a40-a8ab-14e09636a724
```

Are you sure you want to delete this resource? [y/N]: y

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to use and manage retention rules:

- CreateRetentionRule
- GetRetentionRule
- ListRetentionRules
- UpdateRetentionRule
- DeleteRetentionRule

Using Object Lifecycle Management

By using Object Lifecycle Management to manage your Object Storage and Archive Storage data, you can reduce your storage costs and the amount of time you spend manually managing data.

Object Lifecycle Management works by taking automated action based on rules that you define. These rules instruct Object Storage to delete uncommitted multipart uploads, move objects to a different storage tier, and delete supported resources on your behalf within a given bucket. A bucket's lifecycle rules are collectively known as an object lifecycle policy. The resources that Object Lifecycle Management supports include objects, object versions, and uncommitted or failed multipart uploads.

For example, you can define rules that automatically do things like the following:

- Move Standard tier objects with a `.doc` extension to either the Infrequent Access or Archive tier 60 days after creation.
- Move Standard tier objects to the Archive tier 30 days after creation, and then automatically delete those archived objects after 180 days.
- Move Standard tier objects to the Infrequent Access tier 90 days after creation.
- Delete any previous object versions 120 days after the object version transitions from the latest version to a previous version.
- Delete uncommitted or failed multipart uploads after 5 days.

Each Object Storage or Archive Storage bucket can have a single lifecycle policy consisting of up to 1,000 rules. Object-related rules can have object name prefix and pattern matching conditions. Uncommitted multipart upload rules do not support prefix and pattern matching conditions.

You can create, edit, delete, enable, and disable individual rules in the Console as needed. To update a lifecycle policy using the CLI or API, overwrite an existing policy with a new policy. Ensure that the new policy is inclusive of all the policy rules that you want to apply to the bucket.
Object Storage

Required IAM Policies

Important:
You cannot use Object Lifecycle Management until you authorize the Object Storage service to archive and delete objects on your behalf. See Service Permissions on page 3467 for more information.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

User Permissions

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators:

• The policy Let Object Storage admins manage buckets and objects on page 2149 lets the specified group do everything with buckets and objects, including adding and managing lifecycle policies.
• If you create more restrictive policies that grant individual permissions:
  • OBJECT_VERSION_DELETE is required to delete previous object versions on your behalf using lifecycle policies.
  • OBJECT_UPDATE_TIER is required to change the storage tier of an object.

See Details for Object Storage, Archive Storage, and Data Transfer on page 2324 for more information on Object Storage user permissions.

Service Permissions

To execute object lifecycle policies, you must authorize the service to archive and delete objects on your behalf. To do so, create the following policy in the root compartment of your tenancy:

Allow service objectstorage-<region_identifier> to manage object-family in compartment <compartment_name>

Because Object Storage is a regional service, you must authorize the Object Storage service in each region you use lifecycle policies. Object Storage ensures that your data is not read from any unauthorized region.

If you don't have permissions to write policies for the root compartment of your tenancy, contact your Oracle Cloud Infrastructure administrator. To determine the region identifier value of an Oracle Cloud Infrastructure region, see Regions and Availability Domains on page 180.

Instead of using the policy verb manage, you can grant individual permissions to the service. For example:

Allow service objectstorage-<region_identifier> to manage object-family in compartment <compartment_name>
where any {request.permission='BUCKET_INSPECT',
request.permission='BUCKET_READ',
request.permission='OBJECT_INSPECT',
request.permission='OBJECT_CREATE',
request.permission='OBJECT_DELETE',
request.permission='OBJECT_VERSION_DELETE'}

Options

When creating object lifecycle policy rules, you have the following options:

• When a lifecycle rule is created, the system generates a default name for that rule, for example lifecycle-rule-20190321-1559. This rule name identifies the current year, month, day, and time that the rule was created. You can use that system-generated name for your new rule or you can specify a different name for it.
• You can create lifecycle rules that do the following:
  • Move or delete all objects in the bucket.
  • Move or delete objects in the bucket that match the object name filters you specify. You can select objects using both object name prefixes and pattern matching. See Using Object Name Filters on page 3468 for details.
  • Delete uncommitted or failed multipart uploads. For more information, see Using Multipart Uploads on page 3477.

If object versioning is enabled or suspended on a bucket, you can also create lifecycle rules that do the following:
  • Move or delete the previous versions of all objects in the bucket.
  • Move or delete the previous versions of objects in the bucket that match the name filters you specify. You can select objects using both object name prefixes and pattern matching. See Using Object Name Filters on page 3468 for details.

• You specify the number of days until the specified action is taken.
• You decide whether a new rule is enabled or disabled upon creation.

Using Object Name Filters

Use object name filters to specify a subset of objects, object versions, or previous object versions that a lifecycle rule applies to. Create a separate object name filter rule for each rule target (objects, object versions, or previous object versions).

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not specify object name filters if you want a rule to apply to the all objects, all object versions, or all previous object versions target.</td>
</tr>
</tbody>
</table>

You can add object name filters in any order. Object Lifecycle Management evaluates the precedence of the rules as follows:
1. Pattern exclusions
2. Pattern inclusions
3. Prefix inclusions

Using Prefix Matching to Filter Objects

When naming objects, you can use prefix strings without a delimiter so that certain bulk operations can be performed by matching on the prefix portion of the object name. For example, in the object names below, the string `gloves_27_` serves as a prefix for matching purposes when performing lifecycle management archive or deletions:

- `gloves_27_dark_green.jpg`
- `gloves_27_light_blue.jpg`
- `gloves_27_deep_purple.jpg`
- `gloves_27_bright_orange.jpg`

See Object Naming Using Prefixes and Hierarchies on page 3420 for complete details.

Using Pattern Matching to Filter Objects

Object Storage supports the following pattern matching characters to either include or exclude objects:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Pattern Examples</th>
<th>Matches</th>
<th>Doesn’t Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches 0 or more characters</td>
<td>*.tmp</td>
<td>foo.tmp&lt;br&gt;foo/bar/baz.tmp</td>
<td>tmp&lt;br&gt;Atmp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.xls</td>
<td>.xls&lt;br&gt;/home/user/file.xlsx</td>
<td>xls&lt;br&gt;.xl</td>
</tr>
<tr>
<td>Character</td>
<td>Description</td>
<td>Pattern Examples</td>
<td>Matches</td>
<td>Doesn't Match</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>/archive/*</td>
<td>/archive/sub/dir/</td>
<td>/archive/1/2/3/4/ /archive/1/2/3/4/ /f0o.txt</td>
<td>/src/archive/a /archive/b</td>
</tr>
<tr>
<td>?</td>
<td>Matches any one character</td>
<td>X?Z</td>
<td>XyZ</td>
<td>XZ</td>
</tr>
<tr>
<td></td>
<td>X_Z</td>
<td>XYYZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\</td>
<td>Escapes the next character</td>
<td>\dir\sub/*</td>
<td>\dir\sub\ABC</td>
<td>dir\sub\abc</td>
</tr>
<tr>
<td></td>
<td>\dir\sub\</td>
<td></td>
<td>\dir\sub\</td>
<td>dirstub</td>
</tr>
<tr>
<td>[...]</td>
<td>Matches a group of characters, which can be:</td>
<td>[-ab3]</td>
<td>-</td>
<td>-a</td>
</tr>
<tr>
<td></td>
<td>A set of characters, for example:</td>
<td>a</td>
<td>-ab</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Zaf9@ ].</td>
<td>b</td>
<td>3b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Matches any character in the brackets.</td>
<td>backup.tar.gz.[0-9]</td>
<td>backup.tar.gz.0</td>
<td>backup.tar.gz10</td>
</tr>
<tr>
<td></td>
<td>A range of characters, for example: [a-f].</td>
<td>backup.tar.gz.5</td>
<td>backup.tar.gz.9</td>
<td>backup.tar.gz</td>
</tr>
<tr>
<td></td>
<td>Matches any character in the range:</td>
<td>page-[0-9]*</td>
<td>page-0</td>
<td>page-</td>
</tr>
<tr>
<td></td>
<td>[a-f] is equivalent to [abcdef].</td>
<td>page-2</td>
<td>page-A1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For character ranges only the CHARACTER-CHARACTER-CHARACTER pattern is supported:</td>
<td>page-22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ab-yz] is not valid.</td>
<td>page-2X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[a-mn-z] is not valid.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Character ranges cannot start with ^ or colon (:).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To include a hyphen (-) in the range, make it the first or last character.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[a-z]</td>
<td>[a-z]</td>
<td>a</td>
<td>z</td>
<td>[a-z]</td>
</tr>
</tbody>
</table>
Patterns are limited to 1024 characters. The following are examples of invalid patterns:

- \n
- [^a-z]

- [z-a]

- [:isalpha:]

**Scope and Constraints**

Understand the following scope and constraints regarding object lifecycle policy rules:

- When you create a lifecycle policy rule, that rule applies to all objects, all object versions, or all previous object versions that exist in the bucket unless you add object name filters for that target.

- **Prefix** and **pattern matching** filtering applies only to rules for objects, object versions, or previous object versions. Object filtering does not apply to uncommitted multipart uploads.

- A rule that deletes an object always takes priority over a rule that would move that same object to another storage tier.

- When you create a rule that moves or deletes previous object versions, you specify the number of days until the move or deletion occurs. The "number of days" countdown is based on when the object version transitioned from being the latest object version to being a previous object version. This time can be determined by looking at the "last modified" time of the preceding most recent version of the object. The following screenshot illustrates the time used to start the countdown for archival or deletion in the.

- Be aware of minimum retention periods when you create rules that move or delete the latest version or previous versions of objects.
  
  - The Archive tier has a minimum retention requirement of 90 days. Objects moved or deleted from the Archive tier that have not met the 90-day retention minimum are billed for 90 days of storage.
  
  - Infrequent Access tier has a minimum retention requirement of 31 days. Objects moved or deleted from the Infrequent Access tier that have not met the 31-day retention minimum are billed for 31 days of storage.

- You can create up to 1,000 lifecycle rules per bucket.

**Working with Object Lifecycle Management Policies**

You can create, delete, edit, or disable lifecycle policy rules using the Console, the Command Line Interface (CLI), an SDK, or the API.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects deleted on your behalf by lifecycle policies cannot be recovered. Be sure when creating and editing your lifecycle policies that you are not unintentionally deleting data you want to retain. Oracle recommends that you test your lifecycle policy on development data before using the policy in production.</td>
</tr>
</tbody>
</table>
Using the Console
To create a lifecycle policy rule

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment containing the bucket for which you want to create a lifecycle rule.
3. Click the bucket name.
4. Click Lifecycle Policy Rules under Resources to access the lifecycle policy rule list.
5. Click Create Rule.
6. Provide the following information:

   • **Name:** Required. The system generates a default rule name that reflects the current year, month, day, and time, for example lifecycle-rule-20190321-1559. If you change this default to any other rule name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
   
   • **Target:** Required. Select the target to which the lifecycle rule applies.
     • If object versioning is **Disabled**, select the rule target **Objects** or **Uncommitted Multipart Uploads**.
     • If object versioning is **Enabled** or **Suspended** select the rule target **Latest Version of Objects**, **Previous Versions of Objects**, or **Uncommitted Multipart Uploads**.

   • **Lifecycle Action:**
     • If the rule target is **Objects**, **Latest Version of Objects**, or **Previous Versions of Objects**, select **Move to Archive**, **Move to Infrequent Access**, or **Delete**.
     • If the rule target is **Uncommitted Multipart Uploads**, **Delete** is the only option and is selected by default.
   
   • **Number of Days:** The number of days until the specified action is taken.

Note:  
If the rule archives or deletes a previous object version, the "number of days" countdown is based on when the object version transitioned from being the latest object version to being a previous object version. This time can be determined by looking at the "last modified" time of the preceding most recent version of the object. The following screenshot illustrates the time used to start the countdown for archival or deletion in the.

7. If the rule target is **Objects**, **Latest Version of Objects**, or **Previous Versions of Objects**, you can optionally add one or more **Object Name Filters** to specify which objects the lifecycle rule applies to. You can choose objects or
object versions using prefixes and pattern matching. If no object name filters are specified, the rule applies to all objects in the bucket.

To create an object name filter:

a. Click Add Filter.
b. Select the Filter Type.
c. Enter the Filter Value.
d. Click Add Another Filter to add as many filters as you need for this rule.

8. Select whether the rule is enabled or disabled upon creation using the State selector.
9. Click Create.

To edit a lifecycle policy rule

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment containing the bucket for which you want to edit a lifecycle rule.
3. Click the bucket name.
4. Click Lifecycle Policy Rules under Resources to access the rule list.
5. Click the Actions icon (three dots) to the right of the rule that you want to edit, and then click Edit.
6. In the Edit Lifecycle Rule dialog box, edit the following as needed for each rule you want to change.
   • Name: A user-friendly name for the rule. Avoid entering confidential information.
   • Lifecycle Action:
     • If the rule target is Objects, Latest Version of Objects, or Previous Versions of Objects, select Move to Archive, Move to Infrequent Access, or Delete.
     • If the rule target is Uncommitted Multipart Uploads, Delete is the only option and is selected by default.
     • Number of Days: The number of days until the specified action is taken.
     • If the rule pertains to objects or object versions, you can edit, delete, or add prefix or pattern Object Name Filters.
   • Enable or disable the rule using the State selector.
7. Click Save Changes.

To enable, disable, or delete a lifecycle policy rule

You can enable, disable, or delete a rule using the Console. The system stops the execution of disabled or deleted rules immediately.

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment containing the bucket for which you want to enable, disable, or delete a lifecycle rule.
3. Click the bucket name.
4. Click Lifecycle Policy Rules under Resources to access the rule list.
5. Click the Actions icon (three dots) to the right of the rule that you want to manage, and then click one of the following:
   • Enable (only displays if the rule is disabled)
   • Disable (only displays if the rule is enabled)
   • Delete

Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.
To create or replace a lifecycle policy for a bucket

**Note:**

To edit an existing lifecycle policy using the CLI, you need to replace the policy with a new complete version that includes all changed rules.

```bash
oci os object-lifecycle-policy put --namespace <object_storage_namespace> --bucket-name <bucket_name> --items <json_formatted_lifecycle_policy>
```

**Tip:**

The `--items` option requires that you provide key-value pair input as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

The `--items` key-value pair input must specify the following:

```json
[
  {
    "action": "string",
    "isEnabled": true,
    "name": "string",
    "objectNameFilter": {
      "exclusionPatterns": [
        "string",
        "string"
      ],
      "inclusionPatterns": [
        "string",
        "string"
      ],
      "inclusionPrefixes": [
        "string",
        "string"
      ]
    },
    "target": "string",
    "timeAmount": 0,
    "timeUnit": "string"
  }
]
```

Specify one of the following values for `action`:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARCHIVE</td>
<td>Specify this action to move objects, object versions, or previous object versions to the Archive tier.</td>
</tr>
<tr>
<td>INFREQUENT_ACCESS</td>
<td>Specify this action to move objects, object versions, or object versions to the Infrequent Access tier.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Specify this action to delete objects, object versions, or object versions.</td>
</tr>
<tr>
<td>ABORT</td>
<td>Use this action to delete failed or incomplete multipart uploads.</td>
</tr>
</tbody>
</table>

Specify one of the following values for `target`:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>objects</td>
<td>Use this action to move objects, object versions, or previous object versions to the Archive tier.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>object-versions</td>
<td>Use this action to move objects, object versions, or previous object versions to the Infrequent Access tier.</td>
</tr>
<tr>
<td>multipart-uploads</td>
<td>Use this action to delete objects, object versions, or previous object versions.</td>
</tr>
</tbody>
</table>

Specify `timeUnit` in days.

The following example creates or replaces a lifecycle policy that includes a rule for moving previous object versions with names that include the pattern `*.doc` from the Standard tier to the Archive tier after 60 days. The policy also includes a rule that deletes previous object versions after 180 days.

```bash
oci os object-lifecycle-policy put --namespace MyNamespace --bucket-name MyStandardTierBucket --items '[
  {
    "action": "ARCHIVE",
    "is-enabled": true,
    "name": "Move-to-Archive-Rule",
    "object-name-filter": {
      "exclusion-patterns": null,
      "inclusion-patterns": [
        "*.doc"
      ],
      "inclusion-prefixes": null
    },
    "target": "previous-object-versions",
    "time-amount": 60,
    "time-unit": "DAYS"
  },
  {
    "action": "DELETE",
    "is-enabled": true,
    "name": "Delete-Rule",
    "object-name-filter": {
      "exclusion-patterns": null,
      "inclusion-patterns": [
        "*.doc"
      ],
      "inclusion-prefixes": null
    },
    "target": "previous-object-versions",
    "time-amount": 180,
    "time-unit": "DAYS"
  }
]
```

The following example creates or replaces a lifecycle policy that includes a rule for moving all objects from the Standard tier to the Infrequent Access tier after 45 days. The policy also includes a rule that moves all objects to the Archive tier after 90 days.

```bash
oci os object-lifecycle-policy put --namespace MyNamespace --bucket-name MyStandardTierBucket --items '[
  {
    "action": "INFREQUENT_ACCESS",
    "is-enabled": true,
    "name": "Move-to-Infrequent-Access-Rule",
    "object-name-filter": null,
    "target": "objects",
    "time-amount": 45,
    "time-unit": "DAYS"
  },
  {
    "action": "ARCHIVE",
    "is-enabled": true,
    "name": "Move-to-Archive-Rule",
    "object-name-filter": null,
    "target": "objects",
    "time-amount": 90,
    "time-unit": "DAYS"
  }
]
```
The following example creates or replaces a lifecycle policy rule that deletes previous object versions from the Archive tier after 240 days:

```bash
oci os object-lifecycle-policy put --namespace MyNamespace --bucket-name MyArchiveTierBucket --items
'[  
  {  
      "action": "DELETE",  
      "is-enabled": true,  
      "name": "Delete-from-Archive-Rule",  
      "object-name-filter": null,  
      "target": "previous-object-versions",  
      "time-amount": 240,  
      "time-unit": "DAYS"
  }
]
```

The following example creates or replaces a lifecycle policy rule that deletes all uncommitted or failed multipart uploads after 5 days:

```bash
oci os object-lifecycle-policy put --namespace MyNamespace --bucket-name MyBucket --items
'[  
  {  
      "action": "ABORT",  
      "is-enabled": true,  
      "name": "Delete-Failed-Multipart-Uploads-Rule",  
      "object-name-filter": null,  
      "target": "multipart-uploads",  
      "time-amount": 5,  
      "time-unit": "DAYS"
  }
]
```

Instead of using the `--items` option, you can pass the JSON key-value pairs in a file. For example:

```bash
oci os object-lifecycle-policy put --namespace MyNamespace --bucket-name MyStandardTierBucket --file /path/to/file/filename
```

On Windows, to pass complex input to the CLI as a JSON string, you must enclose the entire block in double quotes. Inside the block, each double quote for the key and value strings must be escaped with a backslash (\) character.

For example:

```bash
oci os object-lifecycle-policy put --namespace MyNamespace --bucket-name MyStandardTierBucket --items "[{"action"":"ARCHIVE","is-enabled":true,"name":"move-to-Archive-rule","target":"previous-object-versions","timeAmount":180,"timeUnit":"DAYS"}]"
```
To delete a bucket's lifecycle policy

Delete all of the lifecycle policy rules that you have defined for the specified bucket.

```
oci os object-lifecycle-policy delete --namespace <object_storage_namespace> --bucket-name <bucket_name>
```

For example:

```
oci os object-lifecycle-policy delete --namespace MyNamespace --bucket-name MyStandardTierBucket
```

When prompted, confirm the deletion.

To get a bucket's lifecycle policy

Get all of the lifecycle policy rules that you have defined for the specified bucket.

```
oci os object-lifecycle-policy get --namespace <object_storage_namespace> --bucket-name <bucket_name>
```

For example:

```
oci os object-lifecycle-policy get --namespace MyNamespace --bucket-name MyStandardTierBucket
{
  "data": {
    "items": [
      {
        "action": "ABORT",
        "is-enabled": true,
        "name": "Delete-Failed-Multipart-Uploads-Rule",
        "object-name-filter": null,
        "target": "multipart-uploads",
        "time-amount": 5,
        "time-unit": "DAYS"
      },
      {
        "action": "DELETE",
        "is-enabled": true,
        "name": "Delete-from-Archive-Rule",
        "object-name-filter": {
          "exclusion-patterns": null,
          "inclusion-patterns": null,
          "inclusion-prefixes": null
        },
        "target": "objects",
        "time-amount": 240,
        "time-unit": "DAYS"
      },
      {
        "action": "INFREQUENT_ACCESS",
        "is-enabled": true,
        "name": "Move-to-Infrequent-Access-Rule",
        "object-name-filter": {
          "exclusion-patterns": null,
          "inclusion-patterns": null,
          "inclusion-prefixes": null
        },
        "target": "objects",
        "time-amount": 45,
        "time-unit": "DAYS"
      }
    ]
  }
}``

For example, to get the lifecycle policy that archives objects after 30 days:

```bash
oci os object-lifecycle-policy get --namespace MyNamespace --bucket-name MyBucketWithoutVersioning
```

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage object lifecycle policies:

- PutObjectLifecyclePolicy
- GetObjectLifecyclePolicy
- DeleteObjectLifecyclePolicy

Using Multipart Uploads

The Oracle Cloud Infrastructure Object Storage service supports multipart uploads for more efficient and resilient uploads, especially for large objects. You can perform multipart uploads using the API, the Software Development Kits and Command Line Interface on page 4225, or the Command Line Interface (CLI) on page 4192. The Console uses multipart uploads to upload objects larger than 64 MiB.
With multipart uploads, individual parts of an object can be uploaded in parallel to reduce the amount of time you spend uploading. Multipart uploads performed through the API can also minimize the impact of network failures by letting you retry a failed part upload instead of requiring you to retry an entire object upload.

Multipart uploads can accommodate objects that are too large for a single upload operation. Oracle recommends that you perform a multipart upload to upload objects larger than 100 MiB. The maximum size for an uploaded object is 10 TiB. Object parts must be no larger than 50 GiB. For large uploads performed through the API, you have the flexibility of pausing between the uploads of individual parts, and resuming the upload when your schedule and resources allow.

You can use object lifecycle policy rules to automatically delete any uncommitted or failed multipart uploads after a specified number of days. See Using Object Lifecycle Management on page 3466 for details.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you are new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

For administrators:

- You can create a policy that lets the specified IAM group manage Object Storage namespaces, buckets, and their associated objects in all compartments in the tenancy:

  ```
  Allow group <IAM_group_name> to manage object-family in tenancy
  ```

- Alternatively, you can create policies that reduce the scope of access. For example, to let the specified group manage only buckets and objects in a particular compartment in the tenancy:

  ```
  Allow group <IAM_group_name> to manage buckets in compartment <compartment_name>
  ```

  **Important:**
  
  If you write more restrictive policies, ensure that you include the permissions required for multipart uploads. The user needs a policy that grants both OBJECT_CREATE and OBJECT_OVERWRITE permissions.

For more information about other alternatives for writing policies, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

**Monitoring Resources**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For more information about monitoring multipart uploads, see Object Storage Metrics on page 3499.

**Using the Multipart Upload API**

A multipart upload performed using the API consists of the following steps:

1. Initiating an upload
2. Uploading object parts
3. Committing the upload

Before you use the multipart upload API, you are responsible for creating the parts to upload. Object Storage provides API operations for the remaining steps. The service also provides API operations for listing in-progress multipart
uploads, listing the object parts in an in-progress multipart upload, and aborting in-progress multipart uploads
initiated through the API. Here we provide a high-level overview of the API steps, but you can refer to the API
Reference for specifics about supported API calls.

Creating Object Parts
With multipart upload, you split the object you want to upload into individual parts. Individual parts can be as large as
50 GiB. Decide what part number you want to use for each part. Part numbers can range from 1 to 10,000. You do not
need to assign contiguous numbers, but Object Storage constructs the object by ordering part numbers in ascending
order.

Initiating an Upload
After you finish creating object parts, initiate a multipart upload by making a CreateMultipartUpload REST API call.
Provide the object name and any object metadata. Object Storage responds with a unique upload ID that you must
include in any requests related to this multipart upload. Object Storage also marks the upload as active. The upload
remains active until you explicitly commit it or abort it.

Uploading Object Parts
Make an UploadPart request for each object part upload. In the request parameters, provide the Object Storage
namespace, bucket name, upload ID, and part number. In the request body, include the object part. Object parts can
be uploaded in parallel and in any order. When you commit the upload, Object Storage uses the part numbers to
sequence object parts. Part numbers do not have to be contiguous. If multiple object parts are uploaded using the same
upload ID and part number, the CommitMultipartUpload API commits the last part uploaded.

Object Storage returns an ETag (entity tag) value for each part uploaded. You need both the part number and
corresponding ETag value for each part when you commit the upload.

If you have network issues, you can restart a failed upload for an individual part. You do not need to restart the entire
upload. If for some reason, you cannot perform an upload all at once, multipart upload lets you continue uploading
parts at your own pace. While a multipart upload is still active, you can keep adding parts as long as the total number
is less than 10,000.

You can check on an active multipart upload by listing all parts that have been uploaded. (You cannot list information
for an individual object part in an active multipart upload.) The ListMultipartUploadParts operation requires the
Object Storage namespace, bucket name, and upload ID. Object Storage responds with information about the parts
associated with the specified upload ID. Parts information includes the part number, ETag value, MD5 checksum, and
part size (in bytes).

Similarly, if you have multiple multipart uploads occurring simultaneously, you can see what uploads are in-progress.
Make an ListMultipartUploads API call to list active multipart uploads in the specified Object Storage namespace and
bucket.

Charges for parts storage begin accruing when you upload data.

Committing the Upload
When you have uploaded all object parts, commit the upload. Use the CommitMultipartUpload request parameters
to specify the Object Storage namespace, bucket name, and upload ID. Include the part number and corresponding
ETag value for each part in the body of the request. When you commit the upload, Object Storage constructs the
object from its constituent parts. The object is stored in the specified bucket and Object Storage namespace. You can
treat it like you would any other object. Garbage collection releases storage space occupied by any part numbers you
uploaded, but did not include in the CommitMultipartUpload request.

You cannot list or retrieve parts from a completed upload. You cannot append or remove parts from the completed
upload either. If you want, you can replace the object by initiating a new upload.

If you decide to abort a multipart upload instead of committing it, wait for in-progress part uploads to complete and
then use the AbortMultipartUpload operation. If you abort an upload while part uploads are still in progress anyway,
Object Storage cleans up both completed and in-progress parts. Upload IDs from aborted multipart uploads cannot be reused.

**API Documentation**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage multipart uploads:

- AbortMultipartUpload
- CommitMultipartUpload
- CreateMultipartUpload
- ListMultipartUploadParts
- ListMultipartUploads
- UploadPart (see Special Instructions for Object Storage PUT for signing request requirements)

**Using the CLI**

When you perform a multipart upload using the CLI, you do not need to split the object into parts as you are required to do by the API. Instead, you specify the part size of your choice, and Object Storage splits the object into parts and performs the upload of all parts automatically. You can choose to set the maximum number of parts that can be uploaded in parallel. By default, the CLI limits the number of parts that can be uploaded in parallel to three. When using the CLI, you do not have to perform a commit when the upload is complete.

You can also use the CLI to list in-progress multipart uploads, and to abort multipart uploads initiated through the API.

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**To perform a multipart upload using the CLI**

To upload an object, run `oci os object put` with the `--part-size` flag. The `--part-size` value represents the size of each part in mebibytes (MiBs). Object Storage waives the minimum part size restriction for the last uploaded part. The `--part-size` value must be an integer.

Optionally, you can use the `--parallel-upload-count` flag to set the maximum number of parallel uploads allowed.

```
oci os object put --namespace <object_storage_namespace> --bucket-name <bucket_name> --file <file_location> --name <object_name> --part-size <upload_part_size_in_MB> --parallel-upload-count <maximum_number_parallel_uploads>
```

For example:

```
oci os object put --namespace MyNamespace --bucket-name MyBucket --file ~/path/to/file --name MyObject --parallel-upload-count 10 --part-size 500
```

Upload ID: 277fff55-e1b5-e81d-5f81-c374a8f33998

Split file into 12 parts for upload.

Uploading object ################################################################ 100%

```
{ "etag": "861c8341-74d8-4142-8da4-28e1ce7783ba", "last-modified": "Wed, 25 Sep 2019 19:59:15 GMT", "opc-multipart-md5": "9Qnleyou2yMiyOO9Bc7o1A==--12" }
```

For more information on the `oci os object put` command, see To upload an object to a bucket.
To list the parts of an unfinished or failed multipart upload

```
oci os multipart list --namespace <object_storage_namespace> --bucket-name <bucket_name>
```

For example:

```
oci os multipart list --namespace MyNamespace --bucket-name MyBucket

"data": [
  {
    "bucket": "MyBucket",
    "namespace": "MyNamespace",
    "object": "MyObject",
    "time-created": "2019-07-25T21:55:21.973000+00:00",
    "upload-id": "0b7abd48-9ff2-9d5f-2034-63a02fdd7afa"
  },
  {
    "bucket": "MyBucket",
    "namespace": "MyNamespace",
    "object": "MyObject",
    "time-created": "2019-07-25T21:53:09.246000+00:00",
    "upload-id": "1293ac9d-83f8-e055-a5a7-d1e13277b5c0"
  },
  {
    "bucket": "MyBucket",
    "namespace": "MyNamespace",
    "object": "MyObject",
    "time-created": "2019-07-25T21:46:34.981000+00:00",
    "upload-id": "33e7a875-9e94-c3bc-6577-2ee5d8226b53"
  }
...]
```

**Tip:**

See the Command Line Reference for command options to control the pagination of the list output.

To delete a part of an uncommitted or failed multipart upload

```
oci os multipart abort --namespace <object_storage_namespace> --bucket-name <bucket_name> --object-name <object_name> --upload-id <upload_ID>
```

For example:

```
oci os multipart abort --namespace MyNamespace --bucket-name MyBucket --object-name MyObject --upload-id 0b7abd48-9ff2-9d5f-2034-63a02fdd7afa
WARNING: Are you sure you want to permanently remove this incomplete upload? [y/N]: y
```

**Tip:**

The CLI interface asks you to confirm the deletion request. To delete without the confirmation prompt, use the --force flag.

You can also create a lifecycle policy that automatically deletes uncommitted or failed multipart uploads. See Using Object Lifecycle Management on page 3466 for details.

To delete all parts of an uncommitted or failed multipart upload

```
#!/bin/bash
BUCKET=$1
```
oci os multipart list --bucket-name $BUCKET | \
  jq -c '.data | map({"o": .object, "i": "upload-id"}) | .[]' | \ 
while read JSON; do
  OBJECTNAME=$(echo $JSON | jq '.o' | sed -e 's/"//g;')
  UPLOADID=$(echo $JSON | jq '.i' | sed -e 's/"//g;')
  echo Removing Object name $OBJECTNAME, ID $UPLOADID
  oci os multipart abort --bucket-name $BUCKET \
    --object-name $OBJECTNAME \
    --upload-id $UPLOADID \
    --force
done

You can also create a lifecycle policy that automatically deletes uncommitted or failed multipart uploads. See Using Object Lifecycle Management on page 3466 for details.

Using Pre-Authenticated Requests

Pre-authenticated requests provide a way to let users access a bucket or an object without having their own credentials, as long as the request creator has permissions to access those objects. For example, you can create a request that lets an operations support user upload backups to a bucket without owning API keys. Or, you can create a request that lets a business partner update shared data in a bucket without owning API keys.

When you create a pre-authenticated request, a unique URL is generated. Anyone you provide this URL to can access the Object Storage resources identified in the pre-authenticated request, using standard HTTP tools like curl and wget.

**Important:**

Assess the business requirement for and the security ramifications of pre-authenticated access to a bucket or objects.

A pre-authenticated request URL gives anyone who has the URL access to the targets identified in the request. Carefully manage the distribution of the URL.

**Required Permissions**

**To Create a Pre-Authenticated Request**

To create or manage pre-authenticated requests, you need `PAR_MANAGE` permission to the target bucket or object.

While you only need `PAR_MANAGE` permission to create a pre-authenticated request, you must also have the appropriate permissions for the access type that you are granting. For example:

- If you are creating a pre-authenticated request for uploading objects to a bucket, you need `OBJECT_CREATE` and `OBJECT_OVERWRITE` permissions in addition to `PAR_MANAGE`.
- If you are creating a pre-authenticated request for read/write access to objects in a bucket, you need `OBJECT_READ`, `OBJECT_CREATE`, and `OBJECT_OVERWRITE` permissions in addition to `PAR_MANAGE` to grant user read/write access to objects.

**Important:**

If the creator of a pre-authenticated request is deleted or loses the required permissions after they created the request, the request will no longer work.

**To Use a Pre-Authenticated Request**

Permissions of the pre-authenticated request creator are checked each time you use a pre-authenticated request. The pre-authenticated request no longer works when any of the following occurs:

- Permissions of the pre-authenticated request creator have changed.
- User who created the pre-authenticated request is deleted.
• Federated user who created the pre-authenticated request has lost the user capabilities that they had when they created the request.
• Pre-authenticated request has expired.

Options
When creating a pre-authenticated request, you have the following options:
• You can specify the name of a bucket that a pre-authenticated request user has write access to and can upload one or more objects to.
• You can specify the name of an object that a pre-authenticated request user can read from, write to, or read from and write to.

Scope and Constraints
Understand the following scope and constraints regarding pre-authenticated requests:
• Users can't list bucket contents.
• You can create an unlimited number of pre-authenticated requests.
• There is no time limit to the expiration date that you can set.
• You can't edit a pre-authenticated request. If you want to change user access options in response to changing requirements, you must create a new pre-authenticated request.
• The target and actions for a pre-authenticated request are based on the creator's permissions. The request is not, however, bound to the creator's account login credentials. If the creator's login credentials change, a pre-authenticated request is not affected.
• You cannot delete a bucket that has a pre-authenticated request associated with that bucket or with an object in that bucket.

Working with Pre-Authenticated Requests
You can create, delete, or list pre-authenticated requests using the Console, using the CLI, or by using an SDK to access the API.

Important:
The unique URL provided by the system when you create a pre-authenticated request is the only way a user can access the bucket or object specified as the request target. Copy the URL to durable storage. The URL is displayed only at the time of creation and cannot be retrieved later.

After creating a pre-authenticated request, you can use a tool like curl to read and write data using the pre-authenticated request.

To put an object

$ curl -X PUT --data-binary '@<local-filename>' <unique-PAR-URL>

For example:

$ curl -X PUT --data-binary '@using-dita-guide.pdf'
https://objectstorage.us-phoenix-1.oraclecloud.com/p/j3DoSvgQHbUaw6ADzHkDlnaqMuXWeF_lhTxCiS9ngCw/n/docs/b/par-bucket/o/using-dita-guide.pdf

To get an object

$ curl -X GET <unique-PAR-URL>
For example:

```bash
$ curl -X GET https://objectstorage.us-phoenix-1.oraclecloud.com/p/j3DoSvqQHbUaw6ADzHkD1naqMuXWef_lhTxCiS9ngCw/n/namespace/b/par-bucket/o/using-dita-guide.pdf
```

### Using the Console

**To create a pre-authenticated request for a bucket**

See [Service Limits](#) on page 215 for a list of applicable limits and instructions for requesting a limit increase.

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment where the bucket is.
3. Click the bucket name.
4. Click **Pre-Authenticated Requests** under **Resources** to display the list of pre-authenticated requests.
5. Click **Create Pre-Authenticated Request**.
6. Provide the following information:
   - **Name**: The system automatically generates a default, pre-authenticated request name that reflects the current year, month, day, and time, for example `par-bucket-20191101-1327`.
     If you change this default or any other pre-authenticated request name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
   - **Pre-Authenticated Request Target**: Select **Bucket**.
   - **Expiration**: Accept the one week, system-generated expiration date or use the date and time editor to use a different expiration date and time.
7. Click **Create Pre-Authenticated Request**.

   After a request is created, the **Pre-Authenticated Request Details** dialog box displays the URL used to access the bucket.

8. Click **Copy** to copy the URL for future reference.

```
Note:
The unique URL provided by the system when you create a pre-authenticated request is the only way a user can access the bucket or object specified as the request target. Copy the URL to durable storage. The URL is displayed only at the time of creation and cannot be retrieved later.
```

9. Click **Close**.

**To create a pre-authenticated request for an object**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment where the bucket is.
3. Click the bucket name.
4. Click **Objects** under **Resources** to display the list of objects.
5. For the object you want to create a pre-authenticated request, click the Actions icon (three dots), and then click **Create Pre-Authenticated Request**.
6. Provide the following information:
   • **Name**: The system generates a default, pre-authenticated request name that reflects the current year, month, day, and time, for example `par-object-object-name-20191101-1429`. If you change this default or any other pre-authenticated request name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.
   • **Pre-Authenticated Request Target**: Select **Object**.
   • **Object Name**: The name of the object that you want authenticated by this rule.
   • **Access Type**: Select one of the following.
     - Permit read on the object
     - Permit writes to the object
     - Permit reads on and writes to the object
   • **Expiration**: Accept the one week, system-generated expiration date or use the date and time editor to a different expiration date and time.

7. Click **Create Pre-Authenticated Request**. After a request is created, the **Pre-Authenticated Request Details** dialog displays the URL used to access the object.

8. Click **Copy** to copy the URL for future reference.

   **Note:**
   The unique URL provided by the system when you create a pre-authenticated request is the only way a user can access the bucket or object specified as the request target. Copy the URL to durable storage. The URL is displayed only at the time of creation and cannot be retrieved later.

9. Click **Close**.

**To copy a pre-authenticated request ID**

To copy the ID for a pre-authenticated request to the clipboard, do the following:

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment where the bucket is.
3. Click the bucket name.
4. Click **Pre-Authenticated Requests** under **Resources** to display the list of pre-authenticated requests.
5. For the pre-authenticated request ID that you want to copy, click the Actions icon (three dots), and then click **Copy Pre-Authenticated Request ID**.

   The ID for the selected pre-authentication request is copied to the clipboard.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192. For a complete list of flags and options available for CLI commands, see the **Command Line Reference**.

**To create a pre-authenticated request for a bucket**

```bash
oci os preauth-request create --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <preauthenticated_request_name> --access-type AnyObjectWrite --time-expires <timestamp>
```

Note the following:

- To create a pre-authenticated request for a bucket, use the `AnyObjectWrite` enum value with the `--access-type` flag. Pre-authenticated requests for buckets permit writes to the bucket by default.
- The `<timestamp>` is required and must be an RFC 3339 timestamp. For example:

  2017-09-01T00:09:51.000+02:00.
Note:
The unique URL provided by the system when you create a pre-authenticated request is the only way a user can access the bucket or object specified as the request target. Copy the URL to durable storage. The URL is displayed only at the time of creation and cannot be retrieved later.

To create a pre-authenticated request for an object

**oci os preauth-request create --namespace <object_storage_namespace> --bucket-name <bucket_name> --name <preauthenticated_request_name> --access-type <enum_value> --time-expires <timestamp> -on <object_name_or_null>**

The `<enum_value>` for `--access-type` is one of the following:

- ObjectRead (permits read on the object)
- ObjectWrite (permits writes to the object)
- ObjectReadWrite (permits reads on and writes to the object)

The `<timestamp>` is required and must be an RFC 3339 timestamp. For example: 2017-09-01T00:09:51.000+02:00.

Avoid entering confidential information in the pre-authenticated request name.

Note:
The unique URL provided by the system when you create a pre-authenticated request is the only way a user can access the bucket or object specified as the request target. Copy the URL to durable storage. The URL is displayed only at the time of creation and cannot be retrieved later.

To list a pre-authenticated request

**oci os preauth-request list --namespace <object_storage_namespace> --bucket-name <bucket_name>**

To get a pre-authenticated request

**oci os preauth-request get --namespace <object_storage_namespace> --bucket-name <bucket_name> --par-id <preauthenticated_request_id>**

To delete a pre-authenticated request

**oci os preauth-request delete --namespace <object_storage_namespace> --bucket-name <bucket_name> --par-id <preauthenticated_request_id>**

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to work with pre-authenticated requests:

- CreatePreauthenticatedRequest
- DeletePreauthenticatedRequest
- GetPreauthenticatedRequest
- ListPreauthenticatedRequests
Copying Objects

This topic describes how to copy objects in Object Storage. You can copy objects to other buckets in the same region and to buckets in other regions.

Required IAM Policies

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object copy does not work if you do not authorize the Object Storage service to copy objects on your behalf. See Service Permissions on page 3487 for more information.</td>
</tr>
</tbody>
</table>

User Permissions

You must have the required access to both the source and destination buckets when performing an object copy. You must also have permissions to manage objects in the source and destination buckets.

For administrators:

- You can create a policy that lets the specified IAM group manage Object Storage namespaces, buckets, and their associated objects in all compartments in the tenancy:

  Allow group <IAM_group_name> to manage object-family in tenancy

- Alternatively, you can create policies that reduce the scope of access. For example, to let the specified group manage only buckets and objects in a particular compartment in the tenancy:

  Allow group <IAM_group_name> to manage buckets in compartment <compartment_name>

For more information about other alternatives for writing policies, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

Service Permissions

Because Object Storage is a regional service, you must authorize the Object Storage service for each region carrying out copy operations on your behalf. For example, you might authorize the Object Storage service in region US East (Ashburn) to manage objects on your behalf. After you authorize the Object Storage service, you can copy an object stored in a US East (Ashburn) bucket to a bucket in another region.

To determine the region identifier value of an Oracle Cloud Infrastructure region, see Regions and Availability Domains on page 180.

For administrators:

To enable object copy, you must authorize the service to manage objects on your behalf:

- You can create a policy that authorizes the service in the specified region to manage Object Storage namespaces, buckets, and their associated objects in all compartments in the tenancy:

  Allow service objectstorage-<region_identifier> to manage object-family in tenancy
Instead of using the policy verb `manage`, you can create a policy that reduces the scope of access by instead using one of the following statements:

```bash
Allow service objectstorage-<region_identifier> to manage object-family in tenancy where any {request.permission='OBJECT_READ',
  request.permission='OBJECT_INSPECT', request.permission='OBJECT_CREATE',
  request.permission='OBJECT_OVERWRITE',
  request.permission='OBJECT_DELETE'}

Allow service objectstorage-<region_identifier> to manage object-family in compartment <compartment_name>
  where any {request.permission='OBJECT_READ',
  request.permission='OBJECT_INSPECT', request.permission='OBJECT_CREATE',
  request.permission='OBJECT_OVERWRITE',
  request.permission='OBJECT_DELETE'}
```

**Copy Object Work Requests**

The Object Storage service handles copy requests asynchronously. The service creates a queue for copy requests, and then processes the requests when system resources become available. To provide visibility for in-progress copy operations, Object Storage creates a work request. You can track the progress of the copy operation by monitoring the status of the work request.

The work request statuses are:

- **ACCEPTED**
  The copy request is in the work request queue to be processed.

- **IN PROGRESS**
  The object copy is in progress.

- **SUCCEEDED**
  The copy operation has successfully completed.

- **CANCELLING**
  The copy request is in the process of being canceled.

- **CANCELED**
  The copy request has been canceled.

- **FAILED**
  The copy operation has failed. Work requests that do not complete because of overwrite rules or insufficient user authorizations are assigned the failed status.

  You can determine the reason a copy failed in the following ways:

  - To use the CLI, see To obtain the details of a failed copy work request on page 3491.
  - To use the API, see ListWorkRequestErrors.

**Copy Object Overwrite Rules**

Use overwrite rules to control the copying of objects based on their entity tag (ETag) values.

- **Overwrite destination object**: Use this option when you do not want to limit a copy operation by an ETag value. This option is the default. This option can be used for any copy operation, regardless of whether it involves overwriting an existing object.

- **Do not overwrite any destination object**: Use this option to prevent the overwriting an existing copy of an object in the destination location, regardless of the destination object's ETag value.
• **Overwrite destination object only if it matches the specified ETag**: Use this option to prevent the accidental overwriting of an object in the destination location that does not have the specified ETag. When you use this option, the copy operation only succeeds if the ETag you supply when initiating the copy request matches the ETag of the destination object.

• **Copy object only if the source matches the specified ETag**: Use this option if you want the copy operation successful only if the ETag you supply when initiating the copy request matches the ETag of the source object. For objects that are intentionally updated and overwritten as part of data management activity, this option ensures that only the specified version of the object (as indicated by the ETag) is allowed to be copied. If the object's ETag value changes after the copy work request is created, but before the copy operation is run, the copy operation will not complete.

Caution: If you overwrite an object, the operation cannot be undone.

### Scope and Constraints

- Objects cannot be copied directly from Archive Storage. To copy objects that are currently in Archive Storage, you must first restore the object to the Standard Object Storage tier. Objects can be copied directly to Archive tier buckets from the Standard or Infrequent Access tiers. When you copy objects into an Archive Storage bucket, the copy of the object is immediately archived.
- Specify an existing target bucket for the copy request. The copy operation does not automatically create buckets.
- When an object is copied, the destination object receives a new ETag value.
- If you rename, overwrite, or delete a source object during a copy operation, the copy operation fails and the destination object is not created or overwritten.
- Bulk copying is not supported. Identify a single object in the copy request.

### Using the Console

The Console consumes the REST API and is subject to the same considerations as any Oracle Cloud Infrastructure client.

**To make a copy of an object**

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment that contains the bucket that contains your object.
3. Select the bucket containing the object that you want to copy.
4. Click Objects under Resources to display a list of objects in the bucket.
5. For the object you want to copy (the source object), click the Actions icon (three dots), and then click Copy.
6. In the Copy Object dialog, enter the following:
   - **Destination Namespace**: The Object Storage Namespace of the destination bucket for your copied object. The namespace string of your tenancy is supplied as the default value.
   - **Destination Region**: The Oracle Cloud Infrastructure region containing the destination bucket for your copied object. Your tenancy must be subscribed to a region for you to copy an object to a bucket in that region.
   - **Destination Bucket**: The name of the destination bucket for your copied object. Specify an existing target bucket. The copy operation does not automatically create buckets.
   - **Destination Object Name**: Optionally, you can specify a different destination object name. By default, the Destination Object Name is the same name as the object you are copying.
   - **Destination Storage Tier**: If you are uploading to a Standard tier bucket, you can optionally specify the storage tier to upload the object to:
     - Infrequent Access
     - Archive
   - **Overwrite Rule**: Select the overwrite rule appropriate for your copy request. See Copy Object Overwrite Rules for information on the overwrite rule options.
7. Click **Copy Object**.
   
   A dialog confirms that your copy request was submitted successfully.

**To monitor the status of an object copy work request**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment containing your bucket.
3. Click the bucket name of the bucket containing the object being copied.
4. Click **Work Requests** under **Resources**.
   
   A list of work requests is displayed. The **status** of the request and details including object name, request ID, and the destination bucket's name, region, and **namespace** is also displayed.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**To make a copy of an object**

```
oci os object copy --namespace-name <object_storage_namespace> --bucket-name <source_bucket_name> --source-object-name <source_object> --destination-namespace <destination_namespace_string> --destination-region <destination_region> --destination-bucket <destination_bucket_name> --destination-object-name <destination_object_name>
```

For example:

```
oci os object copy --namespace-name ansh8lvrlzpy --bucket-name photos --source-object-name hummingbird.jpg --destination-namespace ansh8lvrlzpy --destination-region uk-london-1 --destination-bucket UK_photos --destination-object-name hummingbird.jpg
```

If you are uploading to a Standard tier bucket, you can optionally specify the storage tier to upload the object to:

- **Infrequent Access**
- **Archive**

```
oci os object copy --namespace-name <object_storage_namespace> --bucket-name <source_bucket_name> --source-object-name <source_object> --destination-namespace <destination_namespace_string> --destination-object-storage-tier <destination_object_storage_tier> --destination-region <destination_region> --destination-bucket <destination_bucket_name> --destination-object-name <destination_object_name>
```

For example:

```
oci os object copy --namespace-name ansh8lvrlzpy --bucket-name photos --source-object-name hummingbird.jpg --destination-namespace ansh8lvrlzpy --destination-object-storage-tier Archive --destination-region uk-london-1 --destination-bucket UK_photos --destination-object-name hummingbird.jpg
```

**To get the status of an object copy work request**

```
oci os work-request get --work-request-id <request_id>
```

If you do not have the work request ID, you can get a list of work requests, including the request IDs, for a specified compartment, see To get a list of work requests for a compartment on page 3491.
To obtain the details of a failed copy work request

```
oci os work-request-errors list --work-request-id <request_id>
```

If you do not have the work request ID, you can get a list of work requests, including the request IDs, for a specified compartment, see To get a list of work requests for a compartment on page 3491.

To get a list of work requests for a compartment

```
oci os work-request list --compartment-id <compartment_id>
```

To cancel a copy object work request

```
oci os work-request cancel --work-request-id <request_id>
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to view and manage work requests for copy object operations:

- CopyObject
- ListWorkRequests
- GetWorkRequest
- CancelWorkRequest
- ListWorkRequestErrors

Using Your Own Keys for Server-Side Encryption

The Oracle Cloud Infrastructure Object Storage service encrypts and decrypts all objects using 256-bit AES encryption. By default, Object Storage service manages the master encryption key used to encrypt each object's encryption keys.

You can alternatively employ one of these encryption strategies:

- You can assign a key that you created and control through the Oracle Cloud Infrastructure Vault service. See Overview of Vault on page 3952 for details.
- You can encrypt objects using your own encryption key. The key you supply is known as a customer-provided encryption key.

This topic provides the details for implementing and using server-side encryption with customer-provided keys (SSE-C).

About SSE-C

Using optional API headers, you can provide your own 256-bit AES encryption key that is used to encrypt and decrypt objects uploaded to and downloaded from Object Storage:

- When you upload an object, you supply the encryption key. Object Storage encrypts the object using that key and immediately deletes the key.
- When you want to download an object, you supply the same key that was used to encrypt the object and Object Storage decrypts and returns the object to you.

You manage the encryption keys and Object Storage manages the encryption and decryption.

**Important:**

Object Storage does not store your encryption keys. You are responsible for tracking the key that is associated with each object and rotating the key as necessary. If you lose your encryption key, you cannot retrieve your object.
Scope and Constraints

Understand the following scope and constraints regarding SSE-C:

- An SSE-C key cannot be associated with a bucket and can only be used to encrypt individual objects.
- You can encrypt objects using your own encryption key using pre-authenticated requests. To retrieve an SSE-C encrypted object using a pre-authenticated request, you need to specify your encryption key.
- To delete or rename an SSE-C encrypted object, you do not need to specify your encryption key.
- You can only specify either a kmsKeyId or an sseCustomerKey in the ReencryptObject request payload, not both. If the request payload is empty, the object is encrypted using the encryption key assigned to the bucket. The bucket encryption mechanism can either be a master encryption key managed by Oracle or the Vault service.
- You can only use the Object Storage APIs and the CLI to provide SSE-C keys. You can't use the Console to upload or retrieve objects using a customer-provided key.
- The Amazon S3 Compatibility API also supports SSE-C.

Using SSE-C

If you want to use your own keys for server-side encryption, specify the following three request headers with the encryption key information:

<table>
<thead>
<tr>
<th>Headers</th>
<th>Description</th>
<th>APIs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>opc-sse-customer-algorithm</td>
<td>Specifies &quot;AES256&quot; as the encryption algorithm.</td>
<td>CopyObject, GetObject, HeadObject, PutObject, CreateMultipartUpload, UploadPart</td>
</tr>
<tr>
<td>opc-sse-customer-key</td>
<td>Specifies the base64-encoded 256-bit encryption key to use to encrypt or decrypt the data.</td>
<td></td>
</tr>
<tr>
<td>opc-sse-customer-key-sha256</td>
<td>Specifies the base64-encoded SHA256 hash of the encryption key.</td>
<td></td>
</tr>
</tbody>
</table>

For CopyObject:

If the source object is encrypted with an SSE-C key, you must also specify the following three headers so that Object Storage can decrypt the object.

<table>
<thead>
<tr>
<th>Headers</th>
<th>Description</th>
<th>APIs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>opc-source-sse-customer-algorithm</td>
<td>Specifies &quot;AES256&quot; as the encryption algorithm to use to decrypt the source object.</td>
<td>CopyObject</td>
</tr>
<tr>
<td>opc-source-sse-customer-key</td>
<td>Specifies the base64-encoded 256-bit encryption key to use to decrypt the source object.</td>
<td></td>
</tr>
<tr>
<td>opc-source-sse-customer-key-sha256</td>
<td>Specifies the base64-encoded SHA256 hash of the encryption key used to decrypt the source object.</td>
<td></td>
</tr>
</tbody>
</table>

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.
If you are new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. For more information about Object Storage-specific policies, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

**Using the CLI**

You can also use your own encryption keys to encrypt objects using the CLI.

You can supply the optional parameter `--encryption-key-file <filename>` for the following commands:

- `oci os object put`
- `oci os object get`
- `oci os object head`
- `oci os object resume-put`
- `oci os object bulk-upload`
- `oci os object bulk-download`
- `oci os object copy`
- `oci os object reencrypt`

`<filename>` points to a file containing the base64-encoded string of the AES-256 encryption key. No other parameters are required. Object Storage decodes the key to compute the SHA256 hash of the encryption key.

If the source object is encrypted with an SSE-C key, you must also specify the optional parameter `--source-encryption-key-file <filename>` for the following commands:

- `oci os object copy`
- `oci os object reencrypt`

`<filename>` points to a file containing the base64-encoded string of the AES-256 source encryption key. No other parameters are required. Object Storage decodes the key to compute the SHA256 hash of the source encryption key.

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**Amazon S3 Compatibility API**

Using the Amazon S3 Compatibility API, customers can continue to use their existing Amazon S3 tools (for example, SDK clients) and partners can make minimal changes to their applications to work with Object Storage. The Amazon S3 Compatibility API and Object Storage datasets are congruent. If data is written to the Object Storage using the Amazon S3 Compatibility API, the data can be read back using the native Object Storage API and conversely.

**Differences between the Object Storage API and the Amazon S3 Compatibility API**

The Object Storage Service provided by Oracle Cloud Infrastructure and Amazon S3 use similar concepts and terminology. In both cases, data is stored as objects in buckets. The differences are in the implementation of features and tools for working with objects.

The following highlights the differences between the two storage technologies:

- **Compartments**
  
  Amazon S3 doesn't use compartments. By default, buckets created using the Amazon S3 Compatibility API or the Swift API are created in the root compartment of the Oracle Cloud Infrastructure tenancy. Instead, you can designate a different compartment for the Amazon S3 Compatibility API or Swift API to create buckets in.

- **Global bucket namespace**
  
  Object Storage doesn't use a global bucket namespace. Each tenant is associated with one default namespace that spans all compartments within a region. The namespace serves as a container for all of your buckets and objects. You control bucket names within your namespace, however, bucket names must be unique within each region. You can have a bucket named `MyBucket` in US West (Phoenix) and a bucket named `MyBucket` in Germany Central (Frankfurt).
• **Encryption**
  The Oracle Cloud Infrastructure Object Storage service encrypts all data at rest by default. Encryption can't be turned on or off using the API.

• **Object Level Access Control Lists (ACLs)**
  Oracle Cloud Infrastructure does not use ACLs for objects. Instead, IAM policies are used to manage access to compartments, buckets, and objects.

For more information, see [Overview of the Object Storage service](#).

**Amazon S3 Compatibility API Prerequisites**

To enable application access from Amazon S3 to Object Storage, you need to set up access to Oracle Cloud Infrastructure and modify your application.

**Setting up access to Oracle Cloud Infrastructure**

• [Sign Up for Oracle Cloud Infrastructure](#) and obtain a unique namespace.

• Create a [Customer Secret key](#). A Customer Secret key consists of an Access Key/Secret key pair.

**Modifying your application**

• Configure a new endpoint for the application that includes the namespace and the region identifier. For example: mynamespace.compat.objectstorage.us-phoenix-1.oraclecloud.com.

• Set the target region as one of the Oracle Cloud Infrastructure regions.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your application does not support setting the region identifier to the correct Oracle Cloud Infrastructure identifier, you must either set the region to us-east-1 or leave it blank. Using this configuration, you can only use the Amazon S3 Compatibility API in your Oracle Cloud Infrastructure home region. If you can manually set the region, you can use the application against any Oracle Cloud Infrastructure region.</td>
</tr>
</tbody>
</table>

• Configure the application to use the Customer Secret key. The Customer Secret Key consists of an Access Key and Secret Key. Both of these keys must be supplied to the application.

• The application must use path-based access. Virtual host-style access (accessing a bucket as bucketname.namespace.compat.objectstorage.region.oraclecloud.com) is not supported.

You can now use the Amazon S3 Compatibility API to access Object Storage in Oracle Cloud Infrastructure.

**Amazon S3 Compatibility API Support**

Amazon S3 Compatibility API support is provided at the bucket level and object level.

**Bucket APIs**

The following bucket APIs are supported:

• [DeleteBucket](#)

• [GetLocation](#)

• [HeadBucket](#)

• [GetService](#) (list all my buckets)

• [ListObjects](#)

• [PutBucket](#)

**Object APIs**

The following object APIs are supported:

• [BulkDelete](#)
Object Storage

- **DeleteObject**
- **GetObject**
- **HeadObject**
- **PutObject**
- **RestoreObjects**

**Multipart Upload APIs**

The following multipart upload APIs are supported:

- **AbortMultipartUpload**
- **CompleteMultipartUpload**
- **InitiateMultipartUpload**
- **ListParts**
- **ListUploads**
- **UploadPart**

**Tagging APIs**

The following tagging APIs are supported:

- **DeleteBucketTagging**
- **GetBucketTagging**
- **PutBucketTagging**

**SSE-C Support**

Using optional API headers, you can provide your own 256-bit AES encryption key that is used to encrypt and decrypt objects uploaded to and downloaded from Object Storage.

If you want to use your own keys for server-side encryption, specify the following three request headers with the encryption key information:

<table>
<thead>
<tr>
<th>Headers</th>
<th>Description</th>
<th>APIs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-amz-server-side-encryption-customer-algorithm</td>
<td>Specifies &quot;AES256&quot; as the encryption algorithm.</td>
<td>GetObject, HeadObject</td>
</tr>
<tr>
<td>x-amz-server-side-encryption-customer-key</td>
<td>Specifies the base64-encoded 256-bit encryption key to use to encrypt or decrypt the data.</td>
<td>PutObject, InitiateMultipartUpload, UploadPart</td>
</tr>
<tr>
<td>x-amz-server-side-encryption-customer-key-md5</td>
<td>Specifies the base64-encoded 128-bit MD5 digest of the encryption key. This value is used to check the integrity of the encryption key.</td>
<td></td>
</tr>
</tbody>
</table>

Object Storage has distinct APIs for copying objects and copying parts. Amazon S3 uses the presence of the following headers in **PutObject** and **UploadPart** to determine copy operations. To copy a source object that is encrypted with an SSE-C key, you must specify these three headers so that Object Storage can decrypt the object.

<table>
<thead>
<tr>
<th>Headers</th>
<th>Description</th>
<th>APIs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-amz-copy-source-server-side-encryption-customer-algorithm</td>
<td>Specifies &quot;AES256&quot; as the encryption algorithm to use to decrypt the source object.</td>
<td>PutObject, UploadPart</td>
</tr>
<tr>
<td>x-amz-copy-source-server-side-encryption-customer-key</td>
<td>Specifies the base64-encoded 256-bit encryption key to use to decrypt the source object.</td>
<td></td>
</tr>
<tr>
<td>Headers</td>
<td>Description</td>
<td>APIs Supported</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>x-amz-copy-source-server-side-encryption-customer-key-md5</td>
<td>Specifies the base64-encoded 128-bit MD5 digest of the encryption key used to decrypt the source object.</td>
<td></td>
</tr>
</tbody>
</table>

**Supported Amazon S3 Clients**

Here are some examples of configuring various client applications to talk to Object Storage's Amazon S3-compatible endpoints. Use an existing or create a special signing key to authenticate with Amazon S3, which is an Access Key/Secret Key pair. See Managing User Credentials on page 2456 for details.

**AWS SDK for Java**

The following is an example of configuring AWS SDK for Java.

```java
// Get S3 credentials from the console and put them here
AWSCredentialsProvider credentials = new AWSStaticCredentialsProvider(new
BasicAWSCredentials("gQ4+YC530sBa8qZI6WcbUbtH8oar0exampleuniqueID", "7fa22331be62bf4605dc9a42aaeexampleuniqueID"));

// Your namespace
String namespace = "namespace";

// The region to connect to
String region = "us-ashburn-1";

// Create an S3 client pointing at the region
String endpoint = String.format("%s.compat.objectstorage.%s.oraclecloud.com",namespace,region);
AwsClientBuilder.EndpointConfiguration endpointConfiguration = new
AwsClientBuilder.EndpointConfiguration(endpoint, region);
AmazonS3 client = AmazonS3Client.builder()
  .standard()
  .withCredentials(credentials)
  .withEndpointConfiguration(endpointConfiguration)
  .disableChunkedEncoding()
  .enablePathStyleAccess()
  .build();
```

**AWS SDK for Javascript**

The following is an example of configuring AWS SDK for Javascript.

```javascript
s3 = new AWS.S3({
  region: 'us-ashburn-1',
  endpoint: 'https://' + mynamespace + '.compat.objectstorage.us-ashburn-1.oraclecloud.com',
  accessKeyId: 'gQ4+YC530sBa8qZI6WcbUbtH8oar0exampleuniqueID',
  secretAccessKey: '7fa22331be62bf4605dc9a42aaeexampleuniqueID',
  s3ForcePathStyle: true,
  signatureVersion: 'v4',
});
```
**AWS SDK for Python (Boto 3)**

The following is an example of configuring AWS SDK for Python (Boto 3).

```python
import boto3
s3 = boto3.resource('s3',
   aws_access_key_id="gQ4+YC530sBa8qZ167WcbUbtH8oar0exampleuniqueID",
   aws_secret_access_key="7fa22331ebe62bf4605dc9a42aaexampleuniqueID",
   region_name="us-phoenix-1", # Region name here that matches the endpoint
   endpoint_url="https://mynamespace.compat.objectstorage.us-
   phoenix-1.oraclecloud.com" # Include your namespace in the URL
)

# Print out the bucket names
for bucket in s3.buckets.all():
    print bucket.name
```

**Designating Compartments for the Amazon S3 Compatibility and Swift APIs**

In the Oracle Cloud Infrastructure Object Storage service, a bucket is a container for storing objects in a compartment within an Object Storage namespace. A bucket is associated with a single compartment and data is stored as objects in buckets.

In addition to the native Object Storage APIs, Object Storage provides API support for both Amazon S3 Compatibility API and Swift API. However these APIs do not understand the Oracle Cloud Infrastructure concept of a compartment. By default, buckets created using the Amazon S3 Compatibility API or the Swift API are created in the root compartment of the Oracle Cloud Infrastructure tenancy. Instead, you can designate a different compartment for the Amazon S3 Compatibility API or Swift API to create buckets in.

When you designate a different compartment to use for the Amazon S3 Compatibility API or Swift API, any new buckets you create using the Amazon S3 Compatibility API or the Swift API are created in this newly designated compartment. Buckets previously created in a different compartment are not automatically moved to the newly designated compartment. See Managing Buckets on page 3398 if you want to move previously created buckets to this newly designated compartment.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

Compartments have policies that indicate what actions a user can perform on a bucket and all the objects in the bucket.

For administrators:

- To change the default compartments for Amazon S3 Compatibility API and Swift API, a user must belong to a group with NAMESPACE_UPDATE permissions.
- To see the current default compartments for Amazon S3 Compatibility API and Swift API, a user must belong to a group with NAMESPACE_READ permissions.
- To move a bucket to a different compartment, a user must belong to a group with BUCKET_UPDATE and BUCKET_CREATE permissions in the source compartment, and BUCKET_CREATE permissions in the target compartment.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for buckets and objects, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324.
**Viewing and Specifying Designated Compartments**

You can view the current default compartment designations for Amazon S3 Compatibility API and Swift API data. If your permissions allow, you can also change the Amazon S3 Compatibility API and Swift API compartment designations.

Designated compartment names:
- Must be unique across all the compartments in your tenancy.
- Can be from 1 to 100 characters in length.
- Must not contain confidential information.
- Valid are letters (upper or lower case), numbers, hyphens, and underscore.

**Using the Console**

**To view your Amazon S3 Compatibility API and Swift API compartment designations**

Open the Profile menu and click Tenancy: `<your_tenancy_name>`.

Your default compartment designations for the APIs are listed under Object Storage Settings.

**To edit your tenancy's Amazon S3 Compatibility API and Swift API compartment designations**

1. Open the Profile menu and click Tenancy: `<your_tenancy_name>`.
2. Click Edit Object Storage Settings.
3. In the Edit Object Storage Settings dialog:
   - Select the compartment that you want for the Amazon S3 Compatibility API Designated Compartment.
   - Select the compartment that you want for the Swift API Designated Compartment.
4. Click Save.

   The new Object Storage Settings are displayed.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**To get your tenancy's Amazon S3 Compatibility API and Swift API compartment designations**

Use this CLI command to display metadata associated with the Amazon S3 and Swift compartments for the specified namespace in your tenancy.

```
oci os ns get-metadata --namespace <object_storage_namespace>
```

For example:

```
oci os ns get-metadata --namespace MyNamespace
{
   "data": {
      "default-s3-compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "default-swift-compartment-id": "ocid.compartment.oc1..exampleuniqueID",
      "namespace": "MyNamespace"
   }
}
```

**To update your tenancy's Amazon S3 Compatibility API compartment designation**

Use this CLI command to specify the default Amazon S3 compartment for the specified namespace in your tenancy.

```
oci os ns update-metadata --namespace <object_storage_namespace> --default-s3-compartment-id <your_oci_compartment_id>
```
<your_oci_compartment_id> specifies a compartment that is not the root compartment of your tenancy.

For example:

```bash
oci os ns update-metadata --namespace MyNamespace --default-s3-compartment-id ocid.compartment.oc1..exampleuniqueID
{
  "data": {
    "default-s3-compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "default-swift-compartment-id": null,
    "namespace": null
  }
}
```

To update your tenancy's Swift API compartment designations

Use this CLI command to specify the default Swift compartment for the specified namespace in your tenancy.

```bash
oci os ns update-metadata --namespace <object_storage_namespace> --default-swift-compartment-id <your_oci_compartment_id>
```

<your_oci_compartment_id> specifies a compartment that is not the root compartment of your tenancy.

For example:

```bash
oci os ns update-metadata --namespace MyNamespace --default-swift-compartment-id ocid.compartment.oc1..exampleuniqueID
{
  "data": {
    "default-s3-compartment-id": null,
    "default-swift-compartment-id": "ocid.compartment.oc1..exampleuniqueID",
    "namespace": null
  }
}
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operation to get your default Amazon S3 Compatibility API and Swift API compartment designations, and change those compartment designations:

- GetNamespaceMetadata
- UpdateNamespaceMetadata

Object Storage Metrics

You can monitor the health, capacity, and performance of your buckets and objects by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace oci_objectstorage (the Object Storage service).

Resources include buckets and objects.

Overview of the Object Storage Service Metrics

Object Storage can store an unlimited amount of unstructured data of any content type, including analytic data and rich content, like images and videos. The Object Storage service metrics help you measure the amount of storage you're using. You can also use these metrics to monitor the performance of requests in terms of latency and utilization as measured by counts of requests made per bucket.
**Required IAM Policy**

To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

**Available Metrics: oci_objectstorage**

The metrics listed in the following tables are automatically available for any buckets you create. You do not need to enable monitoring on the resource to get these metrics. However, you must have an object stored in a bucket to get any metrics. Buckets with no objects emit no metric data.

Each metric includes the following dimensions:

**RESOURCEID**

The OCID of the bucket to which the metric applies.

**RESOURCEDISPLAYNAME**

The name of the bucket.

**TIER**

The storage tier (standard or archive) where the object resides.

**Default Metrics**

The following default metric charts are available for each Object Storage bucket from the bucket details page. See To view default metric charts for a bucket.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description/ Emit Frequency</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ObjectCount</td>
<td>Number of Objects</td>
<td>count</td>
<td>The count of objects in the bucket, excluding any multipart upload parts that have not been discarded (aborted) or committed. Emit frequency: every hour</td>
<td>resourceID resourceDisplayName tier</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description/ Emit Frequency</td>
<td>Dimensions</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>StoredBytes</td>
<td>Bucket Size</td>
<td>bytes</td>
<td>The size of the bucket, excluding any multipart upload parts that have not been discarded (aborted) or committed. Emit frequency: every hour</td>
<td></td>
</tr>
</tbody>
</table>

**Custom Query Metrics**

The following custom query metric charts are available using Metrics Explorer. See To view custom query metric charts using Metrics Explorer on page 3503.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description/ Emit Frequency</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllRequests</td>
<td>All Requests Count</td>
<td>count</td>
<td>The total number of all HTTP requests made in a bucket. Emit frequency: every 100 ms</td>
<td>resourceID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resourceDisplayName</td>
</tr>
<tr>
<td>ClientErrors</td>
<td>Client-Side Error Count</td>
<td>count</td>
<td>The total number of 4xx errors for requests made in a bucket. Emit frequency: every 100 ms</td>
<td></td>
</tr>
</tbody>
</table>
| EnabledOLM     | Enabled Object Lifecycle Management | count | Indicates whether a bucket has any executable Object Lifecycle Management policies configured. EnabledOLM emits:  
• 1 if policies are configured  
• 0 if no policies are configured  
Emit frequency: every 3 hours |                                  |
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description/ Emit Frequency</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirstByteLatency</td>
<td>First Byte Latency Time</td>
<td>time (ms)</td>
<td>The per-request time measured from the time Object Storage receives the complete request to when Object Storage returns the first byte of the response. Emit frequency: every 100 ms</td>
<td></td>
</tr>
<tr>
<td>PostRequests</td>
<td>PostObject Request Count</td>
<td>count</td>
<td>The total number of HTTP Post requests made in a bucket. Emit frequency: every 100 ms</td>
<td></td>
</tr>
<tr>
<td>PutRequests</td>
<td>PutObject Request Count</td>
<td>count</td>
<td>The total number of PutObject requests made in a bucket. Emit frequency: every 100 ms</td>
<td></td>
</tr>
<tr>
<td>TotalRequestLatency</td>
<td>Overall Latency Time</td>
<td>time (ms)</td>
<td>The per-request time from the first byte received by Object Storage to the last byte sent from Object Storage. Emit frequency: every 100 ms</td>
<td></td>
</tr>
<tr>
<td>UncommittedParts</td>
<td>Incomplete MultiPart Upload Size</td>
<td>bytes</td>
<td>The size of any multipart upload parts that have not been discarded (aborted) or committed. Emit frequency: every hour</td>
<td>resourceID, resourceDisplayName, tier</td>
</tr>
</tbody>
</table>
Using the Console
To view default metric charts for a bucket
1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the Compartment that contains the bucket you want to view, and then click the bucket's name.
3. In the Resources menu, click Metrics.

The Metrics page displays a default set of charts for the current bucket.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts by dimension
1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Metric Namespace, select oci_objectstorage.
3. For Dimensions, click Add.
4. For Dimension Name, select a dimension and then select a Dimension Value.

Add more dimensions as needed.
5. Click Done.

The Service Metrics page displays a default set of charts for the selected metric namespace and dimension. For more information about the emitted metrics, see the foregoing table. You can also use the Monitoring service to create custom queries.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view custom query metric charts using Metrics Explorer
1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.

The Metrics Explorer page displays an empty chart with fields to build a query.
2. Select a compartment.
3. From Metric Namespace, select oci_objectstorage.
4. From Metric Name, select a metric.
5. (Optional) Refine your query.
   For instructions, see To create a query on page 2702.
6. Click Update Chart.

The chart shows the results of your new query. You can optionally add more queries by clicking Add Query below the chart.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:
- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Accessing Object Storage Resources Across Tenancies

This topic describes how to write policies that let your tenancy access Object Storage resources in other tenancies.
If you're new to policies, see Getting Started with Policies on page 2135 and Details for Object Storage, Archive Storage, and Data Transfer on page 2324.

Cross-Tenancy Policies

Your organization might also want to share resources with another organization that has its own tenancy. It could be another business unit in your company, a customer of your company, a company that provides services to your company, and so on. In cases like these, you need cross-tenancy policies in addition to the required user and service policies described previously.

To access and share resources, the administrators of both tenancies need to create special policy statements that explicitly state the resources that can be accessed and shared. These special statements use the words Define, Endorse, and Admit.

Endorse, Admit, and Define Statements

Here's an overview of the special verbs used in cross-tenancy statements:

- **Endorse**: States the general set of abilities that a group in your own tenancy can perform in other tenancies. The Endorse statement always belongs in the tenancy with the group of users crossing the boundaries into the other tenancy to work with that tenancy's resources. In the examples, we refer to this tenancy as the source.

- **Admit**: States the kind of ability in your own tenancy that you want to grant a group from the other tenancy. The Admit statement belongs in the tenancy who is granting "admittance" to the tenancy. The Admit statement identifies the group of users that requires resource access from the source tenancy and identified with a corresponding Endorse statement. In the examples, we refer to this tenancy as the destination.

- **Define**: Assigns an alias to a tenancy OCID for Endorse and Admit policy statements. A Define statement is also required in the destination tenancy to assign an alias to the source IAM group OCID for Admit statements. Define statements must be included in the same policy entity as the endorse or the admit statement.

The Endorse and Admit statements work together, but they reside in separate policies, one in each tenancy. Without a corresponding statement that specifies access, a particular Endorse or Admit statement grants no access. Agreement is required from both tenancies.

Source tenancy policy statements

The source administrator creates policy statements that endorse a source IAM group allowed to manage resources in the destination tenancy.

Here is an example of a broad policy statement that endorses the IAM group StorageAdmins group to do anything with all Object Storage resources in any tenancy:

```plaintext
Endorse group StorageAdmins to manage object-family in any-tenancy
```

To write a policy that reduces the scope of tenancy access, the destination administrator must provide the destination tenancy OCID. Here is an example of policy statements that endorse the IAM group StorageAdmins group to manage Object Storage resources in the DestinationTenancy only:

```plaintext
Define tenancy DestinationTenancy as ocid1.tenancy.oc1..<unique_ID>
Endorse group StorageAdmins to manage object-family in tenancy DestinationTenancy
```

Destination tenancy policy statements

The destination administrator creates policy statements that:

- Defines the source tenancy and IAM group that is allowed to access resources in your tenancy. The source administrator must provide this information.

- Admits those defined sources to access Object Storage resources that you want to allow access to in your tenancy.
Here is an example of policy statements that endorse the IAM group StorageAdmins in the source tenancy to do anything with all Object Storage resources in your tenancy:

```
Define tenancy SourceTenancy as ocid1.tenancy.oc1..<unique_ID>
Define group StorageAdmins as ocid1.group.oc1..<unique_ID>
Admit group StorageAdmins of tenancy SourceTenancy to manage object-family in tenancy
```

Here is an example of policy statements that endorse the IAM group StorageAdmins in the source tenancy to manage Object Storage resources only the SharedBuckets compartment:

```
Define tenancy SourceTenancy as ocid1.tenancy.oc1..<unique_ID>
Define group StorageAdmins as ocid1.group.oc1..<unique_ID>
Admit group StorageAdmins of tenancy SourceTenancy to manage object-family in compartment SharedBuckets
```

**Hadoop Support**

Using the HDFS connector, you can run Hadoop or Spark jobs against data in the Oracle Cloud Infrastructure Object Storage service. The connector has the following features:

- Supports read and write data stored in Object Storage
- Is compatible with existing buckets of data
- Is compatible with Hadoop 2.7.2

For information about downloading, configuring, and using the HDFS connector, see [HDFS Connector for Object Storage](#) on page 4347.
Chapter 29

Registry

This chapter explains how to store, share, and manage development artifacts like Docker images in an Oracle-managed registry.

Overview of Registry

Oracle Cloud Infrastructure Registry is an Oracle-managed registry that enables you to simplify your development to production workflow. Oracle Cloud Infrastructure Registry makes it easy for you as a developer to store, share, and manage development artifacts like Docker images. And the highly available and scalable architecture of Oracle Cloud Infrastructure ensures you can reliably deploy your applications. So you don't have to worry about operational issues, or scaling the underlying infrastructure.

You can use Oracle Cloud Infrastructure Registry as a private Docker registry for internal use, pushing and pulling Docker images to and from the Registry using the Docker V2 API and the standard Docker command line interface (CLI). You can also use Oracle Cloud Infrastructure Registry as a public Docker registry, enabling any user with internet access and knowledge of the appropriate URL to pull images from public repositories in Oracle Cloud Infrastructure Registry.

Oracle Cloud Infrastructure Registry supports private access from other Oracle Cloud Infrastructure resources in a virtual cloud network (VCN) in the same region through a service gateway. Setting up and using a service gateway on a VCN lets resources (such as worker nodes in clusters managed by Container Engine for Kubernetes) access Oracle Cloud Infrastructure services such as Oracle Cloud Infrastructure Registry without exposing them to the public internet. No internet gateway is required and resources can be in a private subnet and use only private IP addresses. For more information, see Access to Oracle Services: Service Gateway on page 3256.

Oracle Cloud Infrastructure Registry is integrated with IAM, which provides easy authentication with native Oracle Cloud Infrastructure identity.

For an introductory tutorial, see Pushing an Image to Oracle Cloud Infrastructure Registry.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

For general information about using the API, see REST APIs on page 4368.

Note that Oracle Cloud Infrastructure Registry fully implements a Docker protocol that enables you to use the Docker Registry HTTP API (as well as the Oracle Cloud Infrastructure API) to manage images. See Preparing for Registry...
on page 3507 for the list of regional endpoints, and see the Docker documentation for information about using the Docker Registry HTTP API.

**Resource Identifiers**

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers on page 197.

**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you're a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Registry Capabilities and Limits**

In each region that is enabled for your tenancy, you can create up to 500 repositories in Oracle Cloud Infrastructure Registry consuming a maximum of 500 GB in total (if you need more storage, Contact Us). Each repository can hold up to 100,000 images. See Service Limits on page 215.

**Required IAM Service Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're new to policies, see Getting Started with Policies and Common Policies.

For more details about policies for Oracle Cloud Infrastructure Registry, see:

- Policies to Control Repository Access on page 3527
- Details for Registry on page 2335

**Preparing for Registry**

Before you can push and pull Docker images to and from Oracle Cloud Infrastructure Registry:

- You must have access to an Oracle Cloud Infrastructure tenancy. The tenancy must be subscribed to one or more of the regions in which Registry is available (see Availability by Region on page 3508).
- You must have access to the Docker CLI (for example, to push and pull images on a local machine, you'll need to have installed Docker on the local machine).
- You must either belong to a group to which a policy grants the appropriate permissions, or belong to the tenancy's Administrators group. See Policies to Control Repository Access on page 3527.
- You must have an Oracle Cloud Infrastructure auth token. If you don't have an auth token already, see Getting an Auth Token on page 3527.
Registry

Availability by Region

Registry is available in the Oracle Cloud Infrastructure regions listed at Regions and Availability Domains on page 180. Refer to that topic to see region identifiers, region keys, and availability domain names.

Note that Oracle Cloud Infrastructure Registry fully implements a Docker protocol that enables you to use the Docker Registry HTTP API (as well as the Oracle Cloud Infrastructure API) to manage images at the regional endpoints below. See the Docker documentation for information about using the Docker Registry HTTP API.

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Available Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td>• <a href="https://ap-melbourne-1.ocir.io">https://ap-melbourne-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://mel.ocir.io">https://mel.ocir.io</a></td>
</tr>
<tr>
<td>India South (Hyderabad)</td>
<td>• <a href="https://ap-hyderabad-1.ocir.io">https://ap-hyderabad-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://hyd.ocir.io">https://hyd.ocir.io</a></td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>• <a href="https://ap-mumbai-1.ocir.io">https://ap-mumbai-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://bom.ocir.io">https://bom.ocir.io</a></td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>• <a href="https://ap-osaka-1.ocir.io">https://ap-osaka-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://kix.ocir.io">https://kix.ocir.io</a></td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td>• <a href="https://ap-seoul-1.ocir.io">https://ap-seoul-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://icn.ocir.io">https://icn.ocir.io</a></td>
</tr>
<tr>
<td>South Korea North (Chuncheon)</td>
<td>• <a href="https://ap-chuncheon-1.ocir.io">https://ap-chuncheon-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://yny.ocir.io">https://yny.ocir.io</a></td>
</tr>
<tr>
<td>Australia East (Sydney)</td>
<td>• <a href="https://ap-sydney-1.ocir.io">https://ap-sydney-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://syd.ocir.io">https://syd.ocir.io</a></td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td>• <a href="https://ap-tokyo-1.ocir.io">https://ap-tokyo-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://nrt.ocir.io">https://nrt.ocir.io</a></td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>• <a href="https://ca-montreal-1.ocir.io">https://ca-montreal-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://yul.ocir.io">https://yul.ocir.io</a></td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>• <a href="https://ca-toronto-1.ocir.io">https://ca-toronto-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://yyz.ocir.io">https://yyz.ocir.io</a></td>
</tr>
<tr>
<td>Netherlands Northwest (Amsterdam)</td>
<td>• <a href="https://eu-amsterdam-1.ocir.io">https://eu-amsterdam-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://ams.ocir.io">https://ams.ocir.io</a></td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>• <a href="https://eu-frankfurt-1.ocir.io">https://eu-frankfurt-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://fra.ocir.io">https://fra.ocir.io</a></td>
</tr>
<tr>
<td>Switzerland North (Zurich)</td>
<td>• <a href="https://eu-zurich-1.ocir.io">https://eu-zurich-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://zrh.ocir.io">https://zrh.ocir.io</a></td>
</tr>
<tr>
<td>UAE East (Dubai)</td>
<td>• <a href="https://me-dubai-1.ocir.io">https://me-dubai-1.ocir.io</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://dxb.ocir.io">https://dxb.ocir.io</a></td>
</tr>
<tr>
<td>Region Name</td>
<td>Available Endpoints</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| Saudi Arabia West (Jeddah)     | https://me-jeddah-1.ocir.io  
|                                | https://jed.ocir.io     |
| Chile (Santiago)               | https://sa-santiago-1.ocir.io  
|                                | https://scl.ocir.io     |
| Brazil East (Sao Paulo)        | https://sa-saopaulo-1.ocir.io  
|                                | https://gru.ocir.io     |
| UK South (London)              | https://uk-london-1.ocir.io  
|                                | https://lhr.ocir.io     |
| UK West (Newport)              | https://uk-cardiff-1.ocir.io  
|                                | https://cwl.ocir.io     |
| US East (Ashburn)              | https://us-ashburn-1.ocir.io  
|                                | https://iad.ocir.io     |
| US West (Phoenix)              | https://us-phoenix-1.ocir.io  
|                                | https://phx.ocir.io     |
| US West (San Jose)             | https://us-sanjose-1.ocir.io  
|                                | https://sjc.ocir.io     |

Registry Concepts

This topic describes key concepts you need to understand when using Oracle Cloud Infrastructure Registry.

Images

You can store, share, and manage Docker images in Oracle Cloud Infrastructure Registry. A Docker image is a read-only template with instructions for creating a Docker container. A Docker image holds the application that you want Docker to run as a container, along with any dependencies. To create a Docker image, you first create a Dockerfile to describe that application. You then build the Docker image from the Dockerfile. Having created a Docker image, you store it in a Docker registry such as Oracle Cloud Infrastructure Registry.

Typically, you’ll group together different versions of the same Docker image into a named repository in the registry (for example, into a repository named 'project01/acme-web-app'), and give each image version a different tag (for example, '4.6.3'). So each image in the registry is uniquely identified by the combination of its repository name and its tag (for example, 'project01/acme-web-app:4.6.3', 'project01/acme-web-app:4.6.4', and so on).

Repositories

A repository is a meaningfully named collection of related images grouped together for convenience in Oracle Cloud Infrastructure Registry. Typically, you’ll group together different versions of the same source image into the same repository (for example, into a repository named project01/acme-web-app), and give each image version a different tag (for example, 4.6.3). So each image in the registry is uniquely identified by the combination of its repository name and its tag (for example, project01/acme-web-app:4.6.3, project01/acme-web-app:4.6.4, and so on).

Repositories can be private or public. Any user with internet access and knowledge of the appropriate URL can pull images from a public repository in Oracle Cloud Infrastructure Registry.
A repository exists within a particular tenancy, region, and compartment. When referring to the tenancy that owns a repository, you specify the tenancy's namespace. The tenancy namespace is an auto-generated random string of alphanumeric characters. For example, the namespace of the `acme-dev` tenancy might be `ansh81vru1zp`. Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, `acme-dev`). To find out the tenancy namespace of the current tenancy, open the Profile menu and click Tenancy:

You must belong to the tenancy's Administrators group or have been granted the REPOSITORY_MANAGE permission to:

- create a new public repository
- change an existing repository into a public repository
- change an existing public repository into a private repository

If you make a repository private, you (along with users belonging to the tenancy's Administrators group) will be able to perform any operation on the repository. You can use identity policies to allow other users to perform other operations on repositories (both public and private) that you create.

Usually, before pushing any images, you'll create an empty repository in a compartment and give the repository a name (for example, `project01/acme-web-app`). If you belong to the tenancy's Administrators group or have been granted the REPOSITORY_MANAGE permission, you can also specify whether the repository is to be private or public (see Policies to Control Repository Access on page 3527). Having created the repository, images you subsequently push to Oracle Cloud Infrastructure Registry that include the repository name are pushed to that repository.

For example, for convenience you might want to group together multiple versions of an image in the `acme-dev` tenancy in the Ashburn region into the repository called `project01/acme-web-app`. First, you create the `project01/acme-web-app` repository. Then, you include the name of the repository when you push the image, in the format `<region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>`. For example, `iad.ocir.io/ansh81vru1zp/project01/acme-web-app:4.6.3`.

Note that creating an empty repository in advance of pushing an image is almost certainly going to be your normal workflow. And if you're only authorized to manage repositories in compartments and not in the tenancy's root compartment, you'll always have to create a repository before pushing an image. However, if you're in the unusual position of mostly intending to push images to the root compartment, creating an empty repository in advance is not strictly necessary. For more information, see Notes about Repository Creation on page 3513.

### Terminology Summary

When working with repositories in Oracle Cloud Infrastructure Registry, you'll find it helpful to have a clear understanding of the following terms and how they relate to each other.

**Repository path**

A repository path (sometimes referred to as `<repo-path>` in this documentation) is the fully-qualified path to a repository in Oracle Cloud Infrastructure Registry. It has the following structure:

```
<region-key>.ocir.io/<tenancy-namespace>/<repo-name>
```

For example:

- `iad.ocir.io/ansh81vru1zp/project01/acme-web-app`
- `us-phoenix-1.ocir.io/cbujsx0t3wa3r/my-hello-app`

**Region key**

A region key (sometimes referred to as `<region-key>` in this documentation) identifies the Oracle Cloud Infrastructure Registry region you are using.

For example:

- `iad.ocir.io`
Registry

- us-phoenix-1.ocir.io

For the list of region keys, see Availability by Region on page 3508.

tenancy namespace

A tenancy namespace (sometimes referred to as `<tenancy-namespace>` in this documentation) is an auto-generated, random, and immutable string of alphanumeric characters. For example, the namespace of the acme-dev tenancy might be ansh81vru1zp.

Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lowercase letters (for example, acme-dev). To find out the tenancy namespace of the current tenancy, open the Profile menu (<tenancy-namespace>) and click Tenancy: The tenancy namespace is shown in the Object Storage Namespace field.

repository name

A repository name (sometimes referred to as `<repo-name>` in this documentation) is the name of a repository in Oracle Cloud Infrastructure Registry, to and from which you can push and pull images. Repository names can include one or more slash characters, and are unique across all compartments in the entire tenancy.

For example:

- project01/acme-web-app
- project01/my-test-app
- my-hello-app
- project01/acme-web-app/component1
- project01/acme-web-app/component2
- project01/acme-web-app/component1/subcomponent1

Note that although a repository name can include slash characters, the slash does not represent a hierarchical directory structure. It is simply one character in a string of characters. As a convenience, you might choose to start the names of several different repositories with the same string, perhaps ending in a slash (such as project01/). Such a string is sometimes called a 'repository name prefix'. But a repository named project01/acme-web-app need not have any relationship with a repository named project01/my-test-app. Using the same repository name prefix for some repositories simply makes it easier to organize and control access to them in Oracle Cloud Infrastructure Registry, which can contain many other repositories.

registry identifier

A registry identifier is an Oracle Cloud Infrastructure Registry region key and a tenancy namespace. It has the following structure:

```text
<region-key>.ocir.io/<tenancy-namespace>
```

For example:

- iad.ocir.io/ansh81vru1zp
- us-phoenix-1.ocir.io/cbujsx0t3wa3r

image path

An image path is the fully-qualified path to a particular image in a registry. It extends the repository path by adding the tag associated with the image. It has the structure:

```text
<region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>
```

For example:

- iad.ocir.io/ansh81vru1zp/project01/acme-web-app:version2.0.test
• us-phoenix-1.ocir.io/cbuwx0t3wa3r/my-hello-app:latest

tag

A tag or image tag (sometimes referred to as \texttt{<tag>} in this documentation) is a string used to refer to a particular image in a known repository. For example:

• 4.6.3
• 4.6.4
• version2.0.test

image name

The term 'image name' is sometimes used as a short-hand way to refer to a particular image in a particular repository. In this context, an image name has the structure:

\texttt{<repo-name>:<tag>}

For example:

• project01/acme-web-app:4.6.3
• project01/acme-web-app:4.6.4
• my-hello-app:latest

Creating a Repository

Using Oracle Cloud Infrastructure Registry, you can create an empty repository in a compartment and give it a name that's unique across all compartments in the entire tenancy.

Having created the new repository, you can push an image to the repository using the Docker CLI (see Pushing Images Using the Docker CLI on page 3513). Any images you subsequently push to the registry that include the same repository name are grouped into that repository.

Note that creating an empty repository in advance of pushing an image is almost certainly going to be your normal workflow. And if you're only authorized to manage repositories in compartments and not in the tenancy's root compartment, you'll always have to create a repository before pushing an image. However, if you're in the unusual position of mostly intending to push images to the root compartment, creating an empty repository in advance is not strictly necessary. For more information, see Notes about Repository Creation on page 3513.

Using the Console

To create a repository in Oracle Cloud Infrastructure Registry:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the region in which to create the repository.
3. Choose a Compartment you have permission to work in.
4. Click Create Repository.
5. In the Create Repository dialog box, specify details for the new repository:

   • **Compartment**: The compartment in which to create the new repository. The default compartment is the one you selected previously, but you can select any compartment that you have permission to work in.

   • **Repository Name**: A name of your choice for the new repository. The name you enter must be unique across all compartments in the entire tenancy. Avoid entering confidential information.

   • **Public**: Whether the new repository will be a public repository or a private repository. You can only make the new repository public if you belong to the tenancy’s Administrators group or have been granted the REPOSITORY_MANAGE permission. If you make the new repository public, any user with internet access and knowledge of the appropriate URL will be able to pull images from the repository. If you make the repository private, you (along with users belonging to the tenancy's Administrators group) will be able to perform any operation on the repository.
6. Click **Create Repository**.

7. (Optional) If you want to automatically create new private repositories in the tenancy’s root compartment when docker push commands don't include the name of an existing repository:

   a. Click **Settings**, and then select **General**.

   b. Select **Create repositories on first push in root compartment** to automatically create a new private repository in the tenancy's root compartment if the repository referenced in a docker push command doesn't already exist.

For more information about creating a new repository if the repository referenced in a docker push command doesn't already exist, see **Notes about Repository Creation** on page 3513.

### Using the CLI

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192. For a complete list of flags and options available for CLI commands, see the **Command Line Reference**.

#### To create a repository

```
oci artifacts container repository create --display-name <repo-name> --compartment-id <compartment_ocid>
```

For example:

```
oci artifacts container repository create --display-name project01/acme-web-app --compartment-id ocid1.compartment.oc1..aaaaaaaarvdfa72n...
```

### Using the API

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the **CreateContainerRepository** operation to create a repository.

### Notes about Repository Creation

Creating an empty repository in advance of pushing an image is almost certainly going to be your normal workflow. And if you're only authorized to manage repositories in compartments and not in the tenancy's root compartment, you'll always have to create a repository before pushing an image. However, if you're in the unusual position of mostly intending to push images to the tenancy's root compartment, creating an empty repository in advance is not strictly necessary.

When you push an image, you normally use a command in the format `docker push <region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>`. However, if you select the **Create repositories on first push in root compartment** option and push an image with a command that includes the name of a repository that doesn't already exist, a new private repository is created automatically in the root compartment.

For example, if you enter a command like `docker push iad.ocir.io/ansh81vru1zp/project02/acme-web-app:7.5.2` and the `project02/acme-web-app` repository doesn't exist, a private repository called `project02/acme-web-app` is created automatically in the root compartment.

Note that you must belong to the tenancy's Administrators group or have been granted the **REPOSITORY_MANAGE** permission on the tenancy to create the new private repository in the tenancy's root compartment. See **Policies to Control Repository Access** on page 3527.

### Pushing Images Using the Docker CLI

You use the Docker CLI to push images to Oracle Cloud Infrastructure Registry.

To push an image, you first use the `docker tag` command to create a copy of the local source image as a new image (the new image is actually just a reference to the existing source image). As a name for the new image, you
Registry

specify the fully qualified path to the target location in Oracle Cloud Infrastructure Registry where you want to push the image, including the name of a repository.

For example, assume you have a local image named acme-web-app:latest (the image name comprising the repository name of acme-web-app, and the image tag of latest). Let's say you want to push this image to Oracle Cloud Infrastructure Registry into a repository called project01/acme-web-app with an image tag of version2.0.test, in the Ashburn region of the acme-dev tenancy. When you use the `docker tag` command, you'd name the new image with the fully qualified path to its destination, in the format `<region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>`. So in this case, you'd name the new image `iad.ocir.io/ansh81vru1zp/project01/acme-web-app:version2.0.test`. Subsequently, when you use the `docker push` command, the image's name ensures it is pushed to the correct destination.

Your permissions control the images you can push to Oracle Cloud Infrastructure Registry (see Policies to Control Repository Access on page 3527). You can push images to repositories you've created (see Creating a Repository on page 3512). You can also push images to repositories that the groups to which you belong have been granted access by appropriate identity policies. If you belong to the Administrators group, you can push images to any repository in the tenancy.

Note that the instructions in this topic assume that the repository to which you want to push images already exists. That will usually be the case, but need not always be so (see Notes about Repository Creation on page 3513).

To push images to Oracle Cloud Infrastructure Registry using the Docker CLI:

1. If you already have an auth token, go to the next step. Otherwise:
   a. In the top-right corner of the Console, open the Profile menu (.userdetails) and then click User Settings to view the details.
   b. On the Auth Tokens page, click Generate Token.
   c. Enter a friendly description for the auth token. Avoid entering confidential information.
   d. Click Generate Token. The new auth token is displayed.
   e. Copy the auth token immediately to a secure location from where you can retrieve it later, because you won’t see the auth token again in the Console.
   f. Close the Generate Token dialog.
2. In a terminal window on the client machine running Docker, log in to Oracle Cloud Infrastructure Registry by entering `docker login <region-key>.ocir.io`, where `<region-key>` corresponds to the key for the Oracle Cloud Infrastructure Registry region you’re using. For example, `docker login iad.ocir.io`. See Availability by Region on page 3508.
3. When prompted for a username, enter your username in the format `<tenancy-namespace>/jdoe@acme.com`. For example, `ansh81vru1zp/jdoe@acme.com`. If your tenancy is federated with Oracle Identity Cloud Service, use the format `<tenancy-namespace>/oracleidentitycloudservice/<username>`.
4. When prompted for a password, enter the auth token you copied earlier.
5. Locate the image on the client machine that you want to push:
   a. In a terminal window on your client machine, enter `docker images` to list the available images.

For example:

```
$ docker images
REPOSITORY       TAG          IMAGE ID       CREATED          SIZE
acme-web-app      latest       8e0506e14874  2 hours ago     162.6 MB
acme-web-app      version1.0   7d9495d03763  2 hours ago     162.6 MB
<none>            <none>       6ebd328f833d  5 hours ago     162.6 MB
hello-world       latest       80b84820d442  5 weeks ago     890 B
```
b. Find the local image on the client machine that you want to push to Oracle Cloud Infrastructure Registry.

In the output of the `docker images` command, look for the specific image that you want to push. You'll need to uniquely identify this image later, in one of the following ways:

- using its id
- using its image name (its repository name and image tag separated by a colon)

For example, on the client machine you might have an acme-web-app image. In the output of the `docker images` command, look for the specific acme-web-app image that you want to push. You can uniquely identify that particular image in one of the following ways:

- using its id (for example, 8e0506e14874)
- using its image name (its repository name and image tag separated by a colon, for example `acme-web-app:latest`)

c. Use the `docker tag` command to create a copy of the original image as a new image (the new image is actually just a reference to the existing original image). As a name (or tag) for the new image, you specify the fully qualified path to the target location in Oracle Cloud Registry where you want to push the image, by entering:

```
docker tag <image-identifier> <target-tag>
```

where:

- `<image-identifier>` uniquely identifies the original image, either using the image's id (for example, 8e0506e14874), or the image's name (its original repository name and image tag separated by a colon, for example `acme-web-app:latest`).
- `<target-tag>` is the fully qualified path to the target location in Oracle Cloud Infrastructure Registry where you want to push the image, in the format `<region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>` where:
  - `<region-key>` is the key for the Oracle Cloud Infrastructure Registry region you're using. For example, iad. See Availability by Region on page 3508.
  - `ocir.io` is the Oracle Cloud Infrastructure Registry name.
  - `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy that owns the repository to which you want to push the image (as shown on the Tenancy Information page). For example, the namespace of the acme-dev tenancy might be `ansh81vru1zp`. Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, `acme-dev`). Note also that your user must have access to the tenancy.
  - `<repo-name>` is the name of the target repository to which you want to push the image (for example, `project01/acme-web-app`). Note that you'll usually specify a repository that already exists, but that need not always be the case (see Notes about Repository Creation on page 3513).
  - `<tag>` is an image tag you want to give the image in Oracle Cloud Infrastructure Registry (for example, `version2.0.test`).

For example, combining the previous examples, you might enter:

```
docker tag 8e0506e14874 iad.ocir.io/ansh81vru1zp/project01/acme-web-app:version2.0.test
```

6. Confirm that the Docker image has been correctly tagged on the client machine by entering `docker images` and verifying that the list of images includes an image with the tag you specified.

For example:

```
$ docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
Oracle Cloud Infrastructure User Guide 3515
```
Push the Docker image from the client machine to Oracle Cloud Infrastructure Registry by entering:

```
docker push <target-tag>
```

where `<target-tag>` is in the format `<region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>` where:

- `<region-key>` is the key for the Oracle Cloud Infrastructure Registry region you're using. For example, `iad`. See Availability by Region on page 3508.
- `ocir.io` is the Oracle Cloud Infrastructure Registry name.
- `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy that owns the repository to which you want to push the image (as shown on the Tenancy Information page). For example, the namespace of the acme-dev tenancy might be `ansh81vru1zp`. Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, `acme-dev`). Note also that your user must have access to the tenancy.
- `<repo-name>` is the name of the target repository to which you want to push the image (for example, `project01/acme-web-app`). Note that you'll usually specify a repository that already exists, but that need not always be the case (see Notes about Repository Creation on page 3513).
- `<tag>` is an image tag you want to give the image in Oracle Cloud Infrastructure Registry (for example, `version2.0.test`).

For example:

```
docker push iad.ocir.io/ansh81vru1zp/project01/acme-web-app:version2.0.test
```

### Pulling Images Using the Docker CLI

You use the Docker CLI to pull images from Oracle Cloud Infrastructure Registry.

Your permissions control the images you can pull from Oracle Cloud Infrastructure Registry (see Policies to Control Repository Access on page 3527). You can pull images from repositories you've created, from public repositories, and from repositories that the groups to which you belong have been granted access by identity policies. If you belong to the Administrators group, you can pull images from any repository in the tenancy.

To pull images from Oracle Cloud Infrastructure Registry using the Docker CLI:

1. If you already have an auth token, go to the next step. Otherwise:

   a. In the top-right corner of the Console, open the Profile menu and then click User Settings to view the details.
   b. On the Auth Tokens page, click Generate Token.
   c. Enter a friendly description for the auth token. Avoid entering confidential information.
   d. Click Generate Token. The new auth token is displayed.
   e. Copy the auth token immediately to a secure location from where you can retrieve it later, because you won't see the auth token again in the Console.
   f. Close the Generate Token dialog.
2. In a terminal window on the client machine running Docker, log in to Oracle Cloud Infrastructure Registry by entering `docker login <region-key>.ocir.io`, where `<region-key>` corresponds to the key for the Oracle Cloud Infrastructure Registry region you're using. For example, `docker login iad.ocir.io`. See **Availability by Region** on page 3508.

3. When prompted for a username, enter your username in the format `<tenancy-namespace>/<username>`, where `<tenancy-namespace>` is the auto-generated Object Storage namespace string of your tenancy (as shown on the **Tenancy Information** page). For example, `ansh81vru1zp/jdoe@acme.com`. If your tenancy is federated with Oracle Identity Cloud Service, use the format `<tenancy-namespace>/oracleidentitycloudservice/<username>`.

4. When prompted for a password, enter the auth token you copied earlier.

5. Pull the Docker image from Oracle Cloud Infrastructure Registry to the client machine by entering:

```
docker pull <region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>
```

where:
- `<region-key>` is the key for the Oracle Cloud Infrastructure Registry region you're using. For example, `iad`. See **Availability by Region** on page 3508.
- `ocir.io` is the Oracle Cloud Infrastructure Registry name.
- `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy that owns the repository from which you want to pull the image (as shown on the **Tenancy Information** page). For example, the namespace of the acme-dev tenancy might be `ansh81vru1zp`. Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, `acme-dev`). Note also that your user must have access to the tenancy.
- `<repo-name>` is the name of a repository from which you want to pull the image (for example, `project01/acme-web-app`). Note that your user must have access to the repository (see **Repositories** on page 3509).
- `<tag>` is the tag of the image that you want to pull from Oracle Cloud Infrastructure Registry (for example, `version2.0.test`).

For example:

```
docker pull iad.ocir.io/ansh81vru1zp/project01/acme-web-app:version2.0.test
```

Note that if you don't specify a `<tag>` in the `docker pull` command, Docker pulls the image that has the latest tag.

6. Confirm that the image has been pulled from Oracle Cloud Infrastructure Registry by entering `docker images` and verifying that the list of images on the client machine now includes the image you just pulled.

For example:

```
$ docker images
REPOSITORY                                      TAG                 IMAGE ID          CREATED       SIZE
iad.ocir.io/ansh81vru1zp/project01/acme-web-app version2.0.test 8e0506e14874      1 minute ago  162.6 MB
acme-web-app                                    latest 8e0506e14874      2 hours ago   162.6 MB
acme-web-app                                    version1.0 7d9495d03763      2 hours ago   162.6 MB
<none>                                          <none> 6ebd328f833d      5 hours ago   162.6 MB
hello-world                                     latest 80b84820d442      5 weeks ago   890 B
```
Pulling Images from Registry during Kubernetes Deployment

During the deployment of an application to a Kubernetes cluster, you'll typically want one or more images to be pulled from a Docker registry. In the application's manifest file you specify the images to pull, the registry to pull them from, and the credentials to use when pulling the images. The manifest file is commonly also referred to as a pod spec, or as a deployment.yaml file (although other filenames are allowed).

If you want the application to pull images that reside in Oracle Cloud Infrastructure Registry, you have to perform two steps:

1. You have to use kubectl to create a Docker registry secret. The secret contains the Oracle Cloud Infrastructure credentials to use when pulling the image. When creating secrets, Oracle strongly recommends you use the latest version of kubectl (see the kubectl documentation).
2. You have to specify the image to pull from Oracle Cloud Infrastructure Registry, including the repository location and the Docker registry secret to use, in the application's manifest file.

To create a Docker registry secret:

1. If you haven't already done so, follow the steps to set up the cluster's kubeconfig configuration file and (if necessary) set the KUBECONFIG environment variable to point to the file. Note that you must set up your own kubeconfig file. You cannot access a cluster using a kubeconfig file that a different user set up. See Setting Up Cluster Access on page 876.
2. In a terminal window, enter:

```bash
kubectl create secret docker-registry <secret-name> --docker-server=<region-key>.ocir.io --docker-username='<tenancy-namespace>/<oci-username>' --docker-password='<oci-auth-token>' --docker-email='<email-address>
```

where:

- `<secret-name>` is a name of your choice, that you will use in the manifest file to refer to the secret. For example, ocirsecret
- `<region-key>` is the key for the Oracle Cloud Infrastructure Registry region you're using. For example, iad. See Availability by Region on page 3508.
- `ocir.io` is the Oracle Cloud Infrastructure Registry name.
- `<tenancy-namespace>` is the auto-generated Object Storage namespace string of the tenancy containing the repository from which the application is to pull the image (as shown on the Tenancy Information page). For example, the namespace of the acme-dev tenancy might be ansh81vrulzp. Note that for some older tenancies, the namespace string might be the same as the tenancy name in all lower-case letters (for example, acme-dev).
- `<oci-username>` is the username to use when pulling the image. The username must have access to the tenancy specified by `<tenancy-namespace>`. For example, jdoe@acme.com. If your tenancy is federated with Oracle Identity Cloud Service, use the format oracleidentitycloudservice/<oci-username>
- `<oci-auth-token>` is the auth token of the user specified by `<oci-username>`. For example, k\]j64r(1sJSSF-;)K8
- `<email-address>` is an email address. An email address is required, but it doesn't matter what you specify. For example, jdoe@acme.com

Note the use of single quotes around strings containing special characters.

For example, combining the previous examples, you might enter:

```bash
kubectl create secret docker-registry ocirsecret --docker-server=phx.ocir.io --docker-username='ansh81vrulzp/jdoe@acme.com' --docker-password='k\]j64r(1sJSSF-;)K8' --docker-email='jdoe@acme.com'
```

Having created the Docker secret, you can now refer to it in the application manifest file.
To specify the image to pull from Oracle Cloud Infrastructure Registry, along with the Docker secret to use, during deployment of an application to a cluster:

1. Open the application's manifest file in a text editor.
2. Add the following sections to the manifest file:
   a. Add a `containers` section that specifies the name and location of the container you want to pull from Oracle Cloud Infrastructure Registry, along with other deployment details.
   b. Add an `imagePullSecrets` section to the manifest file that specifies the name of the Docker secret you created to access the Oracle Cloud Infrastructure Registry.

Here's an example of what the manifest might look like when you've added the `containers` and `imagePullSecrets` sections:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: ngnix-image
spec:
  containers:
    - name: ngnix
      image: phx.ocir.io/ansh81vru1zp/project01/ngnix-lb:latest
      imagePullPolicy: Always
      ports:
        - name: nginx
          containerPort: 8080
          protocol: TCP
      imagePullSecrets:
        - name: ocirsecret
```

3. Save and close the manifest file.

### Viewing Images and Image Details

To make sure you pull the correct image or to identify images that you no longer need, you can find out detailed information about the images in Oracle Cloud Infrastructure Registry.

Your permissions control the images in Oracle Cloud Infrastructure Registry that you can view information about (see Policies to Control Repository Access on page 3527). You can view information about images in repositories you've created, and in repositories that the groups to which you belong have been granted access by identity policies. If you belong to the Administrators group, you can view information about images in any repository in the tenancy.

#### Using the Console

To view images and image details:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the registry's region.
3. Choose a Compartment you have permission to work in.
4. Click the name of the repository that contains the image you want to see detailed information about. You see all the different images in the repository, along with the tag of each image and when it was pushed to the registry. You can sort the different images by the date they were pushed or by their tag.
5. Click the image for which you want to see detailed information. The Summary page shows you the size of the image, when it was pushed and by which user, and the number of times the image has been pulled. Use the options on the Summary page as follows:
   - Display the Layers tab to see the SHA message digest of each layer in the selected image.
   - Display the Associated Tags tab to see the full path for the image with the tag you select. Note that if you select a different tag, the summary details change accordingly.
6. (Optional) If you want to pull an image, select **Copy Pull Command** from the **Actions** menu button. The command you copy includes the fully qualified path to the image's location in Oracle Cloud Infrastructure Registry, in the format `<region-key>.ocir.io/<tenancy-namespace>/<repo-name>:<tag>`. For example, `docker pull iad.ocir.io/ansh81vru1zp/project01/acme-web-app:version2.0.test`. See **Pulling Images Using the Docker CLI** on page 3516.

**Using the CLI**

For information about using the CLI, see **Command Line Interface (CLI)** on page 4192. For a complete list of flags and options available for CLI commands, see the **Command Line Reference**.

To view details of an image

```
oci artifacts container image get --image-id <image-ocid>
```

For example:

```
oci artifacts container image get --image-id
ocid1.containerimage.oc1.phx.0.ansh81vru1zp.aaaaaaaalqzjyks...
```

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225. Use the **ListContainerImages** and **GetContainerImage** operations to see image details.

**Deleting and Undeleting an Image**

When you no longer need an old image or you simply want to clean up the list of image tags in a repository, you can delete images from Oracle Cloud Infrastructure Registry.

Your permissions control the images in Oracle Cloud Infrastructure Registry that you can delete (see **Policies to Control Repository Access** on page 3527). You can delete images from repositories you've created, and from repositories that the groups to which you belong have been granted access by identity policies. If you belong to the Administrators group, you can delete images from any repository in the tenancy.

You can undelete an image you've previously deleted, for up to 48 hours after you deleted it. After that time, the image is permanently removed from Oracle Cloud Infrastructure Registry. You use the Oracle Cloud Infrastructure REST API and CLI to undelete images.

In addition to deleting individual images as described below, you can set up image retention policies to delete images automatically based on selection criteria you specify (see **Retaining and Deleting Images Using Retention Policies** on page 3522).

Note that when you delete an image, it can take up to 48 hours for the deletion to take effect and for storage to actually be released. If you are deleting images to release storage, remember that you can also **Contact Us** to obtain more storage.

**Using the Console**

To delete an image from Oracle Cloud Infrastructure Registry:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Container Registry**.
2. Choose the registry's region.
3. Choose a **Compartment** you have permission to work in.
4. Click the name of the repository from which to delete the image.
5. Click the name of the image that you want to delete.
6. Select **Delete Image** from the **Actions** menu and confirm that you want to delete the image.
You can undelete an image you've previously deleted, for up to 48 hours after you deleted it. After that time, the image is permanently removed from Oracle Cloud Infrastructure Registry.

**Using the CLI**

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**To delete an image**

```
oci artifacts container image delete --image-id <image-ocid>
```

For example:

```
oci artifacts container image delete --image-id
ocid1.containerimage.oc1.phx.0.ansh81vrulzp.aaaaaaaaalqzjyks...
```

**To undelete an image**

```
oci artifacts container image restore --image-id <image-ocid>
```

For example:

```
oci artifacts container image restore --image-id
ocid1.containerimage.oc1.phx.0.ansh81vrulzp.aaaaaaaaalqzjyks...
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the DeleteContainerImage operation to delete an image.

Use the RestoreContainerImage operation to undelete an image you've previously deleted.

**Untagging Images**

When you want to clean up the list of images in a repository without actually deleting images, you can remove the tags from images in Oracle Cloud Infrastructure Registry (known as 'untagging').

Your permissions control the images in Oracle Cloud Infrastructure Registry that you can untag (see Policies to Control Repository Access on page 3527). You can untag images in repositories you've created, and images in repositories that the groups to which you belong have been granted access by identity policies. If you belong to the Administrators group, you can untag images in any repository in the tenancy.

**Using the Console**

To untag an image in Oracle Cloud Infrastructure Registry:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the registry's region.
3. Choose a Compartment you have permission to work in.
4. Click the name of the repository containing the image you want to untag.
5. Click the name of the image that you want to untag.
6. Click the tag that you want to remove, select Remove tag from the Actions menu, and confirm that you want to remove the tag.
Tip:
To view the untagged images in a repository, click the name of the repository and then select Untagged under Image Filter.

Using the CLI
For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

To untag an image

```bash
oci artifacts container image remove-version --image-id <image-ocid> --image-version <version>
```

For example:

```bash
oci artifacts container image remove-version --image-id ocid1.containerimage.oc1.phx.0.ansh81vrulzp.aaaaaaalqzjyks... --image-version 1.0
```

Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the RemoveContainerVersion operation to untag an image.

Retaining and Deleting Images Using Retention Policies
You can set up image retention policies to automatically delete images that meet particular selection criteria, namely:

- images that have not been pulled for a certain number of days
- images that have not been tagged for a certain number of days
- images that have not been given particular Docker tags specified as exempt from automatic deletion

An hourly process checks images against the selection criteria, and any that meet the selection criteria are automatically deleted.

You'll often find image retention policies are a more convenient way to manage the images in a repository than manually deleting individual images (see Deleting and Undeleting an Image on page 3520).

In each region in a tenancy, there's a global image retention policy. The global image retention policy's default selection criteria retain all images, so that no images are automatically deleted. However, you can change the global image retention policy so that images are deleted if they meet the criteria you specify. A region's global image retention policy applies to all repositories in the region, unless it is explicitly overridden by one or more custom image retention policies.

You can set up custom image retention policies to override the global image retention policy with different criteria for specific repositories in a region. Having created a custom image retention policy, you apply the custom retention policy to a repository by adding the repository to the policy. The global image retention policy no longer applies to repositories that you add to a custom retention policy.

If you have manage permission on the tenancy, you can:

- modify each region's own global image retention policy
- create new custom image retention policies
- modify the criteria of existing custom image retention policies
- delete custom image retention policies

If you have manage permission on a repository, you can:
• add the repository to a custom image retention policy
• remove the repository from a custom image retention policy

Note the following:
• Only one custom image retention policy at a time can apply to a repository. If a repository has already been added to a custom retention policy and you want to add the repository to a different custom retention policy, you have to remove the policy from the first retention policy before adding it to the second.
• When you create or update an image retention policy, the hourly process that checks images for deletion will ignore the new or updated policy for several hours. This cooling-off period enables you to refine the policy criteria to select only the images you want to delete, and thus reduces the chance of images being deleted unexpectedly. After this period, the policy is included in the hourly process and images are checked and deleted accordingly.
• The global image retention policy (and any custom image retention policies you create) are specific to a particular region. To delete images consistently in different regions in your tenancy, set up image retention policies in each region with identical selection criteria.
• When you delete an image, it can take up to 48 hours for the deletion to take effect and for storage to actually be released. If you are deleting images to release storage, remember that you can also Contact Us to obtain more storage.

Using the Console to Edit the Global Image Retention Policy

Provided you have manage permission on the tenancy, you can edit the region’s global image retention policy that applies to all repositories in a region (except for repositories that have been explicitly added to a custom image retention policy).

To edit the global image retention policy:
1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the registry’s region.
3. Click Settings, and then select Image retention policies.
   You see the current selection criteria of the region’s global image retention policy, along with any custom image retention policies that override the global image retention policy for specific repositories.
4. Click Edit Global Policy.
5. In the Global Image Retention Policy dialog, specify new criteria for the global retention policy:
   • Delete any images that haven't been pulled in n days: Select this option if you want to delete images that have not been pulled for the number of days you specify.
   • Delete any images that haven't been tagged in n days: Select this option if you want to delete images that have not been tagged for the number of days you specify.
   • Exempt Tags: If you want to prevent images from being deleted on the basis of Docker tags they’ve been given, specify those tags as exempt in a comma-separated list. An image that has been given one of the exempt tags will not be deleted, even if the image meets the other criteria. You can include the asterisk (*) as a wildcard to represent none, one, or more characters. For example, you might specify latest,prod-*,*-tail,*.100.*.
6. Click Save Settings.

Going forward, the criteria you entered for the region’s global image retention policy will apply to all repositories in the region, except for repositories that have been explicitly added to a custom image retention policy. Images in repositories that have not been added to a custom image retention policy will be deleted from Oracle Cloud Infrastructure Registry if they meet the criteria you specified in the global image retention policy.

When you create or update an image retention policy, the hourly process that checks images for deletion will ignore the new or updated policy for several hours. This cooling-off period enables you to refine the policy criteria to select only the images you want to delete, and thus reduces the chance of images being deleted unexpectedly. After this period, the policy is included in the hourly process and images are checked and deleted accordingly.
Using the Console to Create a New Custom Image Retention Policy to Override the Global Policy

Provided you have manage permission on the tenancy, you can create a new custom image retention policy to override the region's global image retention policy for the repositories you specify. A custom image retention policy is specific to the region in which you create it.

To create a new custom image retention policy:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the registry's region.
3. Click Settings, and then select Image retention policies.
   
   You see the current selection criteria of the region's global image retention policy, along with any existing custom image retention policies that override the global image retention policy for specific repositories.
4. Click Create Policy.
5. In the Create Repository Image Retention Policy dialog, specify criteria for the new retention policy:
   
   • Policy Name: A name of your choice for the policy. Avoid entering confidential information.
   • Delete any images that haven't been pulled in $n$ days: Select this option if you want to delete images that have not been pulled for the number of days you specify.
   • Delete any images that haven't been tagged in $n$ days: Select this option if you want to delete images that have not been tagged for the number of days you specify.
   • Exempt Tags: If you want to prevent images from being deleted on the basis of Docker tags they’ve been given, specify those tags as exempt in a comma-separated list. An image that has been given one of the exempt tags will not be deleted, even if the image meets the other criteria. You can include the asterisk (*) as a wildcard to represent none, one, or more characters. For example, you might specify latest,prod-*,*-.100.*.
6. Click Save Settings.

You can now add repositories to the new custom retention policy.

Using the Console to Remove a Repository from a Custom Image Retention Policy

Provided you have manage permission on a repository, you can remove a repository from a custom image retention policy to which it was previously added.

You might want to remove the repository from a custom image retention policy:

• if you want the region's global image retention policy to apply to the repository
• if you want a different custom image retention policy to apply to the repository (only one custom image retention policy at a time can apply to a repository)

To remove a repository from a custom image retention policy:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the registry's region.
3. Click Settings, and then select Image retention policies.
   
   You see the current selection criteria of the region's global image retention policy, along with any existing custom image retention policies that override the global image retention policy for specific repositories.
4. Locate the custom image retention policy to which the repository has been added.
5. Click the delete icon beside the repository name to remove it from the custom image retention policy.

Going forward, the region's global image retention policy will apply to the repository (unless you add the repository to a different custom image retention policy). The images in the repository will be deleted from Oracle Cloud Infrastructure Registry if they meet the criteria specified in the global image retention policy.
When you create or update an image retention policy, the hourly process that checks images for deletion will ignore the new or updated policy for several hours. This cooling-off period enables you to refine the policy criteria to select only the images you want to delete, and thus reduces the chance of images being deleted unexpectedly. After this period, the policy is included in the hourly process and images are checked and deleted accordingly.

**Using the Console to Add a Repository to a Custom Image Retention Policy**

Provided you have manage permission on a repository, you can add a repository to an existing custom image retention policy.

Note that if a custom image retention policy already applies to the repository, you'll have to remove the repository from the current policy before adding it to a different policy. Note also that a custom image retention policy is specific to the region in which it was created.

To add a repository to an existing custom image retention policy:

1. In the Console, open the navigation menu. Under Solutions and Platform, go to Developer Services and click Container Registry.
2. Choose the registry's region.
3. Click Settings, and then select Image retention policies.

   You see the current selection criteria of the region's global image retention policy, along with the custom image retention policies that have been defined to override the global image retention policy for specific repositories.

4. Locate the custom image retention policy to which you want to add the repository.
5. Click Add Repository and select from the list the repository you want to add to the custom image retention policy.

   Note that the repository list includes all repositories in the region, regardless of whether you have permission to add them to a retention policy. You can only add a repository to a retention policy if you have manage permission on that repository.

   If a repository in the list has a policy name beside it, the repository has already been added to a policy. Before you can add the repository to a different policy, you'll have to remove it from the first policy.

Going forward, the custom retention policy to which you added the repository will override the region's global image retention policy. The images in the repository will be deleted from Oracle Cloud Infrastructure Registry if they meet the criteria specified in the custom retention policy.

When you create or update an image retention policy, the hourly process that checks images for deletion will ignore the new or updated policy for several hours. This cooling-off period enables you to refine the policy criteria to select only the images you want to delete, and thus reduces the chance of images being deleted unexpectedly. After this period, the policy is included in the hourly process and images are checked and deleted accordingly.

**Deleting a Repository**

There is a limit to the number of repositories you can have in any given region in a tenancy. So when you no longer need a repository, it makes sense to delete it from Oracle Cloud Infrastructure Registry.

Your permissions control the repositories in Oracle Cloud Infrastructure Registry that you can delete (see Policies to Control Repository Access on page 3527). You can delete repositories you've created, and repositories that the groups to which you belong have been granted access by identity policies. If you belong to the Administrators group, you can delete any repository in the tenancy.

Note that when you delete a repository, it can take up to 48 hours for the deletion to take effect and for storage to actually be released. If you are deleting repositories to release storage, remember that you can also Contact Us to obtain more storage.
Using the Console

To delete a repository from Oracle Cloud Infrastructure Registry:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Container Registry**.
2. Choose the registry's region.
3. Choose a **Compartment** you have permission to work in.
4. Click the name of the repository that you want to delete.
5. Select **Delete Repository** from the **Actions** menu and confirm that you want to delete the repository.

The repository is permanently removed from Oracle Cloud Infrastructure Registry.

Using the CLI

For information about using the CLI, see [Command Line Interface (CLI)](page 4192). For a complete list of flags and options available for CLI commands, see the [Command Line Reference](page 4225).

To delete a repository

```
oci artifacts container repository delete --repository-id <repository-ocid>
```

For example:

```
oci artifacts container repository delete --repository-id ocid1.containerrepo.oc1.us-phoenix-1.0.ansh81vrulzp.aaaaaaaswec83o...
```

Using the API

For information about using the API and signing requests, see [REST APIs](page 4368) and [Security Credentials](page 179). For information about SDKs, see [Software Development Kits and Command Line Interface](page 4225).

Use the **DeleteContainerRepository** operation to delete a repository.

Moving Repositories Between Compartments

When you create a new repository in Oracle Cloud Infrastructure Registry, you specify the compartment in which to create it. Having created the repository in one compartment, you can subsequently move it to a different compartment. For example, to change the users who are authorized to use the repository, or to change how billing for a repository is charged.

Only users with appropriate permissions can access the repository in the compartment that you move it to.

Your permissions control the repositories in Oracle Cloud Infrastructure Registry that you can move, and the compartments that you can move them to (see [Policies to Control Repository Access](page 3527)). You can move repositories you've created (as well as repositories that the groups to which you belong have been granted access by identity policies) to any compartment to which you have access. If you belong to the Administrators group, you can move any repository in the tenancy to any compartment.

Using the Console

To move a repository in Oracle Cloud Infrastructure Registry from one compartment to another:

1. In the Console, open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Container Registry**.
2. Choose the registry's region.
3. Choose a **Compartment** you have permission to work in.
4. Click the name of the repository that you want to move.
5. Select **Move Compartment** from the **Actions** menu.
6. Select the compartment to which you want to move the repository.
7. Click **Submit** to move the repository.

The repository is moved to the compartment you selected.

Only users with appropriate permissions can now access the repository in the compartment that you’ve moved it to.

**Using the CLI**

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**To move a repository**

```
oci artifacts container repository change-compartment --compartment-id <compartment_ocid_new> --repository-id <repository_ocid>
```

For example:

```
oci artifacts container repository change-compartment --compartment-id ocid1.compartment.oc1..aaaaaaaaswegb83o... --repository-id ocid1.containerrepo.oc1.us-phoenix-1.0.ansh81vrulzp.aaaaaaatxfd94p...
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the ChangeContainerRepositoryCompartment operation to move a repository to a different compartment.

**Getting an Auth Token**

Before you can push and pull Docker images to and from Oracle Cloud Infrastructure Registry, you must already have an Oracle Cloud Infrastructure username and an auth token. If you haven't got an auth token, or you've forgotten it, or you're not sure, you can create a new auth token. You only see the auth token string when you create it, so be sure to copy the auth token to a secure location immediately.

**Tip:**

Each user can have up to two auth tokens at a time. So if you do lose or forget the auth token, you can always create a second auth token.

To create a new auth token:

1. In the top-right corner of the Console, open the **Profile** menu (👤) and then click **User Settings** to view the details.
2. On the **Auth Tokens** page, click **Generate Token**.
3. Enter a friendly description for the auth token. Avoid entering confidential information.
4. Click **Generate Token**. The new auth token is displayed.
5. Copy the auth token immediately to a secure location from where you can retrieve it later, because you won't see the auth token again in the Console.
6. Close the Generate Token dialog.

**Policies to Control Repository Access**

You have fine-grained control over the operations that users are allowed to perform on repositories in Oracle Cloud Infrastructure Registry.

A user's permissions to access repositories comes from the groups to which they belong. The permissions for a group are defined by identity policies. Policies define which actions the members of a group can perform. Users access repositories and perform operations based on the policies set for the groups they are members of. Identity policies
to control repository access can be set at the tenancy and at the compartment level. See Details for Registry on page 2335.

Before you can control access to repositories, you must have already created users and already placed them in appropriate groups (see Managing Users on page 2414 and Managing Groups on page 2419). You can then create policies and policy statements to control repository access (see Managing Policies on page 2450).

Note that users in the tenancy’s Administrators group can perform any operation on any repository in Oracle Cloud Infrastructure Registry that belongs to the tenancy.

**Common Policies**

**Note:**

The policies in this section use example group names, as follows:

- acme-viewers: A group that you want to limit to just viewing a list of repositories.
- acme-pullers: A group that you want to limit to pulling images.
- acme-pushers: A group that you want to allow to push and pull images.
- acme-managers: A group that you want to allow to push and pull images, delete repositories, and edit repository metadata (for example, to make a private repository public).

Make sure to replace the example group names with your own group names.

**Enable users to view a list of all the repositories belonging to the tenancy or to a compartment**

**Type of access:** Ability to see a list of all repositories in Oracle Cloud Infrastructure Registry belonging to the tenancy (or to a particular compartment). Users will not be able to:

- view the images or layers in a repository
- push or pull images from or to a repository

**Where to create the policy:**

- In the tenancy. For example:
  
  Allow group acme-viewers to inspect repos in tenancy

- In the tenancy or in a compartment. For example:
  
  Allow group acme-viewers to inspect repos in compartment acme-compartment

**Enable users to pull images from any repository belonging to the tenancy or to a compartment**

**Type of access:** Ability to pull images (layers and manifests) from any repository in Oracle Cloud Infrastructure Registry that belongs to the tenancy (or to a particular compartment).

**Where to create the policy:**

- In the tenancy. For example:
  
  Allow group acme-pullers to read repos in tenancy

- In the tenancy or in a compartment. For example:
  
  Allow group acme-pullers to read repos in compartment acme-compartment

**Enable users to pull images from specific repositories in the tenancy or in a compartment**

**Type of access:** Ability to pull images (layers and manifests) from any repository in Oracle Cloud Infrastructure Registry that has a name starting with "acme-web-app" and that belongs to the tenancy (or that belongs to a particular compartment).
Where to create the policy:

- In the tenancy. For example:

```plaintext
Allow group acme-pullers to read repos in tenancy where all
   { target.repo.name=/acme-web-app*/ }
```

- In the tenancy or in a compartment. For example:

```plaintext
Allow group acme-pullers to read repos in compartment acme-compartment
   where all { target.repo.name=/acme-web-app*/ }
```

Enable users to push images to any repositories (and create new repositories if necessary) in the tenancy or in a compartment

Type of access: Ability to push images (layers and manifests) to any repository in Oracle Cloud Infrastructure Registry that belongs to the tenancy or to a particular compartment.

If the specified repository doesn't exist yet, the REPOSITORY_CREATE permission ensures users are able to create a new repository in the tenancy's root compartment when they push the image. For more information about this unusual scenario, see Notes about Repository Creation on page 3513.

Where to create the policy:

- In the tenancy. For example:

```plaintext
Allow group acme-pushers to use repos in tenancy
```

```plaintext
Allow group acme-pushers to manage repos in tenancy where ANY
   {request.permission = 'REPOSITORY_CREATE', request.permission =
    'REPOSITORY_UPDATE'}
```

- In the tenancy or in a compartment. For example, in a compartment:

```plaintext
Allow group acme-pushers to use repos in compartment acme-compartment
```

Note that if you create the policy in a compartment other than the root compartment as shown above, users cannot push an image to a repository that doesn't exist yet. That's because the above policy does not give users permission to create a new repository in the tenancy's root compartment. For more information about this unusual scenario, see Notes about Repository Creation on page 3513.

Enable managers to perform any operation on any repository belonging to the tenancy or to a compartment

Type of access: Ability to perform any operation on any repository in Oracle Cloud Infrastructure Registry that belongs to the tenancy (or to a particular compartment), including:

- Pull an image from any repository.
- Push an image to any repository.
- Create a new repository. That is, either to create an empty repository in any compartment, or to create a repository in the tenancy's root compartment when pushing an image for which no repository exists yet. Note that if you create the policy in a compartment other than the root compartment, users cannot push an image to a repository that doesn't exist yet. That's because the policy does not give users permission to create a new repository in the root compartment. For more information about this unusual scenario, see Notes about Repository Creation on page 3513.
- Delete a repository.
- Change a public repository to a private repository, or a private repository to a public repository.

Where to create the policy:
• In the tenancy. For example:

```
Allow group acme-managers to manage repos in tenancy
```

• In the tenancy or in a compartment. For example:

```
Allow group acme-managers to manage repos in compartment acme-compartment
```

Note that if you create the above policy in a compartment other than the root compartment, users cannot push an image to a repository that doesn't exist yet. That's because the policy does not give users permission to create a new repository in the root compartment. For more information about this unusual scenario, see Notes about Repository Creation on page 3513.
Chapter 30

Resource Manager

This chapter introduces the Oracle Resource Manager service and describes how to use it.

Features

Templates

A template is a Terraform configuration that you can use to manage infrastructure. Templates can help those new to infrastructure as code and those who are updating production workflow configurations. Use templates to try out Resource Manager and to apply proven best practices to your production workflow configuration. For information about Oracle-provided templates, see Templates on page 3588.

Create your own private templates to share with others in the tenancy.
Start with a Resource Creation Page

Save your configuration from a resource configuration page to a stack. Use the stack to install, configure, and manage the resource through the "infrastructure-as-code" model. Supported resource configuration pages: Create Compute Instance.

CI/CD with Resource Manager

Remotely store your Terraform configurations using integrated source code control systems, such as GitHub and GitLab. This integration helps you achieve continuous integration and continuous delivery (CI/CD).

For more information about remotely storing your configurations, see Managing Configuration Source Providers on page 3581.

Resource Discovery

A feature to capture deployed resources as Terraform configuration and state files. With this feature, you can:

- Move from manually managed infrastructure to Resource Manager-controlled infrastructure.
- Learn how Terraform uses HashiCorp Configuration Language (HCL) syntax to represent Oracle Cloud Infrastructure resources.
- Duplicate or rebuild existing infrastructure in another compartment.

For more information, see resource discovery and the following instructions:

- To see how Terraform represents your resources on page 3560
- To recreate (clone) existing infrastructure in another compartment on page 3560

Drift Detection

Find out if provisioned resources have different states than those resources defined in the stack's last executed configuration and view detailed drift status for each resource.

You can optionally limit the drift detection to specified resources. Each resource is identified by a resource address, which is a string derived from the resource type and name specified in the stack's Terraform configuration plus an optional index. For example, the resource address for the fourth Compute instance with the name "test_instance" is oci_core_instance.test_instance[3] (resource type of oci_core_instance, a period as delimiter, resource name of test_instance, and index of 3 in brackets). For more details and examples of resource addresses, see the Terraform documentation at https://www.terraform.io/docs/internals/resource-addressing.html#examples.

For more information about drift detection, see drift and the following instructions:

- To detect drift for a stack or selected resources on page 3562
- To view the latest drift detection report on page 3562
- To view an old drift detection report on page 3563

Deploy to Oracle Cloud Button

The Deploy to Oracle Cloud button allows you to launch your remote Terraform configuration using the Create Stack workflow available in Resource Manager.

For more information, see Using the Deploy to Oracle Cloud Button on page 3592.
Overview of Resource Manager

Resource Manager is an Oracle Cloud Infrastructure service that allows you to automate the process of provisioning your Oracle Cloud Infrastructure resources. Using Terraform, Resource Manager helps you install, configure, and manage resources through the “infrastructure-as-code” model.

A Terraform configuration codifies your infrastructure in declarative configuration files. Resource Manager allows you to share and manage infrastructure configurations and state files across multiple teams and platforms. This infrastructure management can’t be done with local Terraform installations and Oracle Terraform modules alone. For more information about the Oracle Cloud Infrastructure Terraform provider, see Terraform Provider on page 4275. For a general introduction to Terraform and the "infrastructure-as-code" model, see https://www.terraform.io.

Key Concepts

Following are brief descriptions of key concepts and the main components of Resource Manager.

configuration

Information to codify your infrastructure. A Terraform configuration can be either a template or a set of one or more files that you write. You can either upload your written configuration directly or store it in a source code control system.

Use your configuration to specify the Oracle Cloud Infrastructure resources in a given stack. For example, specify resource metadata, data source definitions, and variable declarations. Each Terraform configuration file is either HashiCorp Configuration Language (HCL) format or JSON format, as indicated by the file’s extension (either .tf or .tf.json, respectively).

For example configurations, see Terraform provider examples and Templates on page 3588. For more information, see Terraform Configurations for Resource Manager on page 3594 and Authoring Configurations on page 4277; see also Hashicorp: Configuration.

configuration source provider

Connection information to a source code control system where your Terraform configuration files are stored. Use a configuration source provider to create a stack from a remote, versioned Terraform configuration file. A configuration source provider has the following types:

• GitHub: Supported products
  • GitHub Enterprise
  • GitHub Enterprise Server
  • GitHub Enterprise Cloud
  • GitHub Free for organizations
  • GitHub Free for user accounts
  • GitHub Team
• GitLab: Supported products
  • GitLab Community Edition
  • GitLab Enterprise Edition
  • GitLab.com

A configuration source provider has the following lifecycle states:

• Active: The configuration source provider is available for use.

For more information, see Managing Configuration Source Providers on page 3581 and To create a stack on page 3557.

drift

Difference between the actual, real-world state of your infrastructure, and the stack’s last executed configuration. For example, drift occurs when a team member adds a production tag to your resources, or when a resource fails. You can run drift detection reports to determine if provisioned resources have different
states than those resources defined in the stack's last executed configuration. You can also view detailed drift status for each resource.

job

Instructions to perform the actions defined in your configuration. Only one job at a time can run on a given stack; further, you can have only one set of Oracle Cloud Infrastructure resources on a given stack. To provision a different set of resources, you must create a separate stack and use a different configuration.

Resource Manager provides the following job types:

- **Plan**: Parses your Terraform configuration and creates an execution plan for the associated stack. The execution plan lists the sequence of specific actions planned to provision your Oracle Cloud Infrastructure resources. The execution plan is handed off to the apply job, which then executes the instructions.
- **Apply**: Applies the execution plan to the associated stack to create (or modify) your Oracle Cloud Infrastructure resources. Depending on the number and type of resources specified, a given apply job can take some time. You can check status while the job runs.
- **Destroy**: Releases resources associated with a stack. Released resources are not deleted. For example, terminates a Compute instance controlled by a stack. The stack's job history and state remain after running a destroy job. You can monitor the status and review the results of a destroy job by inspecting the stack's log files.
- **Import State**: Sets the provided Terraform state file as the current state of the stack. Use this job to migrate local Terraform environments to Resource Manager.

Jobs store history about their associated stack. For example, plan jobs store generated execution plans and apply jobs store configurations (snapshots) and state files. Jobs reside in the same compartment as the stack they are associated with. An OCI ID is assigned to each job.

A job has the following lifecycle states:

- **Accepted**: The job was accepted for processing.
- **In Progress**: The job is currently executing.
- **Failed**: The job did not complete execution.
- **Succeeded**: The job completed execution.
- **Canceling**: The job is being canceled.
- **Canceled**: The job was canceled.

module

A group of related resources. Use modules to create lightweight and reusable abstractions, so that you can describe your infrastructure in terms of its architecture. For more information, see Creating Modules.

package

Typically a .zip file to a Terraform configuration that is stored in a supported provider, such as GitHub. For more information, see Using the Deploy to Oracle Cloud Button on page 3592.

resource discovery

A feature to capture deployed resources as Terraform configuration and state files. With this feature, you can:

- Move from manually managed infrastructure to Resource Manager-controlled infrastructure.
- Learn how Terraform uses HashiCorp Configuration Language (HCL) syntax to represent Oracle Cloud Infrastructure resources.
- Duplicate or rebuild existing infrastructure in another compartment.

Resource discovery supports the following Oracle Cloud Infrastructure resources: https://www.terraform.io/docs/providers/oci/guides/resource_discovery.html#supported-resources.

To discover resources, use Resource Manager to create a stack from your compartment. The created stack includes a generated Terraform configuration and state file corresponding to the supported resources in the source compartment.
Resource Manager

Note:
Attributes are missing from some supported resources captured using resource discovery. For more information, see https://docs.cloud.oracle.com/iaas/Content/knownissues.htm#orm-attributes.

Details about undiscoverable attributes

In some cases, a required or optional attribute may not be discoverable from the Oracle Cloud Infrastructure services and may be omitted from the generated Terraform configuration. This omission may be expected behavior from the service, which may prevent discovery of certain sensitive attributes or secrets. In such cases, a placeholder value is set along with a comment like this:

```text
admin_password = "<placeholder for missing required attribute>"
#Required attribute not found in discovery, placeholder value set to avoid plan failure
```

The missing required attributes are also added to lifecycle ignore_changes. This addition is done to avoid Terraform plan failure when moving manually managed infrastructure to Terraform-managed infrastructure. Any changes made to such fields are not reflected in the Terraform plan. If you want to update these fields, remove them from ignore_changes.

Resources that depend on availability domains are generated under availability_domain.tf file. These resources include `oci_core_boot_volume`, `oci_file_storage_file_system`, `oci_file_storage_mount_target`, and `oci_file_storage_snapshot`.

Terraform versions supported: 0.12.x, 0.13.x

Stack

The collection of Oracle Cloud Infrastructure resources corresponding to a given Terraform configuration. Each stack resides in the compartment you specify, in a single region; however, resources on a given stack can be deployed across multiple regions. An `OCID` is assigned to each stack.

You can create stacks from templates, from Terraform configurations stored either remotely or locally, or from existing compartments using resource discovery.

A stack created from a compartment represents all supported resources in the entire compartment, at the appropriate scope. If you select the root compartment for your tenancy, then the scope is the tenancy level, such as users and groups. If you select a non-root compartment, then the scope is compartment level, such as Compute instances.

Stack creation is supported from a single compartment only. Stacks cannot be created from nested compartments.

A stack has the following lifecycle states:

- **Creating**: The stack is being created.
- **Active**: The stack is available for use.
- **Deleting**: The stack is being deleted.
- **Deleted**: The stack was deleted.
- **Failed**: The stack could not be created.

State

The state of your resource configuration, stored in JSON format in a state file (`.tfstate`). The state file maps your stack's resources to your configuration and also maintains essential configuration metadata, such as resource dependencies. For instructions, see To view the state of a stack on page 3564 and To view the state of a job on page 3567. Resource Manager generates and updates state files automatically. You cannot edit the file manually.
Resource Manager supports state locking by allowing only one job at a time to run on a given stack. For more information about state files, see Hashicorp: State.

**template**

A pre-built Terraform configuration that provisions a set of resources used in a common scenario. The template can be provided by either Oracle or someone in your tenancy, as a private template. To create stacks from templates, see To create a stack on page 3557. For reference, see Templates on page 3588.

To create private templates, see Managing Private Templates on page 3578.

**Availability**

The Resource Manager service is available in all Oracle Cloud Infrastructure commercial regions. See About Regions and Availability Domains on page 180 for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

**Generalized Workflow**

The following image represents a generalized view of the Resource Manager workflow.
Links in the following steps reference Console instructions; however, you can do the same tasks using the API (through the CLI or other tool).
1. **Create a Terraform configuration.**

   **Note:**
   You can store your Terraform configuration file locally or remotely, using a source code control system. With remote storage, any job running on the associated stack automatically uses the latest version of your configuration. For more information about remotely storing your file, see Managing Configuration Source Providers on page 3581. You can skip this step if you use a template or create a stack from a compartment.

2. Create a stack.
3. Run a plan job, which produces an execution plan.
4. Review the execution plan.
5. If changes are needed in the execution plan, update the configuration and run a plan job again.
6. Run an apply job to provision resources.
7. Review state file and log files, as needed.
8. You can optionally reapply your configuration, with or without making changes, by running an apply job again.
9. Optionally, to release the resources running on a stack, run a destroy job.

For a detailed walkthrough of the Resource Manager workflow, see Getting Started on page 3541.

**Ways to Access Resource Manager**

You can access the Resource Manager service using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

Console: To access Resource Manager using the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.

API: To access Resource Manager through APIs, use Resource Manager API. To access this API using the Command Line Interface (CLI), use the `oci resource-manager` designation.

**Supported Providers**

In addition to `terraform-provider-oci` (the Terraform provider for Oracle Cloud Infrastructure), Resource Manager supports the following third-party Terraform providers.

<table>
<thead>
<tr>
<th>Third-party Terraform Provider</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>terraform-provider-ansible</code></td>
<td>1.0.3</td>
</tr>
<tr>
<td><code>terraform-provider-archive</code></td>
<td>1.1.0, 1.2.2</td>
</tr>
<tr>
<td><code>terraform-provider-checkpoint</code></td>
<td>1.0.0</td>
</tr>
<tr>
<td><code>terraform-provider-chef</code></td>
<td>0.2.0</td>
</tr>
<tr>
<td><code>terraform-provider-cloudinit</code></td>
<td>1.0.0</td>
</tr>
<tr>
<td><code>terraform-provider-digitalocean</code></td>
<td>1.13.0</td>
</tr>
<tr>
<td><code>terraform-provider-github</code></td>
<td>2.3.1</td>
</tr>
</tbody>
</table>
### Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Administrators: For common policies that give groups access to resources in Resource Manager (stacks, jobs, private templates, and configuration source providers), see Policies for Managing Resources Used with Resource Manager on page 2476. For a complete list of Resource Manager permissions, see Details for Resource Manager on page 2336. Policies for managing accessed resource types are also required.

**Important:**

Policies for managing Oracle Cloud Infrastructure resources are also required for Resource Manager operations that access resources. For example, running an apply job on a stack that includes Compute instances and subnets requires policies that grant you permissions for those resource types, in the compartments where you want to provision the resources. To see examples of policies for managing Oracle Cloud Infrastructure resources, see Common Policies on page 2142.

### Limits on Resource Manager Resources

See Resource Manager Limits on page 231.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.
Getting Started

This page helps you get started with Resource Manager by providing an end-to-end walkthrough of the tasks required to create and deploy an Oracle Cloud Infrastructure Compute instance using either a pre-built Terraform configuration or your own Terraform configuration. For a brief introduction to Resource Manager, see Overview of Resource Manager on page 3534.

Highlights

In addition to providing a pre-built Terraform configuration for creating a Compute instance, this walkthrough provides samples that demonstrate how to write a Terraform configuration. Whichever configuration you use (pre-built or your own), Resource Manager uses Terraform to provision the defined resources. The resources are organized into stacks, which you create and provision using jobs.

The walkthrough covers the following tasks:

- Select or create a Terraform configuration.
- Provision the infrastructure:
  - Create a stack in which to provision your infrastructure.
  - Run a plan job against your stack, which parses your configuration and creates an execution plan.
  - Review the generated execution plan.
  - Run an apply job against your stack, which provisions your resources. The apply job follows the execution plan, which is based on your Terraform configuration.
  - Review the resulting infrastructure.

Before You Begin

Ensure that you have installed, obtained, or created the prerequisites:

- An Oracle Cloud Infrastructure tenancy
- The OCID for the compartment where you wish to create your stack.
- A user account that includes the following:
  - An API signing key. For guidance, see Required Keys and OCIDs on page 4179.
  - Required IAM permissions. For more information, see How Policies Work on page 2136 and Details for Resource Manager on page 2336.
- If you want to use the Oracle Cloud Infrastructure CLI, install and configure the CLI first. See Quickstart on page 4195 and Configuring the CLI on page 4202

Task 1a: Select a Pre-built Terraform Configuration

You can select the Compute Instance template with its pre-built Terraform configuration instead of writing your own configuration. These steps guide you through the stack creation process.

1. Click the following link to launch the Create Stack page with the Compute Instance template already selected.
   
   Launch stack with Compute Instance template

2. In the Create Stack page, enter a Name for the new stack (or accept the default name provided). Avoid entering confidential information.

3. From the Create in Compartment drop-down, select the compartment where you want to create the stack.
   
   A compartment from the list scope is set by default.

4. Click Next.
   
   The Configure Variables panel displays variables from the Terraform configuration.
5. Review the variables and make changes as necessary.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not add your private key or other confidential information to configuration variables.</td>
</tr>
</tbody>
</table>

6. Click Next.

7. In the Review panel, verify your stack configuration.

8. Click Create to create your stack.

The stack detail page for the new stack appears.

Congratulations! You have created a stack with the pre-built Terraform configuration from the Compute Instance template. The next step is to provision the infrastructure.

**Task 1b: Create Your Own Terraform Configuration**

If you didn't select a pre-built Terraform configuration, then follow these steps to write your own.

A Terraform configuration is a file that codifies your infrastructure. The configuration defines your Terraform provider, the resources you intend to provision, variables, and specific instructions for provisioning the resources.

This page guides you through selecting the Compute Instance template with its pre-built Terraform configuration or alternatively writing your own configuration using several .tf files within a .zip file.

For more information about writing configurations for use with Resource Manager, see Terraform Configurations for Resource Manager on page 3594 and Terraform Configuration.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not provide user credentials or other confidential information in your Terraform configuration.</td>
</tr>
</tbody>
</table>

**Create an Oracle Cloud Infrastructure Provider**

The following code sample creates a basic Oracle Cloud Infrastructure Terraform provider. You can provide values as variables that are defined either in a variables file or in the provider definition (.tf) file. For more information, see Provider Configuration.

```hcl
provider "oci" {
  region = "${var.region}"
}
```

**Define Variables**

Define the variables you want to use when provisioning your resources. A best practice is to create a "variables" file in the configuration package that you upload. Following is an example from a configuration file that we've named variables.tf. For more information about using variables, see Input Variables. See also Configuring Input Variables.

```hcl
variable "compartment_ocid" {
  default = "ocid1.compartment.oc1..uniqueid"
}

variable "region" {
  default = "us-phoenix-1"
}

variable "InstanceImageOCID" {
  type = "map"
  default = {
```

Oracle Cloud Infrastructure User Guide 3542
For more information about variables declared in the preceding examples, see the following:

- **InstanceImageOCID**: Oracle-Provided Images on page 629
- **InstanceShape**: Compute Shapes on page 655
- **region** and **localAD**: Regions and Availability Domains on page 180

### Create a Virtual Cloud Network (VCN)

The following code sample creates an Oracle Cloud Infrastructure virtual cloud network (VCN) named "ExampleVCN."

```hcl
resource "oci_core_virtual_network" "ExampleVCN" {
    cidr_block = "10.1.0.0/16"
    compartment_id = "${var.compartment_ocid}"
    display_name = "TFExampleVCN"
    dns_label = "tfexamplevcn"
}
```

### Create a Subnet in Your VCN

The following code sample creates a subnet named "ExampleSubnet" in the VCN defined in the previous code sample.

```hcl
resource "oci_core_subnet" "ExampleSubnet" {
    availability_domain = "${var.localAD}"
    cidr_block = "10.1.20.0/24"
    display_name = "TFExampleSubnet"
    dns_label = "tfexamplesubnet"
    security_list_ids = ["${oci_core_virtual_network.ExampleVCN.default_security_list_id}
    compartment_id = "${var.compartment_ocid}"```
Create an Internet Gateway

The following code sample creates an internet gateway named "ExampleIG" in the VCN that we created.

```hcl
resource "oci_core_internet_gateway" "ExampleIG" {
  compartment_id = "${var.compartment_ocid}"
  display_name = "TFExampleIG"
  vcn_id = "${oci_core_virtual_network.ExampleVCN.id}"}
```

Create a Core Route Table

The following code sample creates a Oracle Cloud Infrastructure core route table in the VCN and then applies two route rules.

```hcl
resource "oci_core_route_table" "ExampleRT" {
  compartment_id = "${var.compartment_ocid}"
  vcn_id = "${oci_core_virtual_network.ExampleVCN.id}"
  display_name = "TFExampleRouteTable"
  route_rules {
    cidr_block = "0.0.0.0/0"
    network_entity_id = "${oci_core_internet_gateway.ExampleIG.id}"  
  }
}
```

Create a Compute Instance

The following extended code example creates an Oracle Cloud Infrastructure Compute instance. The code also references the image on which the Compute instance is created, sets boot volume size, adds essential metadata, and applies both free-form and defined tags.

```hcl
resource "oci_core_instance" "TFInstance" {
  count = "${var.NumInstances}"  
  availability_domain = "${var.localAD}"
  compartment_id = "${var.compartment_ocid}"
  display_name = "TFInstance${count.index}"
  shape = "${var.InstanceShape}"
  create_vnic_details {
    subnet_id = "${oci_core_subnet.ExampleSubnet.id}"
    display_name = "primaryvnic"
    assign_public_ip = true
    hostname_label = "tfexampleinstance${count.index}"  
  }
  source_details {
    source_type = "image"
    source_id = "${var.InstanceImageOCID[var.region]}"
    # Apply this to set the size of the boot volume that's created for this instance.
    # Otherwise, the default boot volume size of the image is used.
    # This should only be specified when source_type is set to "image".
    #boot_volume_size_in_gbs = "60"
  }
}
```
# Apply the following flag only if you wish to preserve the attached boot volume upon destroying this instance
# Setting this and destroying the instance will result in a boot volume that should be managed outside of this config.
# When changing this value, make sure to run 'terraform apply' so that it takes effect before the resource is destroyed.
#preserve_boot_volume = true

metadata = {
    sshAuthorizedKeys = "${var.ssh_public_key}"
}

timeouts {
    create = "60m"
}

Finalize the Configuration

Ensure that all of the configuration files are in a single directory. You can store your Terraform configuration file locally or in a source code control system. For more information on storing your file in a source code control system, see Managing Configuration Source Providers on page 3581. Wherever your file is stored, you can select it when creating a stack using the CLI or Console.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make sure your Terraform configuration file is valid. See Authoring Configurations on page 4277 and Terraform Configurations for Resource Manager on page 3594.</td>
</tr>
</tbody>
</table>

Task 2: Provision the Infrastructure

Use your Terraform configuration to build and deploy your infrastructure by taking the following actions:
1. If you created your own Terraform configuration, follow these steps to create a stack in a tenancy compartment of your choosing. (If you selected a pre-built configuration, skip this step.)

A stack is a collection of resources that you can act on as a group. All of the resources that you specify in your configuration are provisioned in the stack that you create.

You can create a stack from a remote, versioned file in a source code control system or a locally accessed file that you upload.

**To create a stack from your .zip file (Console)**

a. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.

b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

c. Click **Create Stack**.

d. On the **Create Stack** page, select **My Configuration**.

   You can either drag and drop your Terraform configuration .zip file onto the control or click **Browse** and navigate to the location of the .zip file. You can also **store your configuration remotely**.

   The dialog box is populated with information contained in the configuration.

e. Enter a **Name** for the new stack (or accept the default name provided). Avoid entering confidential information.

f. Optionally enter a **Description**.

g. From the **Create in Compartment** drop-down, select the compartment where you want to create the stack.

   A compartment from the list scope is set by default.

h. Click **Next**.

   The **Configure Variables** panel displays variables from the selected Terraform configuration file.

i. Review the variables and make changes as necessary.

   **Important:**
   
   Do not add your private key or other confidential information to configuration variables.

j. Click **Next**.

k. In the **Review** panel, verify your stack configuration.

l. Click **Create** to create your stack.

**To create a stack from your .zip file (CLI)**

Use the command related to your file location.

**To create a stack from a remote, versioned file**

Open a command prompt and run `resource-manager stack create-from-git-provider` to create a stack from a file tracked with a configuration source provider:

```
oci resource-manager stack create-from-git-provider --compartment-id <compartment_OCID> --config-source-configuration-source-provider-id <configuration_source_provider_OCID> --config-source-repository-url <repository_url> --config-source-branch-name <branch_name> --display-
```
name "<friendly_name>" --description "<description>" --terraform-version "<version>" --variables <var_file_path> --working-directory "<directory>"

**Note:**

You can return later to update stack settings or add variables after you have created the stack.

For example:

```bash
oci resource-manager stack create-from-git-provider --compartment-id ocid1.tenancy.oc1..uniqueid --config-source-configuration-source-provider-id ocid.ormconfigsourceprovider.oc1..uniqueid --config-source-repository-url https://github.com/user/repo.git --config-source-branch-name mybranch --display-name "My Stack from Git" --description "My Test" --variables file://variables.json --working-directory ""
```

For a complete list of flags and options available for CLI commands, see CLI Help.

**To create a stack from your .zip file**

This section describes how to create a stack from an uploaded configuration file (.zip).

**Note:**

You can also create stacks from configuration files stored in source code control systems, such as Git, and from templates.

On Windows, be sure the .zip file and variables.json files are in the same directory from which you're running the CLI. The CLI currently has a limitation on Windows that prevents correct handling of the files if either one is in a subdirectory.

Open a command prompt and run `oci resource-manager stack create` to create a stack:

```bash
oci resource-manager stack create --compartment-id <compartment_OCID> --config-source <config_file_name> --variables <var_file_path> --display-
name "<friendly_name>" --description "<description>" --working-directory ""

Note:
You can return later to update stack settings or add variables after you have created the stack.

Options
For a complete list of flags and options available for CLI commands, see CLI Help.

• --compartment-id is the OCID of the compartment where you want to create the stack.
• --config-source is the name of a .zip file that contains one or more Terraform configuration files.
• --variables is the path to the file specifying input variables for your resources. Optional.

The Oracle Cloud Infrastructure Terraform provider requires additional parameters when running Terraform locally (unless you are using instance principals). For more information on using variables in Terraform, see Input Variables. See also Input Variable Configuration.
• --display-name is the friendly name for the new stack. Optional.
• --description is the description for the new stack. Optional.
• --working-directory is the root configuration file in the directory. Optional. If not specified, or if null as in this example, then the service assumes that the top-level file in the directory is the root configuration file.

For example:

oci resource-manager stack create --compartment-id ocid1.tenancy.oc1..uniqueid --config-source vcn.zip --variables file://variables.json --display-name "My Example Stack" --description "My Tutorial to Create a VCN" --working-directory ""

Example response

```json
{
   "data": {
      "config-source": {
         "working-directory": null,
         "config-source-type": "ZIP_UPLOAD"
      },
      "defined-tags": {},
      "description": "My Tutorial to Create a VCN",
      "display-name": "My Example Stack",
      "freeform-tags": {},
      "id": "ocid1.ormstack.oc1..uniqueid",
      "lifecycle-state": "ACTIVE",
      "time-created": "2019-04-03T18:26:56.299000+00:00",
      "variables": {
         "compartment_ocid": "ocid1.compartment.oc1..uniqueid",
         "region": "us-phoenix-1"
      }
   }
}
```
2. Generate an execution plan.

The plan job parses your configuration to create an "execution plan," which is a step-by-step representation of the planned deployment in job log entries. Once the plan job has completed, you can evaluate the execution plan by viewing the job's log entries to confirm that it performs the expected operations, and in the intended sequence.

**To run a plan job (Console)**

a. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.

b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

c. Click the name of the stack that you want to use.

   The Stack Details page is displayed.

d. Go to Terraform Actions and select Plan.

e. In the Plan dialog, review the plan job Name and update it if needed.

f. Click Plan.

   The new plan job is listed under Jobs, with an initial state of "Accepted." Soon the status changes to "In Progress." When the job is complete, you can review the execution plan or download the job information.

**To run a plan job (CLI)**

Open a command prompt and run `oci resource-manager job create-plan-job` to run a plan job on the specified stack (`--display-name` is optional):

```
oci resource-manager job create-plan-job --stack-id <stack_OCID> --display-name "<friendly_name>"
```

Depending on the complexity of the configuration, the plan job can take several minutes to complete. When the job is complete, make sure you review the generated execution plan before running an apply job.

**To check the current state of the plan job**

Open a command prompt and run `oci resource-manager job get` to retrieve information about the job:

```
oci resource-manager job get --job-id <plan_job_OCID>
```

**Lifecycle states**

Possible values for lifecycle-state:

- ACCEPTED: The job is queued for execution.
- IN_PROGRESS: The job is running.
- FAILED: The job has failed and stopped running.
- SUCCEEDED: The job has completed successfully.
- CANCELING: The job has been notified to cancel, but has not yet stopped running.
- CANCELED: The job was canceled and has stopped running.

**Example response**

This example shows ACCEPTED for lifecycle-state.

```
{
  "data": {
    "compartment-id": "ocid1.compartment.oc1..uniqueid",
    "defined-tags": null,
    "display-name": "Example Plan Job",
    "freeform-tags": {},
    "id": "ocid1.ormjob.oc1..uniqueid",
    "lifecycle-state": "ACCEPTED",
  }
}
```
3. Review the execution plan to confirm that it represents your intentions.

The execution plan is represented in the log for the plan job you ran previously.

To review an execution plan (the log for the plan job) (Console)

a. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Jobs.

b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

c. Click the name of the plan job that you ran.

d. On the Job Details page, under Resources, click Logs.

For plan jobs, the log file is the execution plan. View the log file for the plan job and note the "message" fields in the sequence of log entries of the log file. These values represent the sequence of operations specified in your configuration.

You can also download the job information.

If changes are needed, update your stack to use a revised configuration and then rerun the plan job to obtain an updated execution plan.

To update the configuration for a stack

**Important:**

Ensure that your Terraform configuration file is valid. See Authoring Configurations on page 4277 and Terraform Configurations for Resource Manager on page 3594.

**Note:**

These instructions don't apply to configurations stored in source code control systems. You can store your Terraform configuration file locally or remotely, using a source code control system. With remote storage, any job running on the associated stack automatically uses the latest version of
If you are only editing your configuration source provider settings, skip this step.

Otherwise, ensure you have your revised Terraform configuration (.zip file or folder) ready for upload.

To edit a Terraform configuration that was generated from a template or existing compartment using resource discovery, first download the configuration. Then use the edited configuration .zip file for the update.

Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.

Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

Click the name of the stack that you want to update.

The Stack Details page is displayed.

In the Stack Information tab, next to Terraform Configuration File (.zip), click Upload New File.

In the Edit Stack dialog, either edit your configuration source provider settings (if applicable) or add your revised Terraform configuration (.zip file or folder).

You can either drag and drop it onto the dialog's control or click Browse and navigate to the location of the file or folder.

The dialog box is populated with information contained in the Terraform configuration.

Click Next as needed and then click Save Changes.

Now you can generate a new execution plan using your revised configuration.

To review an execution plan (the log for the plan job) (CLI)

View the log file and note the "message" fields in the sequence of log entries of the log file. You can view the log file for the specified job as either a paged list of entries or in its raw form.

To view the log as a paged list of entries, open a command prompt and run oci resource-manager job get-job-logs:

```
oci resource-manager job get-job-logs --job-id <job_OCID>
```

To view the log in raw form, open a command prompt and run oci resource-manager job get-job-logs-content:

```
oci resource-manager job get-job-logs-content --job-id <job_OCID>
```

If changes are needed, update your stack to use a revised configuration and then rerun the plan job to obtain an updated execution plan.
4. Provision your resources by running an apply job against the execution plan.

When satisfied with the execution plan, we're ready to do the work of provisioning the stack with the resources that we've defined. The apply job takes the execution plan and "applies" it to the stack. The result is a fully provisioned stack.

**To run an apply job (Console)**

- Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
- Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
- Click the name of the stack that you want to use.
  - The **Stack Details** page is displayed.
- Go to **Terraform Actions** and select **Apply**.
- In the **Apply** dialog, review the apply job **Name** and other settings and update it if needed.
- Click **Apply**.
  - The new apply job is listed under **Jobs**. Monitor its status: "Succeeded" indicates that the job has completed. While the job runs, or after it completes, you can download its log file.
- To view the Terraform state file (shows the state of your resources after running the job), click the name of the apply job and then click **View State** under **Resources**.

**To run an apply job (CLI)**

To check the current state of the apply job

Open a command prompt and run `oci resource-manager job create-apply-job` with the relevant value for `--execution-plan-strategy` (examples use `--display-name`, which is optional):

- To specify a plan job ("apply" an execution plan), use **FROM_PLAN_JOB_ID**:
  ```bash
  oci resource-manager job create-apply-job --stack-id <stack_OCID> --execution-plan-strategy FROM_PLAN_JOB_ID --execution-plan-job-id <plan_job_OCID> --display-name "Example Apply Job"
  ```
- To automatically approve the apply job (no plan job specified), use **AUTO_APPROVED**:
  ```bash
  oci resource-manager job create-apply-job --stack-id <stack_OCID> --execution-plan-strategy AUTO_APPROVED --display-name "Example Apply Job"
  ```

Depending on the complexity of your execution plan, the operation can take some time. Periodically check the lifecycle state of your apply job to see when it switches from **IN_PROGRESS** to **SUCCEEDED**.

**To check the current state of the apply job**

Open a command prompt and run `oci resource-manager job get` to retrieve information about the job:

```bash
oci resource-manager job get --job-id <apply_job_OCID>
```

**Lifecycle states**

Possible values for **lifecycle-state**:

- **ACCEPTED**: The job is queued for execution.
- **IN_PROGRESS**: The job is running.
- **FAILED**: The job has failed and stopped running.
- **SUCCEEDED**: The job has completed successfully.
- **CANCELING**: The job has been notified to cancel, but has not yet stopped running.
• CANCELED: The job was canceled and has stopped running.

To confirm existence of newly provisioned resources, inspect resources in the compartment.
5. Review the log entries and state file for the apply job you just ran.

- See the entries in the job log for more details about the job.

**To view the job log (Console)**

a. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Jobs**.

    You can also access jobs from a stack detail page. Click **Stacks** and then click the name of the stack you want.

b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

c. Click the name of the plan job that you ran.

d. On the **Job Details** page, under **Resources**, click **Logs**.

   For plan jobs, the log file is the execution plan. View the log file for the plan job and note the "message" fields in the sequence of log entries of the log file. These values represent the sequence of operations specified in your configuration.

   You can also download the job information.

**To view the job log (CLI)**

View the log file and note the "message" fields in the sequence of log entries of the log file. You can view the log file for the specified job as either a paged list of entries or in its raw form.

To view the log as a paged list of entries, open a command prompt and run `oci resource-manager job get-job-logs`:

```
oci resource-manager job get-job-logs --job-id <job_OCID>
```

To view the log in raw form, open a command prompt and run `oci resource-manager job get-job-logs-content`:

```
oci resource-manager job get-job-logs-content --job-id <job_OCID>
```

- The job state file represents the job's output in JSON format.

The state file maps your stack's resources to your configuration and also maintains essential configuration metadata, such as resource dependencies. Resource Manager generates and updates state files automatically when you run jobs.

The Resource Manager supports state locking by allowing only one job at a time to run on a given stack. For more information about state files, see Hashicorp: State.

**To view the state of the job (Console)**

a. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Jobs**.

    You can also access jobs from a stack detail page. Click **Stacks** and then click the name of the stack you want.

b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

c. Click the name of the job you want.

d. On the **Job Details** page, click **View State** under **Resources**.

**To view the state of the job (CLI)**
Open a command prompt and run `oci resource-manager job get-job-tf-state` to download the Terraform state of the specified job to the specified file:

```
oci resource-manager job get-job-tf-state --job-id <job_OCID> --file <output_file_name>
```

Example response for an apply job

```json
{
    "data": {
        "lineage": "57ef4f0c-c8cd-8a32-d45f-d2c40be7b915",
        "modules": [
            {
                "depends_on": [],
                "outputs": {},
                "path": [
                    "root"
                ],
                "resources": {
                    "oci_core_virtual_network.vcn1": {
                        "depends_on": [],
                        "deposed": [],
                        "primary": {
                            "attributes": {
                                "cidr_block": "10.0.0.0/16",
                                "compartment_id": "ocid1.tenancy.oc1..uniqueid",
                                "default_dhcp_options_id": "ocid1.dhcpoptions.oc1.phx.uniqueid",
                                "default_route_table_id": "ocid1.routetable.oc1.phx.uniqueid",
                                "default_security_list_id": "ocid1.securitylist.oc1.phx.uniqueid",
                                "display_name": "My VCN display name",
                                "dns_label": "myvcntest",
                                "id": "ocid1.vcn.oc1.phx.uniqueid",
                                "state": "AVAILABLE",
                                "time_created": "2018-05-24 01:13:05.855 +0000 UTC",
                                "vcn_domain_name": "myvcntest.oraclevcn.com"
                            },
                            "id": "ocid1.vcn.oc1.phx.uniqueid",
                            "meta": {
                                "e2bfb730-ecaa-11e6-8f88-34363bc7c4c0": {
                                    "create": 300000000000,
                                    "delete": 300000000000,
                                    "update": 300000000000
                                }
                            },
                            "tainted": false
                        },
                    },
                    "provider": "provider.oci",
                    "type": "oci_core_virtual_network"
                }
            }
        ],
        "serial": 4
    }
}
```
6. When you need to release the resources that you provisioned, run a destroy job on the stack.

A destroy job tears down the stack that you created and then cleans up associated resources without deleting them. For example, the destroy job terminates Compute instances associated with the stack.

**To run a destroy job (Console)**

```
<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can also import state files for resources already managed by Terraform.</td>
</tr>
</tbody>
</table>
```

- a. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
- b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
- c. Click the name of the stack that you want to use.
  The Stack Details page is displayed.
- d. Go to Terraform Actions and select Destroy.
- e. Click Destroy again to confirm your action.
  You can monitor the status and review the results of a destroy job by viewing the state or the logs.
- f. To view the Terraform state file (shows the state of your resources after running the job), click the name of the job to display the Job Details page, then click View State under Resources.
- g. To view the logs for the job, click the name of the job to display the Job Details page, then click Logs under Resources.

**To run a destroy job (CLI)**

```
<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>We recommend running a destroy job before deleting a stack to release associated resources first. When you delete a stack, its associated state file is also deleted; therefore, you lose track of the state of its associated resources. Cleaning up resources associated with a deleted stack can be difficult without the state file, especially when those resources are spread across multiple compartments. To avoid difficult cleanup later, we</td>
</tr>
</tbody>
</table>
```
recommend that you release associated resources first by running a destroy job.

Open a command prompt and run `oci resource-manager job create-destroy-job` to tear down and clean up the resources provisioned by the specified stack:

```
oci resource-manager job create-destroy-job --stack-id <stack_OCID> --execution-plan-strategy=AUTO_APPROVED
```

To confirm deletion of the resources, inspect resources in the compartment.

## Managing Stacks and Jobs

This topic describes how to create, edit, and delete stacks as well as work with jobs, including generating and applying execution plans. Drift detection is also covered in this topic.

### Prerequisites

- **IAM policies:** To manage stacks and jobs, you must be given the required type of access in a *policy* written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which *compartment* you should work in.

  Administrators: For common policies that give groups access to resources in Resource Manager (stacks, jobs, private templates, and configuration source providers), see Policies for Managing Resources Used with Resource Manager on page 2476. For a complete list of Resource Manager permissions, see Details for Resource Manager on page 2336. Policies for managing accessed resource types are also required.

  **Important:** Policies for managing Oracle Cloud Infrastructure resources are also required for Resource Manager operations that access resources. For example, running an apply job on a stack that includes Compute instances and subnets requires policies that grant you permissions for those resource types, in the compartments where you want to provision the resources. To see examples of policies for managing Oracle Cloud Infrastructure resources, see Common Policies on page 2142.

- **Terraform configuration file:** To create or update a stack, you must have a valid Terraform configuration file. See Terraform Configurations for Resource Manager on page 3594 and Authoring Configurations on page 4277.

### Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

### Moving Resources to a Different Compartment

You can move stacks from one compartment to another. When you move a stack to a new compartment, its associated jobs move with it. After you move the stack to the new compartment, inherent policies apply immediately and affect access to the stack and associated jobs through the Console. For more information, see Managing Compartments on page 2431.

### Using the Console

#### Managing Stacks (Console)

**To create a stack**

This section describes how to start from the Create Stack dialog when creating stacks. You can also start your stack creation process from the Create Compute Instance page.
1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click **Create Stack**.
4. In the **Create Stack** dialog, under **Choose the origin of the Terraform configuration**, select the option you want.
   - **My Configuration**: Local folder or .zip file.
     Under **Stack Configuration**, select either **Folder** or **Zip File**.
     You can either drag and drop it onto the dialog's control or click **Browse** and navigate to the folder or file location.
     The dialog box is populated with information contained in the local Terraform configuration.
   - **Template**: Pre-built Terraform configuration (service, architecture, or private template).
     Under **Stack Configuration**, click **Select Template** and then select the template you want. **Private templates** are under the **Private** tab.
     The dialog box is populated with information contained in the Terraform configuration for the selected template.
   - **Source Code Control System**: Remote location using a **configuration source provider**.
     **Steps**
     a. Under **Stack Configuration**, select a **Configuration Source Provider**.
        If you need to create one, see To create a configuration source provider on page 3582.
     b. Select a **Repository**.
        Example: https://gitlab.com/example
     c. Select a **Branch**.
        The list returned is limited to 100 branches.
     d. (Optional) Specify a **Working Directory** for running Terraform.
        Example (one level): Directory
        Example (two levels): Directory/Subdirectory
        If not specified, the root directory is used.
     The dialog box is populated with information contained in the remote Terraform configuration.
   - **Existing Compartment**: Generate a Terraform configuration using **resource discovery**.
     **Steps**
     • Select the **Compartment for Resource Discovery** (the compartment containing the resources that you want to capture).
       A compartment from the list scope is set by default.
     • Select the **Region for Resource Discovery** (the region containing the resources that you want to capture).
     • To filter for specific **Terraform provider services** supported for use with resource discovery, select **Selected** and then select the services you want.
     **Note:**
     This setting cannot be changed when editing the stack later.
5. Enter a **Name** for the new stack (or accept the default name provided). Avoid entering confidential information.
6. Optionally enter a **Description**.
7. From the **Create in Compartment** drop-down, select the compartment where you want to create the stack.
   A compartment from the list scope is set by default.
8. Optionally apply tags to the stack.

If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

9. Click Next.

The Configure Variables panel displays variables from the Terraform configuration.

No variables are listed for the Existing Compartment stack origin because no Terraform configuration exists yet.

10. Review the variables and make changes as necessary.

    | Important: |
    | Do not add your private key or other confidential information to configuration variables. |

11. Click Next.

12. In the Review panel, verify your stack configuration.

13. Click Create to create your stack.

    The stack detail page for the new stack appears.

Existing Compartment stack origin: A work request runs on your stack. When the work request finishes, a job runs to generate a Terraform configuration file for the stack. When the job finishes, the resources in the selected compartment are captured in the generated configuration. You can recreate these resources in another compartment.

To deploy the defined resources, run an apply job on your new stack.

To begin stack creation from the Create Compute Instance page

You can create a stack using the configuration you specify in the Create Compute Instance page available in the Console. Use the new stack to install, configure, and manage your Compute instance through the "infrastructure-as-code" model.

    | Note: |
    | Before you start, view requirements for creating Compute instances. See Required IAM Policy on page 695 and the prerequisites for Creating a Linux Instance on page 697 or Creating a Windows Instance on page 702. |

1. Open the Create Compute Instance page:

    a. Open the navigation menu. Under Core Infrastructure, go to Compute and click Instances.

    b. Click Create Instance.

2. Populate configuration fields to specify stack details. For example, select the image you want to use in your stack.

3. Click Create as Stack.

    The Create Stack dialog window appears. The "Compute Instance" stack origin is indicated at the top of the dialog window, along with any provided instance name.
4. In the **Create Stack** dialog window, do the following.
   a. Enter a **Name** for the new stack. Avoid entering confidential information.
      Example: My Compute Instance
   b. Optionally enter a **Description**.
   c. From the **Create in Compartment** drop-down, select the compartment where you want to create the stack.
      A compartment from the list scope is set by default.
   d. Select a **Terraform Version**.

   **Note:**
   Terraform versions are not backward compatible.

   e. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

   f. Click **Next**.
      The **Configure Variables** panel displays variables from the selected Terraform configuration file.
   g. Review the variables and make changes as necessary.

   **Important:**
   Do not add your private key or other confidential information to configuration variables.

   h. Click **Next**.
   i. In the **Review** panel, verify your stack configuration.
   j. Click **Create** to create your stack.

To deploy the defined Compute *instance*, run an apply job on your new stack.

**To see how Terraform represents your resources**

Learn how Terraform uses HashiCorp Configuration Language (HCL) syntax to represent Oracle Cloud Infrastructure resources.

1. Capture existing infrastructure by creating a stack from that compartment.

   The stack detail page for the new stack appears. A work request runs on your stack. When the work request finishes, a job runs to generate a Terraform configuration file for the stack. When the job finishes, the resources in the selected compartment are captured in the generated configuration.

2. Download the generated Terraform configuration file: In the Stack Information tab of the stack detail page, click **Download**.

**To recreate (clone) existing infrastructure in another compartment**

1. Capture existing infrastructure by creating a stack from that compartment.

   The stack detail page for the new stack appears. A work request runs on your stack. When the work request finishes, a job runs to generate a Terraform configuration for the stack. When the job finishes, the resources in the selected compartment are captured in the generated configuration.

2. Download the generated Terraform configuration file: In the Stack Information tab of the stack detail page, click **Download**.

3. Edit the vars.tf file (variables in the downloaded Terraform configuration file) to specify the destination **compartment_ocid** and **region**.

   Example:

   ```hcl
   variable "compartment_ocid" {
     default = "ocid1.compartment.oc1..uniqueid"
   }
   ```
variable "region" {
    default = "us-phoenix-1"
}

4. If the destination region has more or fewer availability domains than the source region, then edit the vars.tf file to specify the correct number of availability domains.

For example, if you cloned from a region that has 3 availability domains and you want to recreate the infrastructure in a region that has only 1 availability domain, then remove the references to the second and third availability domains.

Example showing 3 availability domains:

```terraform
data oci_identity_availability_domain export_NzDH-EU-FRANKFURT-1-AD-1 {
    compartment_id = var.compartment_ocid
    ad_number      = "1"
}
data oci_identity_availability_domain export_NzDH-EU-FRANKFURT-1-AD-2 {
    compartment_id = var.compartment_ocid
    ad_number      = "2"
}
data oci_identity_availability_domain export_NzDH-EU-FRANKFURT-1-AD-3 {
    compartment_id = var.compartment_ocid
    ad_number      = "3"
}
```

Example showing 1 availability domain:

```terraform
data oci_identity_availability_domain export_NzDH-EU-FRANKFURT-1-AD-1 {
    compartment_id = var.compartment_ocid
    ad_number      = "1"
}
```

5. Create a second stack using the edited configuration file.
   a. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
   b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you’re not sure which compartment to use, contact an administrator.
   c. Click Create Stack.
   d. In the Create Stack dialog, click My Configuration.
   e. Add the downloaded Terraform configuration (.zip) file.
      You can leave other fields as is for now. For reference, see To create a stack on page 3557.
   f. For Terraform Version, select a version supported by resource discovery.
      Terraform versions supported: 0.12.x, 0.13.x
   g. Click Next to display the Configure Variables panel.
   h. Update the compartment_ocid variable to specify the destination compartment for the cloned resources.
   i. If you want to clone the resources to a different region, update the region variable.
   j. Click Next to display the Review panel.
   k. Click Create to create your stack.
      The stack detail page for the second stack appears.

6. To confirm that the stack will create resources as expected, run a plan job.

7. Clone resources: Run an apply job on the new stack.
   The resources are cloned in the specified compartment and region.
To view stacks

You can view stack names, descriptions, states, and time created. The detail page for a stack lists its drift status and allows you to view the latest drift detection report.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you’re not sure which compartment to use, contact an administrator.
3. To display the detail page for a stack, click the stack’s name.

To download the stack’s Terraform configuration file

The Terraform configuration file listed on the stack detail page is the same as the Terraform configuration file listed on the job detail page for the most recent successful job.

Note:

For stacks created using source code control systems, configuration files are not available for download until a job is successfully run on the stack.

To detect drift for a stack or selected resources

You can detect drift for new stacks created from compartments or for stacks where the last job run was Apply or Import State. When detecting drift, you can specify all resources or selected resources.

Drift is the difference between the actual, real-world state of your infrastructure and the stack's last executed configuration. For example, drift occurs when a team member adds a production tag to your resources, or when a resource is deleted.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you’re not sure which compartment to use, contact an administrator.
3. Click the name of the stack to display its detail page.
4. In the Stack Information tab, to the right of Terraform Configuration File (.zip), click Download.

To view the latest drift detection report

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the stack to display its detail page.


   Alternatively go to the Stack Information tab. Under Drift Detection, click View drift detection report.

   A panel lists the drift status of the specified resources defined by the stack. Resources are identified by resource names.

5. To view details of drift status for a resource, click the down arrow.

   Expected and actual properties are listed.

6. (Optional) To make your resources match the properties of your Terraform configuration, run an apply job: In the Stack Details page, go to Terraform Actions and select Apply.

To view an old drift detection report

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the stack to display its detail page.

4. Click Work Requests.

5. Click the work request for the drift detection report you want.

6. In the Work Requests Information tab, click View Drift Detection Report.

   A panel lists the drift status of the specified resources defined by the stack at the time the drift detection was detected. Resources are identified by resource names.

7. To view details of drift status for a resource, click the down arrow.

   Expected and actual properties are listed.

To view the latest drift detection report, see To view the latest drift detection report on page 3562. To detect drift again, see To detect drift for a stack or selected resources on page 3562.

To edit a stack

You can edit stacks. When editing a stack, you can upload a different configuration and change its name, description, and variables.

Note:

If your configuration is stored in a source code control system, such as GitLab, then commit your changes there. The most recent commit is used when you run jobs on the stack. No configuration file is available for download until a job is successfully run on the stack.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the Actions icon (three dots), and then select Edit.

   You can also edit a stack from its detail page. Click the name of the stack to display its detail page and then click Edit Stack.
4. In the **Edit Stack** dialog, change the properties you want.

**Note:**

The stack's Terraform version cannot be changed.

- To edit the values assigned to variables in a stack, click **Configure Variables**.

You can also edit a stack from its detail page. Click the name of the stack to display the **Stack Details** page, click **Variables** (under **Resources**) and then click **Edit Variables**.

**Important:**

Do not add your private key or other confidential information to configuration variables.

If you want to add, reconfigure, or delete variables in a stack, update the Terraform configuration.

5. Click **Save Changes**.

**To view the state of a stack**

Download the state file corresponding to the most recently run job for the stack.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the stack to display its detail page.
4. Go to **More Actions** and select **Download Terraform State**.

**To manage tags for a stack**

Tags are key/value pairs that you can attach to resources to help you organize and track your resources across compartments. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the stack you want.

   The **Stack Details** page lists the details about the selected job.
4. Click **Tags** to view or edit existing tags, or click **Add Tags** to add new ones.

**To move a stack to a different compartment**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the Actions icon (three dots), and then select **Move Stack**.

   You can also move a stack from its detail page. Click the name of the stack to display the **Stack Details** and then click **Move Stack**.
4. In the **Move Resource To A Different Compartment** dialog box, select the compartment that you want to move the stack to.
5. Click **Move Resource**.

**To delete a stack**

**Note:**

Associated resources persist after stack deletion. When you delete a stack, its associated state file is also deleted; therefore, you lose track of the state.
1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the Actions icon (three dots), select Delete, and confirm the operation when prompted.

**Note:**
You cannot undo the delete stack operation.

You can also delete a stack from its detail page. Click the name of the stack to display the Stack Details and then click Delete Stack.

**Managing Jobs (Console)**

*To view jobs and job details*

You can view name, type, status, and other key information about jobs for a given compartment or stack. You can view name, type, status, and other key information about a given job. You can also access the job's execution plan (represented by the job log), Terraform configuration, and Terraform state, as well as view the variables used in the job.

For configurations stored in a source code control system, such as GitLab, job details include the relevant commit identifier.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Jobs.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. To view job details, click the name of the job you want.

The Job Details page lists the details about the selected job.

4. To view variables used in the job, click Variables under Resources.

**To manage tags for a job**

Tags are key/value pairs that you can attach to resources to help you organize and track your resources across compartments. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Jobs.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the job you want.

The Job Details page lists the details about the selected job.

4. Click Tags to view or edit existing tags, or click Add Tags to add new ones.

**To generate an execution plan (run a plan job)**

Running a plan job parses your Terraform configuration and converts it into an execution plan listing resources and actions that will result when an apply job is run. For configurations stored in a source code control system, such as GitLab, the job uses the most recent commit. We recommend generating an execution plan before running an apply job.
1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the stack that you want to use.

   The **Stack Details** page is displayed.

4. Go to **Terraform Actions** and select **Plan**.

5. In the **Plan** dialog, review the plan job **Name** and update it if needed.

6. Click **Plan**.

   The new plan job is listed under **Jobs**, with an initial state of "Accepted." Soon the status changes to "In Progress." When the job is complete, you can review the execution plan or download the job information.

### To view the job log

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Jobs**.

   You can also access jobs from a stack detail page. Click **Stacks** and then click the name of the stack you want.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the plan job that you ran.

4. On the **Job Details** page, under **Resources**, click **Logs**.

   For plan jobs, the log file is the execution plan. View the log file for the plan job and note the "message" fields in the sequence of log entries of the log file. These values represent the sequence of operations specified in your configuration.

   You can also download the job information.

### To update the configuration for a stack

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that your Terraform configuration file is valid. See Authoring Configurations on page 4277 and Terraform Configurations for Resource Manager on page 3594.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your configuration is stored in a source code control system, such as GitLab, then commit your changes there. The most recent commit is used when you run jobs on the stack.</td>
</tr>
</tbody>
</table>

1. If you are only editing your configuration source provider settings, skip this step.

   Otherwise, ensure you have your revised Terraform configuration (.zip file or folder) ready for upload.

   To edit a Terraform configuration that was generated from a template or existing compartment using resource discovery, first download the configuration. Then use the edited configuration .zip file for the update.

2. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.

3. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

4. Click the name of the stack that you want to update.

   The **Stack Details** page is displayed.

5. In the **Stack Information** tab, next to **Terraform Configuration File (.zip)**, click **Upload New File**.

6. In the **Edit Stack** dialog, either edit your configuration source provider settings (if applicable) or add your revised Terraform configuration (.zip file or folder).

   You can either drag and drop it onto the dialog's control or click **Browse** and navigate to the location of the file or folder.

   The dialog box is populated with information contained in the Terraform configuration.
7. Click Next as needed and then click Save Changes.

Now you can generate a new execution plan using your revised configuration.

To download job information

You can download files associated with jobs: Terraform configurations, Terraform states, and logs.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Jobs.

   You can also access jobs from a stack detail page. Click Stacks and then click the name of the stack you want.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the job you want.

   The Job Details page appears.

   You can view the log by clicking Logs under Resources.

   You can view the state of your resources (for relevant jobs) by clicking View State under Resources.

4. Download the job information you want:

<table>
<thead>
<tr>
<th>To download this job-associated file</th>
<th>Click</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terraform configuration (.zip file)</td>
<td>Download Terraform Configuration</td>
</tr>
<tr>
<td>Terraform state (.json file)</td>
<td>Download Terraform State</td>
</tr>
<tr>
<td>Logs (.txt file)</td>
<td>Download Logs (Logs section under Resources)</td>
</tr>
</tbody>
</table>

To run an apply job

When you run an apply job for a stack, Terraform creates the resources and executes the actions defined in your Terraform configuration. For configurations stored in a source code control system, such as GitLab, the job uses the most recent commit. The time required to complete an apply job depends on the number and type of cloud resources to be created.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the stack that you want to use.

   The Stack Details page is displayed.

4. Go to Terraform Actions and select Apply.

5. In the Apply dialog, review the apply job Name and other settings and update it if needed.

6. Click Apply.

   The new apply job is listed under Jobs. Monitor its status: "Succeeded" indicates that the job has completed. While the job runs, or after it completes, you can download its log file.

7. To view the Terraform state file (shows the state of your resources after running the job), click the name of the apply job and then click View State under Resources.

To view the state of a job

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Jobs.

   You can also access jobs from a stack detail page. Click Stacks and then click the name of the stack you want.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the job you want.

4. On the Job Details page, click View State under Resources.

To import an existing Terraform state file (run an import job)

You can import state files for existing resources already managed by Terraform.
1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the stack that you want to use.

   The **Stack Details** page appears.
4. Go to **Terraform Actions** and select **Import State**.
5. In the **Import State File** dialog, review the job **Name** and update it if needed. Avoid entering confidential information.
6. Add your Terraform state file, either by dragging and dropping it onto the dialog's control, or by clicking **Browse** and navigating to the file location.
7. Click **Import**.

   **To release a stack's resources (run a destroy job)**

   Run a destroy job to tear down the resources and clean up the tenancy.

   **Note:**

   We recommend running a destroy job before deleting a stack to release associated resources first. When you delete a stack, its associated state file is also deleted; therefore, you lose track of the state of its associated resources. Cleaning up resources associated with a deleted stack can be difficult without the state file, especially when those resources are spread across multiple compartments. To avoid difficult cleanup later, we recommend that you release associated resources first by running a destroy job.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the stack that you want to use.

   The **Stack Details** page is displayed.
4. Go to **Terraform Actions** and select **Destroy**.
5. Click **Destroy** again to confirm your action.

   You can monitor the status and review the results of a destroy job by viewing the state or the logs.
6. To view the Terraform state file (shows the state of your resources after running the job), click the name of the job to display the **Job Details** page, then click **View State** under **Resources**.
7. To view the logs for the job, click the name of the job to display the **Job Details** page, then click **Logs** under **Resources**.

**Using the CLI**

This section provides basic sample CLI commands for managing stacks and jobs. For information about using the CLI, see **Command Line Interface (CLI)** on page 4192. For a complete list of flags and options available for CLI commands, see **CLI Help**.

**Managing Stacks (CLI)**

**To create a stack from a file (CLI)**

Use the command related to your file location.

**Important:**

Ensure your Terraform configuration file is valid. See **Authoring Configurations** on page 4277 and **Terraform Configurations for Resource Manager** on page 3594.

To create a stack from a file hosted on a source code control system
Open a command prompt and run `resource-manager stack create-from-git-provider` to create a stack from a file tracked with a configuration source provider:

```
oci resource-manager stack create-from-git-provider --compartment-id <compartment_OCID> --config-source-configuration-source-provider-id <configuration_source_provider_OCID> --config-source-repository-url <repository_url> --config-source-branch-name <branch_name> --display-name "<friendly_name>" --description "<description>" --terraform-version "<version>" --variables <var_file_path> --working-directory "<directory>"
```

**Note:**
You can return later to update stack settings or add variables after you have created the stack.

For example:

```
oci resource-manager stack create-from-git-provider --compartment-id ocid1.tenancy.oc1..uniqueid --config-source-configuration-source-provider-id ocid.ormconfigsourceprovider.oc1..uniqueid --config-source-repository-url https://github.com/user/repo.git --config-source-branch-name mybranch --display-name "My Stack from Git" --description "My Test" --variables file://variables.json --working-directory ""
```

For a complete list of flags and options available for CLI commands, see [CLI Help](#).

To create a stack from an uploaded file:

This section describes how to create a stack from an uploaded configuration file (.zip).

**Note:**
You can also create stacks from configuration files stored in source code control systems, such as Git, and from templates.

On Windows, be sure the .zip file and variables.json files are in the same directory from which you're running the CLI. The CLI currently has a limitation on Windows that prevents correct handling of the files if either one is in a subdirectory.

Open a command prompt and run `oci resource-manager stack create` to create a stack:

```
oci resource-manager stack create --compartment-id <compartment_OCID> --config-source <config_file_name> --variables <var_file_path> --display-name "<friendly_name>" --description "<description>" --working-directory ""
```

**Note:**
You can return later to update stack settings or add variables after you have created the stack.

**Options**

For a complete list of flags and options available for CLI commands, see [CLI Help](#).

- `--compartment-id` is the OCID of the compartment where you want to create the stack.
- `--config-source` is the name of a .zip file that contains one or more Terraform configuration files.
- `--variables` is the path to the file specifying input variables for your resources. Optional.

The Oracle Cloud Infrastructure Terraform provider requires additional parameters when running Terraform locally (unless you are using instance principals). For more information on using variables in Terraform, see [Input Variables](#). See also [Input Variable Configuration](#).

- `--display-name` is the friendly name for the new stack. Optional.
- `--description` is the description for the new stack. Optional.
• --working-directory is the root configuration file in the directory. Optional. If not specified, or if null as in this example, then the service assumes that the top-level file in the directory is the root configuration file.

For example:

```
oci resource-manager stack create --compartment-id ocid1.tenancy.oc1..uniqueid --config-source vcn.zip --variables file://variables.json --display-name "My Example Stack" --description "My Tutorial to Create a VCN" --working-directory ""
```

Example response

```
{
  "data": {
    "config-source": {
      "working-directory": null,
      "config-source-type": "ZIP_UPLOAD"
    },
    "defined-tags": {},
    "description": "My Tutorial to Create a VCN",
    "display-name": "My Example Stack",
    "freeform-tags": {},
    "id": "ocid1.ormstack.oc1..uniqueid",
    "lifecycle-state": "ACTIVE",
    "time-created": "2019-04-03T18:26:56.299000+00:00",
    "variables": {
      "compartment_ocid": "ocid1.compartment.oc1..uniqueid",
      "region": "us-phoenix-1"
    }
  }
}
```

To discover resources (create a stack from a compartment)

Open a command prompt and run `oci resource-manager stack create-from-compartment` to create a stack from the specified compartment and region:

```
oci resource-manager stack create-from-compartment --config-source-compartment-id <source_compartment_OCID> --config-source-region <source_region> --config-source-services-to-discover [<services>] --compartment-id <compartment_OCID> --terraform-version <version> --display-name "<friendly_name>" --description "<description>"
```

For example (discovers resources from the core and database Terraform provider services; the source compartment is not a root compartment):

```
oci resource-manager stack create-from-compartment --config-source-compartment-id ocid1.tenancy.oc1..uniqueid1 --config-source-region PHX --config-source-services-to-discover [core, database] --compartment-id ocid1.tenancy.oc1..uniqueid2 --terraform-version 0.13.X --display-name "Stack From Compartment ABC" --description "List of Resources to Duplicate"
```

Example response

```
{
  "data": {
    "config-source": {
      "config-source-type": "COMPARTMENT_CONFIG_SOURCE"
    },
    "defined-tags": {},
    "description": "List of Resources to Duplicate",
    "display-name": "Stack From Compartment ABC",
    "id": "ocid1.ormstack.oc1..uniqueid2",
    "lifecycle-state": "ACTIVE",
    "time-created": "2019-04-03T18:26:56.299000+00:00"
  }
}
```
"display-name": "Stack from Compartment ABC",
"freeform-tags": {},
"id": "ocid1.ormstack.oc1..uniqueid",
"lifecycle-state": "CREATING",
"time-created": "2019-04-03T18:26:56.299000+00:00",
"variables": {
  "compartment_ocid": "ocid1.compartment.oc1..uniqueid1",
  "region": "us-phoenix-1"
}
}

{
"data": {
  "compartment-id": "ocid1.compartment.oc1..uniqueid2",
  "config-source": {
    "compartment-id": "ocid1.compartment.oc1..uniqueid1",
    "config-source-type": "COMPARTMENT_CONFIG_SOURCE",
    "region": "PHX",
    "working-directory": null
  },
  "defined-tags": {},
  "description": "List of Resources to Duplicate",
  "display-name": "Stack From Compartment ABC",
  "freeform-tags": {},
  "id": "ocid1.ormstack.oc1.phx.uniqueid",
  "lifecycle-state": "CREATING",
  "stack-drift-status": "NOT_CHECKED",
  "terraform-version": "0.12.x",
  "time-created": "2020-06-01T18:25:56.102000+00:00",
  "time-drift-last-checked": null,
  "variables": {}
},
"etag": "009010cb57f5162655c6a34f5ef8834f204a734df81e4baa696a7d830488ea25",
"opc-work-request-id": "ocid1.ormworkrequest.oc1.phx.uniqueid"
}

To list resources for discovery

This section describes how to determine which services are supported for resource discovery from a given compartment OCID.

When you create a stack from a compartment, the stack represents all supported resources in the entire compartment, at the appropriate scope. If you select the root compartment for your tenancy, then the scope is the tenancy level, such as users and groups. If you select a non-root compartment, then the scope is compartment level, such as Compute instances.

Open a command prompt and run `oci resource-manager stack list-resource-discovery-services` to retrieve a list of services supported for resource discovery (the compartment OCID is used for authorization only):

```
oci resource-manager stack list-resource-discovery-services --compartment-id <compartment_OCID>
```

To list stacks in a compartment

Open a command prompt and run `oci resource-manager stack list` to list the stacks in a compartment:

```
oci resource-manager stack list --compartment-id <compartment_OCID>
```
To list full details of a stack
Open a command prompt and run `oci resource-manager stack get` to list the details for the specified stack:

```bash
oci resource-manager stack get --stack-id <stack_OCID>
```

To detect drift for a stack
Open a command prompt and run `oci resource-manager stack get` to detect drift for the specified stack:

```bash
oci resource-manager stack detect-drift --stack-id <stack_OCID>
```

To list resource details in the stack's last drift detection report
Open a command prompt and run `oci resource-manager stack get` to list the resource details for the last drift detection report of a specified stack:

```bash
oci resource-manager stack list-resource-drift-details --stack-id <stack_OCID>
```

To delete a stack

**Note:**
Associated resources persist after stack deletion. When you delete a stack, its associated state file is also deleted; therefore, you lose track of the state of its associated resources. Cleaning up resources associated with a deleted stack can be difficult without the state file, especially when those resources are spread across multiple compartments. To avoid difficult cleanup later, we recommend that you release associated resources first by running a destroy job.

Open a command prompt and run `oci resource-manager stack delete` to delete the specified stack:

```bash
oci resource-manager stack delete --stack-id <stack_OCID>
```

Managing Jobs (CLI)

To generate an execution plan (run a plan job)
Open a command prompt and run `oci resource-manager job create-plan-job` to run a plan job on the specified stack (---display-name is optional):

```bash
oci resource-manager job create-plan-job --stack-id <stack_OCID> --display-name "<friendly_name>"
```

Depending on the complexity of the configuration, the plan job can take several minutes to complete. When the job is complete, make sure you review the generated execution plan before running an apply job.

To check the current state of the plan job
Open a command prompt and run `oci resource-manager job get` to retrieve information about the job:

```bash
oci resource-manager job get --job-id <plan_job_OCID>
```

Lifecycle states
Possible values for lifecycle-state:

- ACCEPTED: The job is queued for execution.
- IN_PROGRESS: The job is running.
- FAILED: The job has failed and stopped running.
• SUCCEEDED: The job has completed successfully.
• CANCELING: The job has been notified to cancel, but has not yet stopped running.
• CANCELED: The job was canceled and has stopped running.

Example response
This example shows ACCEPTED for lifecycle-state.

```json
{
  "data": {
    "compartment-id": "ocid1.compartment.oc1..uniqueid",
    "defined-tags": null,
    "display-name": "Example Plan Job",
    "freeform-tags": {},
    "id": "ocid1.ormjob.oc1..uniqueid",
    "lifecycle-state": "ACCEPTED",
    "operation": "PLAN",
    "jobOperationDetails": {
      "operation": "PLAN"
    },
    "stack-id": "ocid1.ormstack.oc1..uniqueid",
    "time-created": "2019-03-09T20:52:13.922000+00:00",
    "time-finished": null,
    "variables": {
      "compartment_ocid": "ocid1.compartment.oc1..uniqueid",
      "region": "us-phoenix-1"
    }
  }
}
```

To review an execution plan (view the log for a plan job)

Review the execution plan to ensure that it accurately reflects your intentions. View the log file and note the "message" fields in the sequence of log entries of the log file. These values represent the sequence of operations specified in your configuration.

Open a command prompt and run `oci resource-manager job get-job-logs` to view the log file for the specified job:

```
oci resource-manager job get-job-logs --job-id <plan_job_OCID>
```

If you see problems or errors and wish to make changes, then update the appropriate configuration file (.tf file), update the stack to use the revised configuration, generate a new execution plan, and then review the new execution plan.

Example response

The command returns JSON objects that describe log entries. Each object has a message member with a property that displays one line of the execution plan. In the example shown below, the plan creates a single virtual cloud network (VCN); the remaining members show details about the VCN.

```json
...
  {
    "level": "INFO",
    "message": "Terraform will perform the following actions:",
    "timestamp": "2018-05-24T00:57:14.170000+00:00",
    "type": "TERRAFORM_CONSOLE"
  },
  {
    "level": "INFO",
```
To update an execution plan (update an uploaded configuration for a stack)

**Note:**

These instructions don't apply to configurations stored in source code control systems. You can store your Terraform configuration file locally or remotely, using a source code control system. With remote storage, any job running on the associated stack automatically uses the latest version of your configuration. For more information about remotely storing your file, see Managing Configuration Source Providers on page 3581.
To edit a Terraform configuration that was generated from a template or existing compartment using resource discovery, first download the configuration. Then use the edited configuration.zip file for the update.

Open a command prompt and run `oci resource-manager stack update` with the option `--config-source` to update the Terraform configuration for the specified stack:

```
oci resource-manager stack update --stack-id <stack_OCID> --config-source <config_file_name>
```

After updating the stack, regenerate and review an execution plan (run a new plan job and then view the log file).

**To run an apply job**

To check the current state of the apply job

Open a command prompt and run `oci resource-manager job create-apply-job` with the relevant value for `--execution-plan-strategy` (examples use `--display-name`, which is optional):

- To specify a plan job ("apply" an execution plan), use `FROM_PLAN_JOB_ID`:

  ```
  oci resource-manager job create-apply-job --stack-id <stack_OCID> --execution-plan-strategy FROM_PLAN_JOB_ID --execution-plan-job-id <plan_job_OCID> --display-name "Example Apply Job"
  ```

  Use this option to "apply" your confirmed execution plan to the stack, execute the instructions, and provision the stack with the specified resources.

- To automatically approve the apply job (no plan job specified), use `AUTO_APPROVED`:

  ```
  oci resource-manager job create-apply-job --stack-id <stack_OCID> --execution-plan-strategy AUTO_APPROVED --display-name "Example Apply Job"
  ```

Depending on the complexity of your execution plan, the operation can take some time. Periodically check the lifecycle state of your apply job to see when it switches from `IN_PROGRESS` to `SUCCEEDED`.

**To check the current state of the apply job**

Open a command prompt and run `oci resource-manager job get` to retrieve information about the job:

```
oci resource-manager job get --job-id <apply_job_OCID>
```

**Lifecycle states**

Possible values for `lifecycle-state`:

- `ACCEPTED`: The job is queued for execution.
- `IN_PROGRESS`: The job is running.
- `FAILED`: The job has failed and stopped running.
- `SUCCEEDED`: The job has completed successfully.
- `CANCELING`: The job has been notified to cancel, but has not yet stopped running.
- `CANCELED`: The job was canceled and has stopped running.

To confirm existence of newly provisioned resources, inspect resources in the compartment.

**To download or view job information**

You can download Terraform configurations and Terraform states associated with jobs. You can also view logs associated with jobs.

For configurations stored in a source code control system, such as GitLab, job details include the relevant commit identifier.

To download the configuration for a job
Open a command prompt and run `oci resource-manager job get-job-tf-config` to download the Terraform configuration of the specified job to the specified file:

```bash
oci resource-manager job get-job-tf-config --job-id <job_OCID> --file <output_file_name>
```

To download the state file for a job

Open a command prompt and run `oci resource-manager job get-job-tf-state` to download the Terraform state of the specified job to the specified file:

```bash
oci resource-manager job get-job-tf-state --job-id <job_OCID> --file <output_file_name>
```

**Example response for an apply job**

```json
{
  "data": {
    "lineage": "57ef4f0c-c8cd-8a32-d45f-d2c40be7b915",
    "modules": [
      {
        "depends_on": [],
        "outputs": {},
        "path": [
          "root"
        ],
        "resources": {
          "oci_core_virtual_network.vcn1": {
            "depends_on": [],
            "deposed": [],
            "primary": {
              "attributes": {
                "cidr_block": "10.0.0.0/16",
                "compartment_id": "ocid1.tenancy.oc1..uniqueid",
                "default_dhcp_options_id": "ocid1.dhcpoptions.oc1.phx.uniqueid",
                "default_route_table_id": "ocid1.routetable.oc1.phx.uniqueid",
                "default_security_list_id": "ocid1.securitylist.oc1.phx.uniqueid",
                "display_name": "My VCN display name",
                "dns_label": "myvcntest",
                "id": "ocid1.vcn.oc1.phx.uniqueid",
                "state": "AVAILABLE",
                "time_created": "2018-05-24 01:13:05.855 +0000 UTC",
                "vcn_domain_name": "myvcntest.oraclevcn.com"
              },
              "id": "ocid1.vcn.oc1.phx.uniqueid",
              "meta": {
                "e2bf730-ecaa-11e6-8f88-34363bc7c4c0": {
                  "create": 300000000000,
                  "delete": 300000000000,
                  "update": 300000000000
                }
              }
            },
            "tainted": false
          },
          "provider": "provider.oci",
          "type": "oci_core_virtual_network"
        }
      }
    ]
  }
}
```
To view the log for a job

View the log file and note the "message" fields in the sequence of log entries of the log file. You can view the log file for the specified job as either a paged list of entries or in its raw form.

To view the log as a paged list of entries, open a command prompt and run `oci resource-manager job get-job-logs`:

```bash
oci resource-manager job get-job-logs --job-id <job_OCID>
```

To view the log in raw form, open a command prompt and run `oci resource-manager job get-job-logs-content`:

```bash
oci resource-manager job get-job-logs-content --job-id <job_OCID>
```

To import an existing Terraform state file (run an import job)

Open a command prompt and run `oci resource-manager x` to import an existing state file for resources already managed by Terraform:

```bash
oci resource-manager job create-import-tf-state-job --stack-id stack_id --tf-state-file state_file
```

To inspect resources in a compartment

Inspecting resources in a compartment allows you to confirm existence of a resource that you provisioned (by running an apply job) or absence of a resource that you released (by running a destroy job).

Open a command prompt and run the CLI command corresponding to the resources you want to inspect.

For example, run `oci network vcn list` to inspect VCN resources in the specified compartment:

```bash
oci network vcn list --compartment-id <compartment_OCID>
```

To release a stack’s resources (run a destroy job)

**Note:**

We recommend running a destroy job before deleting a stack to release associated resources first. When you delete a stack, its associated state file is also deleted; therefore, you lose track of the state of its associated resources. Cleaning up resources associated with a deleted stack can be difficult without the state file, especially when those resources are spread across multiple compartments. To avoid difficult cleanup later, we recommend that you release associated resources first by running a destroy job.

Open a command prompt and run `oci resource-manager job create-destroy-job` to tear down and cleanup the resources provisioned by the specified stack:

```bash
oci resource-manager job create-destroy-job --stack-id <stack_OCID> --execution-plan-strategy=AUTO_APPROVED
```
To confirm deletion of the resources, inspect resources in the compartment.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage stacks:

- ChangeStackCompartment
- CreateStack
- DeleteStack
- DetectStackDrift
- GetStack
- GetStackTfConfig
- GetStackTfState
- ListResourceDiscoveryServices
- ListStackResourceDriftDetails
- ListStacks
- ListTerraformVersions
- UpdateStack

Use these API operations to manage jobs:

- CancelJob
- CreateJob
- GetJob
- GetJobLogs
- GetJobLogsContent
- GetJobTfConfig
- GetJobTfState
- ListJobs
- UpdateJob

Use these API operations to manage work requests:

- GetWorkRequest
- ListWorkRequestErrors
- ListWorkRequestLogs
- ListWorkRequests

**Managing Private Templates**

This topic describes how to create, edit, and delete private templates for reuse of Terraform configurations.

**Prerequisites**

IAM policies: To manage private templates, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in.

Administrators: For common policies that give groups access to resources in Resource Manager (stacks, jobs, private templates, and configuration source providers), see Policies for Managing Resources Used with Resource Manager on page 2476. For a complete list of Resource Manager permissions, see Details for Resource Manager on page 2336. Policies for managing accessed resource types are also required.
Important:

Policies for managing Oracle Cloud Infrastructure resources are also required for Resource Manager operations that access resources. For example, running an apply job on a stack that includes Compute instances and subnets requires policies that grant you permissions for those resource types, in the compartments where you want to provision the resources. To see examples of policies for managing Oracle Cloud Infrastructure resources, see Common Policies on page 2142.

Using the Console

To create a private template

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Private Templates.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click Create Private Template.
4. On the Create Private Template panel, do the following.
   • Configuration: Select either Folder or Zip File, then either drag and drop your configuration onto the dialog's control or click Browse and navigate to the folder or file location.
   • If needed, edit the default Name provided for your private template. Avoid entering confidential information.
   • Type a Description.
   • (Optional) In Details, type a detailed description of your private template. This text is displayed in the Console page listing templates when the template is expanded.
5. Optionally do one or more of the following:
   • To add an icon, click Show Advanced Options and then either drag and drop your icon file onto the dialog’s Template Icon control or click Browse and navigate to the file location.
     Template icon file requirements: PNG format, 50 KB maximum, 110 x 110 pixels.
     The icon is displayed in the Console page listing templates when the template is expanded.
   • To choose a different compartment for storing your new private template, click Show Advanced Options and then select the compartment you want from Create in Compartment.
   • To tag the template, click Show Advanced Options and add your tag.
6. Click Create.

   Congratulations, your private template is now created. You can now share the private template with anyone in your tenancy that has sufficient permissions.

   For instructions to create a stack from your private template, see the template step.

To create a stack from a private template

This section provides instructions for starting the stack creation process from the detail page for a private template. You can alternatively select a private template from the Create Stack page.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Private Templates.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the private template you want.
4. On the detail page for the selected private template, click Create Stack.
   The Create Stack page appears, populated with information contained in the Terraform configuration for the selected template.
6. Enter a Name for the new stack (or accept the default name provided). Avoid entering confidential information.
7. Optionally enter a **Description**.
8. From the **Create in Compartment** drop-down, select the compartment where you want to create the stack.

   A compartment from the list scope is set by default.
9. Optionally apply tags to the stack.

   If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

10. **Click Next**.

    The **Configure Variables** panel displays variables from the Terraform configuration.

    No variables are listed for the **Existing Compartment** stack origin because no Terraform configuration exists yet.

11. Review the variables and make changes as necessary.

    **Important:**

    Do not add your private key or other confidential information to configuration variables.

12. **Click Next**.
13. In the **Review** panel, verify your stack configuration.
14. **Click Create** to create your stack.

    The stack detail page for the new stack appears.

    To deploy the defined resources, **run an apply job** on your new stack.

**To view private templates**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Private Templates**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

**To edit a private template**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Private Templates**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the private template you want.
4. On the detail page for the selected private template, click **Edit**.
5. In the **Edit Template** panel, update the properties you want.
6. **Click Save**.

**To delete a private template**

1. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Private Templates**.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the Actions icon (three dots), select **Delete Private Template**, and confirm the operation when prompted.

    **Note:**

    You cannot undo this operation.

You can also delete a private template from its detail page. Click the name of the template to display the **Private Template Details** page and then click **Delete**.
Using the CLI

This section provides basic sample CLI commands for managing private templates. For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see CLI Help.

To create a private template from an uploaded file

This section describes how to create a private template from an uploaded configuration file (.zip).

Open a command prompt and run `oci resource-manager template create` to create a private template:

```
oci resource-manager template create --compartment-id <compartment_OCID> --display-name "<friendly_name_for_template>" --description "<description>" --long-description "<long-description>" --logo-file <icon_file_name> --from-json <config_file_name>
```

For example:

```
oci resource-manager stack create --compartment-id ocid1.tenancy.oc1..uniqueid --display-name "My Template" --description "My Default VCN" --long-description "Use this template to provision the default VCN." --logo-file file://mylogo.png --from-json file://myconfig.json
```

To create a stack from a private template

This section describes how to create a stack from a private template.

Open a command prompt and run `oci resource-manager stack create-from-template` to create a stack from a private template:

```
oci resource-manager stack create-from-template --compartment-id <compartment_OCID> --template-id "<template_OCID>"
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage private templates:

- ChangeTemplateCompartment
- CreateTemplate
- DeleteTemplate
- GetTemplate
- GetTemplateLogo
- GetTemplateTfConfig
- ListTemplateCategories
- ListTemplates
- UpdateTemplate

Managing Configuration Source Providers

This topic describes how to create, edit, and delete configuration source providers for remote Terraform configurations.

Prerequisites

IAM policies: To manage configuration source providers, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool.
you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in.

Administrators: For common policies that give groups access to resources in Resource Manager (stacks, jobs, private templates, and configuration source providers), see Policies for Managing Resources Used with Resource Manager on page 2476. For a complete list of Resource Manager permissions, see Details for Resource Manager on page 2336. Policies for managing accessed resource types are also required.

**Important:**

Policies for managing Oracle Cloud Infrastructure resources are also required for Resource Manager operations that access resources. For example, running an apply job on a stack that includes Compute instances and subnets requires policies that grant you permissions for those resource types, in the compartments where you want to provision the resources. To see examples of policies for managing Oracle Cloud Infrastructure resources, see Common Policies on page 2142.

### Prerequisites for connecting to GitHub and GitLab

Following are the prerequisites to connect Oracle Cloud Infrastructure Resource Manager to GitHub and GitLab.

- Your GitHub or GitLab server must be accessible over the Internet by Oracle Cloud Infrastructure IP addresses. (This accessibility requirement does not apply to GitLab.com.)
- Make sure Resource Manager can resolve your GitHub or GitLab URL. Make sure that your GitHub or GitLab server is deployed with a well-known root certificate, such as digicert, so that Oracle Cloud Infrastructure can trust its endpoint.
- Configure your network to allow access from Oracle Cloud Infrastructure IP address ranges. Ensure that you include ranges for all relevant services, including the Oracle Services Network (tag: OSN).
- Enable network ingress rules on the VCN where your GitHub or GitLab server is deployed to allow access from Oracle Cloud Infrastructure IP addresses.
- You must have GitHub or GitLab admin or owner permissions for the repository.
- You must have a Personal Access Token (PAT) to your GitHub or GitLab server. The scope read_api is required for use with Resource Manager. For security, we recommend excluding write_repository scope.

To create a PAT, see the relevant documentation:

- GitHub: https://docs.github.com/en/free-pro-team@latest/github/authenticating-to-github/creating-a-personal-access-token
- GitLab: https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html

- You must have Resource Manager permissions required for your task:
  - To create a configuration source provider, you need manage orm-config-source-providers.
  - To create a stack with an existing configuration source provider, you need manage orm-stacks and read orm-config-source-providers.

For more information, see Policies for Managing Resources Used with Resource Manager on page 2476.

For troubleshooting information, see GitHub and GitLab Connection Issues on page 3624.

### Using the Console

**To create a configuration source provider**

**Important:**

To connect to GitHub or GitLab, you must use a Personal Access Token. See Prerequisites for connecting to GitHub and GitLab on page 3582.

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Configuration Source Providers.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click Create Configuration Source Provider.

4. In the Create Configuration Source Provider panel, do the following.
   - Type a Name for your configuration source provider. Avoid entering confidential information.
   - Type a Description.
   - Select the Compartment where you want to create the configuration source provider.
   - Select the Type of configuration source provider you want. Choose from the following options.
     - GitHub: Supported products
       - GitHub Enterprise
         - GitHub Enterprise Server
         - GitHub Enterprise Cloud
         - GitHub Free for organizations
         - GitHub Free for user accounts
         - GitHub Team
     - GitLab: Supported products
       - GitLab Community Edition
       - GitLab Enterprise Edition
       - GitLab.com
   - Paste the Server URL.

   Example URLs:

<table>
<thead>
<tr>
<th>Product</th>
<th>Example URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>GitHub Enterprise Cloud</td>
<td><a href="https://github.com/org-name">https://github.com/org-name</a></td>
</tr>
<tr>
<td>GitHub Enterprise Server</td>
<td><a href="https://hostname/api/v3">https://hostname/api/v3</a></td>
</tr>
<tr>
<td>GitHub Free for Organization</td>
<td><a href="https://github.com/org-name">https://github.com/org-name</a></td>
</tr>
<tr>
<td>GitHub Free for User Accounts</td>
<td><a href="https://github.com">https://github.com</a></td>
</tr>
<tr>
<td>GitHub team</td>
<td><a href="https://github.com/team-name">https://github.com/team-name</a></td>
</tr>
<tr>
<td>GitLab.com product</td>
<td><a href="https://gitlab.com/">https://gitlab.com/</a></td>
</tr>
<tr>
<td>GitLab installation (relative URL)</td>
<td><a href="https://example.com/gitlab">https://example.com/gitlab</a></td>
</tr>
<tr>
<td>GitLab installation (subdomain)</td>
<td><a href="https://gitlab.example.com/">https://gitlab.example.com/</a></td>
</tr>
</tbody>
</table>

   - Paste the Personal Access Token.
   - To tag the new configuration source provider, click Show Advanced Options and add your tag.

   For troubleshooting information, see GitHub and GitLab Connection Issues on page 3624.

5. Click Create.

To edit a configuration source provider

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Configuration Source Providers.

2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.

3. Click the name of the configuration source provider that you want to edit.

4. Click Edit Configuration Source Provider.

5. In the Edit Configuration Source Provider dialog box, update property values as needed.

   For troubleshooting information, see GitHub and GitLab Connection Issues on page 3624.
6. Click Save.

**To delete a configuration source provider**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A configuration source provider cannot be deleted if it is associated with a stack. To remove the association from the stack, edit the stack.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Configuration Source Providers.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
3. Click the name of the configuration source provider that you want to delete.
4. Click Delete Configuration Source Provider and then confirm the action.

**Using the CLI**

This section provides basic sample CLI commands for managing stacks and jobs. For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see CLI Help.

**To create a configuration source provider**

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To connect to GitHub or GitLab, you must use a Personal Access Token. See Prerequisites for connecting to GitHub and GitLab on page 3582.</td>
</tr>
</tbody>
</table>

Choose the option for the provider type you want:

- **GitHub:**
  
  Open a command prompt and run `resource-manager configuration-source-provider create-github-access-token-provider` to create a GitHub configuration source provider:

  ```
  oci resource-manager stack create-github-access-token-provider --api-endpoint <github_url> --access-token <personal_access_token> --compartment-id <compartment_OCID> --display-name "<friendly_name>" --description "<description>"
  ```

  For example:

  ```
  oci resource-manager stack create-github-access-token-provider --api-endpoint https://api.github.com/ --access-token token --compartment-id ocid1.tenancy.oc1..uniqueid --display-name "My Configuration Source Provider" --description "Department 80"
  ```

- **GitLab:**
  
  Open a command prompt and run `resource-manager configuration-source-provider create-gitlab-access-token-provider` to create a GitLab configuration source provider:

  ```
  oci resource-manager stack create-gitlab-access-token-provider --api-endpoint <gitlab_url> --access-token <personal_access_token> --compartment-id <compartment_OCID> --display-name "<friendly_name>" --description "<description>"
  ```

  For example:

  ```
  oci resource-manager stack create-gitlab-access-token-provider --api-endpoint https://gitlab.com/api/v3/ --access-token token --compartment-id ocid1.tenancy.oc1..uniqueid --display-name "My Configuration Source Provider" --description "Department 80"
  ```
For a complete list of flags and options available for CLI commands, see CLI Help.

**To update a configuration source provider**

Choose the option for the provider type you want:

- **GitHub:**

  Open a command prompt and run `resource-manager configuration-source-provider update-github-access-token-provider` to edit the specified configuration source provider:

  ```bash
  oci resource-manager stack update-github-access-token-provider --configuration-source-provider-id <configuration_source_provider_OCID> --api-endpoint <github_url> --access-token <personal_access_token> --display-name "<friendly_name>" --description "<description>"
  ```

  For example:

  ```bash
  oci resource-manager stack update-github-access-token-provider --configuration-source-provider-id ocid.ormconfigsourceprovider.oc1..uniqueid --description "Department 99"
  ```

- **GitLab:**

  Open a command prompt and run `resource-manager configuration-source-provider update-gitlab-access-token-provider` to edit the specified configuration source provider:

  ```bash
  oci resource-manager stack update-gitlab-access-token-provider --configuration-source-provider-id <configuration_source_provider_OCID> --api-endpoint <gitlab_url> --access-token <personal_access_token> --display-name "<friendly_name>" --description "<description>"
  ```

  For example:

  ```bash
  oci resource-manager stack update-gitlab-access-token-provider --configuration-source-provider-id ocid.ormconfigsourceprovider.oc1..uniqueid --description "Department 99"
  ```

For a complete list of flags and options available for CLI commands, see CLI Help.

**To delete a configuration source provider**

**Note:**

A configuration source provider cannot be deleted if it is associated with a stack. To remove the association from the stack, edit the stack.

Open a command prompt and run `resource-manager configuration-source-provider delete` to delete the specified configuration source provider:

```bash
oci resource-manager configuration-source-provider delete --config-source-provider-id <configuration_source_provider_OCID>
```

For a complete list of flags and options available for CLI commands, see CLI Help.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use these API operations to manage configuration source providers:

- ChangeConfigurationSourceProviderCompartment
- CreateConfigurationSourceProvider
- DeleteConfigurationSourceProvider
- GetConfigurationSourceProvider
- ListConfigurationSourceProviders
- UpdateConfigurationSourceProvider

**Using Remote Exec**

With Resource Manager, you can use Terraform's remote exec functionality to execute scripts or commands on a remote computer. You can also use this technique for other provisioners that require access to the remote resource.

**Prerequisites**

- The location where the script is remotely executed must be an Oracle Cloud Infrastructure resource that has a public IP and supports remote login.
- On Windows, WinRM must be enabled. On Linux or Unix, SSH must be enabled.
- A key pair used for signing API requests, with the public key uploaded to Oracle. For more information on generating and uploading keys, see Required Keys and OCIDs on page 4179.

**Authenticating**

We recommend using one of the following approaches, depending on whether you have access to the Vault service. For more information, see Overview of Vault on page 3952.

**With Vault**

First, use Vault to encrypt your private key. For more information, see Managing Keys on page 3962 and Using Keys on page 3998.

Next, provide the encrypted private key to Resource Manager. You can use the decrypt data source to decrypt it.

The following code sample demonstrates this process.

```hcl
data "oci_kms_decrypted_data" "private_key_decrypted" {
  #Required
  ciphertext = "${file(var.encrypted_private_key_path)}"
  crypto_endpoint = "${var.decrypted_data_crypto_endpoint}"
  key_id = "${var.kms_encryption_key_id}"
}

resource "oci_core_instance" "TFInstance1" {
  availability_domain = "${lookup(data.oci_identity_availability_domains.ADs.availability_domains[var.availability_domain - 1],"name")}"
  compartment_id = "${var.compartment_ocid}"
  display_name = "TFInstance"
  hostname_label = "instance3"
  shape = "${var.instance_shape}"
  subnet_id = "${oci_core_subnet.ExampleSubnet.id}"
  source_details {
    source_type = "image"
    source_id = "${var.instance_image_ocid[var.region]}"
  }
  extended_metadata {
    ssh_authorized_keys = "${var.ssh_public_key}" 
  }
```
Without Vault

If you do not have access to the Vault service, you can dynamically generate a key pair and store them in the state file.

1. Generate a key pair using a TLS resource.
2. When you launch the Compute instance, use the public key from the TLS resource.
3. When you establish the SSH connection, provide the private key.

| Caution: |
| You should not save your private key in your Terraform configuration file because that is not a secure location. |

The following sample demonstrates how to use the TLS private key resource to provision a Compute instance, then perform a remote execution on that instance.

```terraform
resource "null_resource" "remote-exec" {
  connection {
    agent = false
    timeout = "30m"
    host = "${oci_core_instance.TFInstance1.public_ip}"
    user = "${var.opc_user_name}"
    private_key = "${data.oci_kms_decrypted_data.test_decrypted_data.plaintext}"
  }

  inline = [
    "touch ~/IMadeAFile.Right.Here"
  ]
}
```
depends_on = ["oci_core_instance.TFInstance1"]

provisioner "remote-exec" {
    connection {
        agent       = false
        timeout     = "30m"
        host        = "${oci_core_instance.TFInstance1.public_ip}"
        user        = "${var.opc_user_name}"
        private_key = "${tls_private_key.public_private_key_pair.private_key_pem}" 
    }

    inline = ["touch ~/IMadeAFile.Right.Here"]
}

Connection Construct

This example demonstrates how to use a connection construct for remote exec. Terraform uses a number of defaults when connecting to a resource, but these can be overridden using a connection block in either a resource or provisioner. For more information, see Provisioner Connections.

Templates

This topic describes Oracle-provided templates available for Resource Manager.

Templates are Oracle-provided, pre-built Terraform configurations that provision sets of resources used in common scenarios. You can access templates from the Console.

<table>
<thead>
<tr>
<th>Template</th>
<th>Type</th>
<th>Description</th>
<th>Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous Data Warehouse Database</td>
<td>Service</td>
<td>Provision an Autonomous Data Warehouse database</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Autonomous Transaction Processing Database</td>
<td>Service</td>
<td>Provision an Autonomous Transaction Processing database</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Block Volume</td>
<td>Service</td>
<td>Provision a block volume in Oracle Cloud Infrastructure</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Compute Instance</td>
<td>Service</td>
<td>Provision a Compute instance in Oracle Cloud Infrastructure</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Data Science</td>
<td>Service</td>
<td>Provision Data Science and its prerequisites</td>
<td>Launch stack</td>
</tr>
</tbody>
</table>

Note:

Create your own private templates to share with others in the tenancy.

Common uses of templates:

- Test-drive the idea of infrastructure as code.
- Apply proven best practices to your production workflow configuration.
<table>
<thead>
<tr>
<th>Template</th>
<th>Type</th>
<th>Description</th>
<th>Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default VCN</td>
<td>Service</td>
<td>Provision a VCN that includes a default route table, DHCP options, and subnets</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Departmental Data Warehousing</td>
<td>Architecture</td>
<td>Provision Autonomous Data Warehouse and Oracle Analytics Cloud to ingest data from multiple flat-file sources and analyze it.</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Hub-and-Spoke Network Topology</td>
<td>Architecture</td>
<td>Provision a hub-and-spoke network topology in Oracle Cloud Infrastructure</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Oracle Cloud Development Kit</td>
<td>Architecture</td>
<td>Provision a Compute instance with Oracle Cloud Infrastructure developer tools already installed</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Sample E-Commerce Application</td>
<td>Architecture</td>
<td>Deploy a sample e-commerce application using Always Free Oracle Cloud resources</td>
<td>Launch stack</td>
</tr>
<tr>
<td>Subnets</td>
<td>Service</td>
<td>Provision subnets in Oracle Cloud Infrastructure</td>
<td>Launch stack</td>
</tr>
</tbody>
</table>

**Preinstalling the Oracle Cloud Development Kit**

This page describes how to provision a Compute instance with the Oracle Cloud Development Kit preinstalled and ready to use.

**What’s Included**

The Oracle Cloud Development Kit template preinstalls the following Oracle Cloud Infrastructure items on the Compute instance:

- Command Line Interface (CLI)
- Terraform Provider on page 4275
- Ansible (includes OCI Ansible modules)
- The following SDKs:
  - Go
  - Java
  - Python
- Git: Use the provided Git command line tool to access any Git-related version control systems, such as Bitbucket, GitHub, and GitLab.

*Instance principal authorization* is set up for installed items and the provisioned Compute instance. An upgrade script is also included.
Steps for Using the Oracle Cloud Development Kit
To provision an instance with the development kit

1. Launch the Create Stack page for the Oracle Cloud Development Kit template by clicking this button:

   ![Deploy to Oracle Cloud](image)

Alternative steps from the Console

a. Open the navigation menu. Under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.
b. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator.
c. Click **Create Stack**.
d. In the **Create Stack** dialog, click **Template**.
e. Under **Stack Configuration**, click **Select Template** and then select **Oracle Cloud Development Kit**.

2. Follow the prompts to configure and save your new stack

a. In the **Create Stack** dialog, enter a **Name** for the new stack (or accept the default name provided). Avoid entering confidential information.
b. Optionally enter a **Description**.
c. From the **Create in Compartment** drop-down, select the compartment where you want to create the stack. A compartment from the list scope is set by default.
d. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
e. Click **Next**.

The **Configure Variables** panel displays the following variables:

- **Instance Shape**: Select the shape you want to use for the Compute instance.
- **Auto-Generate SSH Key Pair**: Either generates an SSH key pair or allows you to upload a public key.
  - Enabled (selected): Automatically generates an SSH key pair for accessing the instance. The private key is stored in the Terraform state file. You'll use the private key later to connect to the instance.
  
  **Important:**
  Do not use this option in production. The Terraform state file containing the private key is visible to anyone with access to the created stack.
  
  - Disabled (cleared): Allows you to upload a public key. No private key is stored. Keep the corresponding private key in a safe location. You'll use the private key later to connect to the instance.
  
  For instructions on generating SSH key pairs, see **Managing Key Pairs on Linux Instances** on page 693.

- **Compute Instance to Access All Resources at Tenancy Level**: Controls the level used for the **dynamic group policy**, which determines what resources are accessible by users of the Compute instance.
  - Enabled (selected): Tenancy level for access to all resources in the tenancy.
  - Disabled (cleared): Compartment level for access to all resources in the same compartment as the instance.

f. Click **Next**.
g. In the **Review** panel, verify your stack configuration.
h. Click **Create** to create your stack.

The new stack appears in the Stack Details page.
3. Provision the instance by running an apply job on the new stack

   a. On the Stack Details page for your new stack, go to Terraform Actions and select Apply.
   b. In the Apply dialog, review the apply job Name and other settings and update it if needed.
   c. Click Apply.

The new apply job is listed under Jobs. Monitor its status: "Succeeded" indicates that the job has completed. While the job runs, or after it completes, you can download its log file.

Once the instance is provisioned (indicated by a "Succeeded" status for the apply job), installation of the development kit items begins. The installation process takes a few minutes. If you connect to the instance before the installation finishes, then a warning message indicates that the installation is still in process. Once the items are installed on the instance, you can immediately use them.

d. To view the Terraform state file (shows the state of your resources after running the job), click the name of the apply job and then click View State under Resources.

Congratulations! You’ve provisioned a Compute instance with the Oracle Cloud Development Kit already installed and ready to use. You can now connect to the instance and use the development kit.

To connect to your newly created instance

Run the following command:

```
ssh -i <private-key> opc@<compute-instance-public-ip>
```

 `<private-key>` is the private key associated with the instance you provisioned from the stack created using the Oracle Cloud Developer Tools template.

 `<compute-instance-public-ip>` is the IP address of the instance.

To retrieve the associated private key and IP address

1. Go to the Stack Details page for your newly provisioned instance:
   a. Open the navigation menu. Under Solutions and Platform, go to Resource Manager and click Stacks.
   b. Click the name of the stack to display its detail page.
2. Click the Application Information tab.
3. Copy the value for Compute Instance IP Address.
4. For the private key, follow the steps that correspond to the key option you selected while creating your stack:
   - If you enabled Auto-Generate SSH Key Pair, then retrieve the generated private key: Copy the value for Generated Private Key for SSH Access.
   - If you disabled Auto-Generate SSH Key Pair, then reference the full path and name of the file that contains the private key corresponding to the public key that you uploaded while creating the stack.

   **Note:**

   When you connect to your instance, the private key file permissions are validated. For security, your private key must be accessible by the owner only; otherwise, you won’t be allowed to connect to the instance. (Owner write permissions are required for you to add the private key to the file.)

   For Unix or Linux, use the command `chmod 600 (-rw-------)`.

For general information about connecting to Compute instances, see Connecting to an Instance on page 733.

Once connected to your instance, you can use the installed development kit.

To use the installed development kit

See the following examples:

- CLI: See Using the CLI on page 4207
  Usage: See Easy Provisioning, CLI Updates
Resource Manager

• **Terraform Provider**
  Usage: See Terraform Provider on page 4275.
• **Ansible** (includes OCI Ansible modules)
  Usage: See Writing a Sample Playbook on page 4332.
• **SDKs:**
  • Go
  • Java
    Usage: See Concepts on page 4233.
  • Python
    Setup and usage: See Client-Side Encryption on page 4244.
    Setup and usage for open source SDKs: See Open Source SDKs
  • Git: Use the provided Git command line tool to access any Git-related version control systems, such as Bitbucket, GitHub, and GitLab.
    Usage: To get help on using Git, access the terminal on your new Compute instance and run `git --help`.

To upgrade the installed development kit

1. Connect to the instance that you provisioned from the Oracle Cloud Development Kit template.
2. Run the upgrade command:

```
update-kit.sh
```

Preconfigured Authorization

Instance principal authorization is set up for installed development kit items and the provisioned Compute instance. The template provides the following preconfiguration:

• A **dynamic group**
• An **IAM policy**, with all resource access determined by stack configuration (either tenancy or compartment level)
• Environment variables set in `.bashrc` on the Compute instance for CLI, Terraform, and Ansible

For more information about instance principal authorization, see Calling Services from an Instance on page 2410.

Using the Deploy to Oracle Cloud Button

This page describes the advanced topic of constructing a URL for **Deploy to Oracle Cloud** button.

When properly linked, this button provides a direct option for your users to create stacks with your Terraform configuration.

![Deploy to Oracle Cloud Button](image)

This button takes a user directly to the **Create Stack** page in the Oracle Cloud Infrastructure Console. The button is linked to a Terraform configuration file package that you specify, so the Terraform configuration is already selected for the user when they **create the stack**. You can store Terraform configuration files in a supported provider.

Example of Functioning Deploy Button

The following **Deploy to Oracle Cloud** button is configured to launch the template from [https://github.com/oracle-quickstart/oci-cloudnative](https://github.com/oracle-quickstart/oci-cloudnative).
Supported Providers

The following providers are supported for forming package URLs to use with the **Deploy to Oracle Cloud** button:

- **GitHub**
  
  Example package URL 1: Direct: https://github.com/myrepo/mydirectory/master.zip
  
  Example package URL 2: Release: https://github.com/myrepo/mydirectory/0.0.1.zip
  
  To get the .zip URL to a release in GitHub, see [https://docs.github.com/en/free-pro-team@latest/github/administering-a-repository/linking-to-releases](https://docs.github.com/en/free-pro-team@latest/github/administering-a-repository/linking-to-releases).

- **GitLab**
  
  Example package URL 1: Direct: https://gitlab.com/myrepo/mydirectory/master.zip
  
  Example package URL 2: Release: https://gitlab.com/myrepo/mydirectory/0.0.1.zip

- **Object Storage (pre-authenticated request URL)**
  
  Example package URL: https://objectstorage.region.oraclecloud.com/p/encrypted-string/n/object-storage-namespace/b/bucket/o/filename

To display the linked deploy button

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that your Terraform configuration file is valid. See <a href="https://docs.oracle.com/en/iaas/Content/Terraform/TerraformConfigurations.htm">Authoring Configurations</a> on page 4277 and <a href="https://docs.oracle.com/en/iaas/Content/Terraform/TerraformConfigurations.htm">Terraform Configurations for Resource Manager</a> on page 3594.</td>
</tr>
</tbody>
</table>

You can display the linked **Deploy to Oracle Cloud** button on repository pages and other web pages.

**Markdown code**

To display the **Deploy to Oracle Cloud** button on a repository page, add the following Markdown code to a README.md file.

```markdown
```

<package-url> is the URL for the .zip file to a Terraform configuration that is stored in a supported provider.

Example Markdown code with a package URL from GitHub:

```markdown
```

**HTML code**

To display the **Deploy to Oracle Cloud** button on a web page, add the following HTML code.

```html
<a href="https://cloud.oracle.com/resourcemanager/stacks/create?zipUrl=<package-url>"
   target="_blank"
   rel="noopener noreferrer">Deploy to Oracle Cloud</a>
```
To create a stack from the linked deploy button

1. Click **Deploy to Oracle Cloud** (the deploy button linked to the Terraform configuration).
2. If you are not yet signed in to the Oracle Cloud Infrastructure Console, then sign in. See [Signing In to the Console](#) on page 41.
   
   The **Create Stack** dialog appears with the selected package identified.
3. Enter a **Name** for the new stack (or accept the default name provided). Avoid entering confidential information.
4. Optionally enter a **Description**.
5. From the **Create in Compartment** drop-down, select the compartment where you want to create the stack.
   
   A compartment from the list scope is set by default.
6. Select a **Terraform Version**.
   
   **Note:**
   
   Terraform versions are not backward compatible.
7. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
8. Click **Next**.
   
   The **Configure Variables** panel displays variables from the selected Terraform configuration file.
9. Review the variables and make changes as necessary.
   
   **Important:**
   
   Do not add your private key or other confidential information to configuration variables.
10. Click **Next**.
11. In the **Review** panel, verify your stack configuration.
12. Click **Create** to create your stack.

To deploy the defined resources, run an apply job on your new stack.

**Terraform Configurations for Resource Manager**

This topic describes requirements and recommendations for Terraform configurations used with Resource Manager. For basic information about Terraform configurations, see [Authoring Configurations](#) on page 4277. For instructions on using configurations with stacks and jobs, see [Managing Stacks and Jobs](#) on page 3557.
You can store your Terraform configuration file locally or remotely, using a source code control system. With remote storage, any job running on the associated stack automatically uses the latest version of your configuration. For more information about remotely storing your file, see Managing Configuration Source Providers on page 3581.

In addition to writing your own Terraform configuration file, you also have the option to generate a Terraform configuration from either an existing compartment using resource discovery or a sample template.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not provide user credentials or other confidential information in your Terraform configurations.</td>
</tr>
</tbody>
</table>

Requirements

Terraform configuration files used with Resource Manager must meet the following requirements.

Terraform Provider

When using Resource Manager, the region field in the provider "oci" block is the only required field. For more information about defining providers, see Configuration File Requirements on page 4278.

File Structure

Resource Manager requires the following file structure for the Terraform configuration:

- The working directory must contain at least one .tf file. The working directory cannot contain a .terraform directory.
- The working directory is the path from which to run Terraform. By default, the working directory is the root directory of your configuration (for an uploaded configuration, the root of your .zip file). When using the API, you can specify a different location for the working directory by setting the workingDirectory parameter.
- The configuration must follow guidelines specified in Authoring Configurations on page 4277.
- No Terraform state files (.tfstate) can exist in the configuration.
- If you plan to upload the configuration locally, then bundle all files into a .zip file.

Modules

Resource Manager supports the following Terraform module sources:

- Local paths
- Terraform Registry
- GitHub
- Bitbucket
- Generic Git repositories
- HTTP URLs

Variables

We recommend using a schema document with your Terraform configuration to facilitate user entry in the Oracle Cloud Infrastructure Console.

Resource Manager does not have requirements for variables in Terraform configurations. Resource Manager supports the native Terraform behavior for handling variables. Terraform sets variables from your variable definitions that use supported type constraints.

Example Terraform Configuration for Resource Manager

The following example shows a Terraform configuration that is contained in a single file. This basic sample defines just one Terraform provider, one Oracle Cloud Infrastructure resource, and a set of variables.

```terraform
variable "compartment_ocid" {}
```
More often, Terraform configurations consist of two or more files bundled together (for an uploaded configuration, the files would be bundled in a .zip file). To see more complex, multi-file Terraform configurations, explore the examples at the Oracle Cloud Infrastructure GitHub: terraform-provider-oci/docs/examples.

Schema Documents

Schema documents are recommended for Terraform configurations when using Resource Manager. Including a schema document allows you to facilitate variable entry in the Oracle Cloud Infrastructure Console by surfacing SSH key controls and by naming, grouping, dynamically prepopulating values, and more, including defining text in the Application Information tab displayed for a created stack.

Requirements for Schema Documents

Schema documents for Resource Manager have the following requirements:

- YAML format.
- Placement under the root folder of the Resource Manager Terraform configuration. (By default, the schema document assumes that the root folder is the working directory.)

Supported Types (Dynamic Prepopulation and Controls)

This section lists the types supported by Resource Manager for dynamic prepopulation and controls.

<table>
<thead>
<tr>
<th>Type (rendered as a dynamically prepopulated dropdown field unless otherwise noted)</th>
<th>Resource identifier</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>oci:core:image:id</td>
<td>Image OCID</td>
<td>Mandatory dependsOn field: compartmentId</td>
</tr>
<tr>
<td>oci:core:instanceshape:name</td>
<td>Instance shape name</td>
<td></td>
</tr>
<tr>
<td>oci:core:ssh:publickey</td>
<td>--</td>
<td>Surfaces a control for adding one or more public SSH keys by dropping files or pasting key values. For more information, see SSH key control.</td>
</tr>
<tr>
<td>oci:core:subnet:id</td>
<td>Subnet OCID</td>
<td></td>
</tr>
<tr>
<td>oci:core:vcn:id</td>
<td>VCN OCID</td>
<td></td>
</tr>
<tr>
<td>oci:database:autonomouscontainerdatabase:id</td>
<td>Autonomous container database OCID</td>
<td></td>
</tr>
<tr>
<td>oci:database:autonomousdatabase:id</td>
<td>Autonomous database OCID</td>
<td></td>
</tr>
<tr>
<td>oci:database:database:id</td>
<td>Database OCID</td>
<td></td>
</tr>
<tr>
<td>oci:database:dbhome:id</td>
<td>DB home OCID</td>
<td></td>
</tr>
<tr>
<td>oci:database:dbsystem:id</td>
<td>DB system OCID</td>
<td></td>
</tr>
<tr>
<td>Type (rendered as a dynamically prepopulated dropdown field unless otherwise noted)</td>
<td>Resource identifier</td>
<td>Comments</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>oci:identity:availabilitydomain:name</td>
<td>Availability domain name</td>
<td></td>
</tr>
<tr>
<td>oci:identity:compartment:id</td>
<td>Compartment OCID</td>
<td></td>
</tr>
<tr>
<td>oci:identity:faultdomain:name</td>
<td>Fault domain name</td>
<td></td>
</tr>
<tr>
<td>oci:identity:region:name</td>
<td>Region name</td>
<td></td>
</tr>
<tr>
<td>oci:kms:vault:id</td>
<td>Vault OCID</td>
<td></td>
</tr>
</tbody>
</table>

**Meta Schema for Validation**

Use the following meta schema file to confirm that your schema document is using supported variable types.

**Meta Schema**

```json
# Meta JSON Schema.
#
# This is used to validate the Schema file when the package is uploaded/loaded into Resource Manager.
# For marketplace, it is also used to validate the package when the package artifact is created in Partner Portal.
#
# NOTE: additionalProperties are set to true explicitly even though this is the default. It must be set to true in
# cases where we use the allOf. This is a quirk of JSON Schema. During validation, allOf means it has to match all of
# the individual definitions separately. It doesn't mean it has to match a Union of the individual definitions. This
# is a known issue with JSON Schema.
title: Schema
type: object
required:
  - variables
  - schemaVersion
additionalProperties: true
properties:
title:
  type: string
description:
  type: string
stackDescription:
  type: string
packageVersion:
  type: string
version:
  type: string
schemaVersion:
  type: string
enum:
  - 1.0.0
  - 1.1.0
locale:
  $ref: '#/definitions/locale'
logoUrl:
  $ref: '#/definitions/url'
source:
  $ref: '#/definitions/source'
informationalText:
  type: string
```
instructions:
  type: string
troubleshooting:
  type: string
allowViewState:
  type: boolean
variables:
  $ref: '#/definitions/variables'
# Deprecated - use variableGroups instead
groupings:
  $ref: '#/definitions/variableGroups'
variableGroups:
  $ref: '#/definitions/variableGroups'
outputs:
  $ref: '#/definitions/outputs'
outputGroups:
  $ref: '#/definitions/outputGroups'
primaryOutputButton:
  type: string
  format: variablereference
definitions:
  source:
    type: object
    properties:
      type:
        type: enum:
        - marketplace
        - quickstart
        - web
      reference:
        type:
        - string
        - number
        additionalProperties: false
variableGroups:
  type: array
  items:
    $ref: '#/definitions/variableGroup'
variableGroup:
  type: object
  required:
  - title
  - variables
  properties:
    title:
      type: string
    variables:
      type: array
      items:
        type: string
        format: variablereference
        visible:
          $ref: '#/definitions/booleanStatement'
        additionalProperties: true
locale:
  enum:
  - en
  default: en
url:
type: string
  pattern: ^https?:\/(www\.)?[-a-zA-Z0-9@:%_.\+~#\=]{2,256}\.[a-z]\
  (2,4)\b([-a-zA-Z0-9@:%\._\+~#\?&//=]*)$

ocid:
  type: string
  pattern: ^ocid1\.(\[a-z0-9-\]{1,32})\.(\[a-z0-9-\]\{1,15\})\.(\[a-z0-9\]
  \{0,24\})\.(\[a-z0-9\]\{60\})$

variables:  
  type: object
  additionalProperties: 
    $ref: '#/definitions/variable'

variable:  
  oneOf: 
    - $ref: '#/definitions/staticVariable'
    - $ref: '#/definitions/dynamicVariable'

baseVariable:  
  type: object
  properties: 
    title: 
      type: string
      minLength: 1
    description: 
      type: string
    required: 
      type: boolean
      default: false
    visible: 
      $ref: '#/definitions/booleanStatement'

booleanStatement:  
  oneOf: 
    - type: boolean
    - type: string
    - $ref: '#/definitions/equality'
    - $ref: '#/definitions/booleanOr'
    - $ref: '#/definitions/booleanAnd'
    - $ref: '#/definitions/booleanNot'

equality:  
  type: object
  properties: 
    eq: 
      type: array
      items: 
        - type: [string, number]
        - type: [string, number]
      additionalItems: false
      additionalProperties: false

booleanOr: 
  type: object
  properties: 
    or: 
      type: array
      items: 
        - $ref: '#/definitions/booleanStatement'
        - $ref: '#/definitions/booleanStatement'
      additionalItems: false
      additionalProperties: false
booleanAnd:
  type: object
  properties:
    and:
      type: array
      items:
        - $ref: '#/definitions/booleanStatement'
        - $ref: '#/definitions/booleanStatement'
      additionalItems: false
      additionalProperties: false

booleanNot:
  type: object
  properties:
    not:
      type: array
      items:
        - $ref: '#/definitions/booleanStatement'
      additionalItems: false
      additionalProperties: false

dependsOnCompartment:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required:
      - dependsOn
    properties:
      dependsOn:
        type: object
        required:
          - compartmentId
        properties:
          compartmentId:
            type: string
            format: variablereference
            additionalProperties: false
            additionalProperties: true

staticVariable:
  oneOf:
    - $ref: '#/definitions/arrayVariable'
    - $ref: '#/definitions/booleanVariable'
    - $ref: '#/definitions/enumVariable'
    - $ref: '#/definitions/integerVariable'
    - $ref: '#/definitions/numberVariable'
    - $ref: '#/definitions/stringVariable'
    - $ref: '#/definitions/passwordVariable'
    - $ref: '#/definitions/datetimeVariable'

dynamicVariable:
  oneOf:
    - $ref: '#/definitions/imageVariable'
    - $ref: '#/definitions/instanceShapeVariable'
    - $ref: '#/definitions/subnetVariable'
    - $ref: '#/definitions/vcnVariable'
    - $ref: '#/definitions/availabilityDomainVariable'
    - $ref: '#/definitions/compartmentVariable'
    - $ref: '#/definitions/faultDomainVariable'
    - $ref: '#/definitions/regionVariable'
    - $ref: '#/definitions/dbSystemVariable'
    - $ref: '#/definitions/dbHomeVariable'
    - $ref: '#/definitions/dbHomeVersionVariable'
    - $ref: '#/definitions/databaseVariable'
- $ref: '#/definitions/autonomousDatabaseVariable'
- $ref: '#/definitions/autonomousContainerDBVariable'
- $ref: '#/definitions/kmsVaultVariable'

nonNegativeInteger:
  type: integer
  minimum: 0

nonNegativeIntegerDefault0:
  allOf:
    - $ref: '#/definitions/nonNegativeInteger'
    - default: 0

arrayVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required: [type]
    properties:
      type:
        enum: [array]
      items:
        $ref: '#/definitions/variable'
      maxItems:
        $ref: '#/definitions/nonNegativeInteger'
      minItems:
        $ref: '#/definitions/nonNegativeIntegerDefault0'
      uniqueItems:
        type: boolean
        default: false
      contains:
        $ref: '#/definitions/variable'
      additionalProperties: true

booleanVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required: [type]
    properties:
      type:
        enum: [boolean]
      default:
        $ref: '#/definitions/booleanStatement'
      default: false
    additionalProperties: true

enumVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required: [type]
    properties:
      type:
        enum: [enum]
      enum:
        type: array
      items:
        type: string
      default:
        $ref: '#/definitions/booleanStatement'
    additionalProperties: true

integerVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required: [type]
properties:
  type:
    enum: [integer]
  default:
    type: integer
  multipleOf:
    type: number
    exclusiveMinimum: 0
  minimum:
    type: number
  maximum:
    type: number
  exclusiveMinimum:
    type: number
  exclusiveMaximum:
    type: number
  additionalProperties: true

numberVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required: [type]
    properties:
      type:
        enum: [number]
      default:
        type: number
      multipleOf:
        type: number
        exclusiveMinimum: 0
      minimum:
        type: number
      maximum:
        type: number
      exclusiveMinimum:
        type: number
      exclusiveMaximum:
        type: number
      additionalProperties: true

stringVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required: [type]
    properties:
      type:
        enum: [string]
      default:
        $ref: '#/definitions/booleanStatement'
      pattern:
        type: string
      maxLength:
        $ref: '#/definitions/nonNegativeInteger'
      minLength:
        $ref: '#/definitions/nonNegativeIntegerDefault0'
      additionalProperties: true

passwordVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required: [type]
    properties:
      type:
        enum: [password]
default:
  $ref: '#/definitions/booleanStatement'
confirmation:
  $ref: '#/definitions/booleanStatement'
additionalProperties: true

datetimeVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required: [type]
    properties:
      type:
        enum: [datetime]
      default: $ref: '#/definitions/booleanStatement'
    additionalProperties: true

imageVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required:
    - type
    - dependsOn
    properties:
      type:
        enum: [oci:core:image:id]
      pattern:
        type: string
      dependsOn:
        type: object
        required:
        - compartmentId
        properties:
          compartmentId:
            type: string
            format: variablereference
          shape:
            type: string
            format: variablereference
          operatingSystem:
            type: string
            format: variablereference
          operatingSystemVersion:
            type: string
            format: variablereference
      additionalProperties: false
  additionalProperties: true

instanceShapeVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required:
    - type
    - dependsOn
    properties:
      type:
        enum: [oci:core:instanceshape:name]
      pattern:
        type: string
      dependsOn:
        type: object
        required:
- compartmentId
  properties:
    imageId:
      type: string
      format: variablereference
    compartmentId:
      type: string
      format: variablereference
    additionalProperties: false
    additionalProperties: true

subnetVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
  - required:
    - type
    - dependsOn
  properties:
    type:
      enum: [oci:core:subnet:id]
    dependsOn:
      type: object
      required:
      - vcnId
      - compartmentId
  properties:
    vcnId:
      type: string
      format: variablereference
    compartmentId:
      type: string
      format: variablereference
    hidePublicSubnet:
      $ref: '#/definitions/booleanStatement'
    hidePrivateSubnet:
      $ref: '#/definitions/booleanStatement'
    hideRegionalSubnet:
      $ref: '#/definitions/booleanStatement'
    hideAdSubnet:
      $ref: '#/definitions/booleanStatement'
    additionalProperties: false
    additionalProperties: true

vcnVariable:
  allOf:
  - $ref: '#/definitions/dependsOnCompartment'
  - required: [type]
  properties:
    type:
      enum: [oci:core:vcn:id]
    additionalProperties: true

availabilityDomainVariable:
  allOf:
  - $ref: '#/definitions/dependsOnCompartment'
  - required: [type]
  properties:
    type:
      enum: [oci:identity:availabilitydomain:name]
    additionalProperties: true

compartmentVariable:
  allOf:
  - $ref: '#/definitions/baseVariable'
- required: [type]
  properties:
    type:
      enum: [oci:identity:compartment:id]
      default:
        $ref: '#/definitions/booleanStatement'
    additionalProperties: true

faultDomainVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required:
      - type
      - dependsOn
    properties:
      type:
        enum: [oci:identity:faultdomain:name]
      dependsOn:
        type: object
        required:
          - compartmentId
          - availabilityDomainName
        properties:
          compartmentId:
            type: string
            format: variablereference
          availabilityDomainName:
            type: string
            format: variablereference
            additionalProperties: false
      additionalProperties: true

regionVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required: [type]
      properties:
        type:
          enum: [oci:identity:region:name]
        default:
          $ref: '#/definitions/booleanStatement'
          default: ${session.region}
      additionalProperties: true

dbSystemVariable:
  allOf:
    - $ref: '#/definitions/dependsOnCompartment'
    - required: [type]
      properties:
        type:
          enum: [oci:database:dbsystem:id]
      additionalProperties: true

dbHomeVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required:
      - type
      - dependsOn
    properties:
      type:
        enum: [oci:database:dbhome:id]
      dependsOn:
type: object
required:
  - dbSystemId
  - compartmentId
properties:
dbSystemId:
type: string
format: variablereference
compartmentId:
type: string
format: variablereference
additionalProperties: false
additionalProperties: true
dbHomeVersionVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required:
      - type
      - dependsOn
    properties:
type:
  enum: [oci:database:dbhome:dbversion]
dependsOn:
type: object
required:
  - dbHomeId
properties:
dbHomeId:
type: string
format: variablereference
additionalProperties: false
additionalProperties: true
databaseVariable:
  allOf:
    - $ref: '#/definitions/baseVariable'
    - required:
      - type
      - dependsOn
    properties:
type:
  enum: [oci:database:database:id]
dependsOn:
type: object
required:
  - dbHomeId
  - compartmentId
properties:
dbHomeId:
type: string
format: variablereference
compartmentId:
type: string
format: variablereference
additionalProperties: false
additionalProperties: true
autonomousDatabaseVariable:
  allOf:
    - $ref: '#/definitions/dependsOnCompartment'
    - required: [type]
properties:
type:
enum: [oci:database:autonomousdatabase:id]
additionalProperties: true

autonomousContainerDBVariable:
  allOf:
  - $ref: '#/definitions/dependsOnCompartment'
  - required: [type]
    properties:
      type:
        enum: [oci:database:autonomouscontainerdatabase:id]
        additionalProperties: true

kmsVaultVariable:
  allOf:
  - $ref: '#/definitions/dependsOnCompartment'
  - required: [type]
    properties:
      type:
        enum: [oci:kms:vault:id]
        additionalProperties: true

sshPublicKeyVariable:
  allOf:
  - $ref: "#/definitions/baseVariable"
  - required: [type]
    properties:
      type:
        enum: [oci:core:ssh:publickey]
        additionalProperties: true

outputs:
  type: object
  additionalProperties:
    $ref: '#/definitions/output'

output:
  oneOf:
  - $ref: '#/definitions/booleanOutput'
  - $ref: '#/definitions/numberOutput'
  - $ref: '#/definitions/stringOutput'
  - $ref: '#/definitions/copyableStringOutput'
  - $ref: '#/definitions/linkOutput'
  - $ref: '#/definitions/ocidOutput'
  - $ref: '#/definitions/mapOutput'
  - $ref: '#/definitions/jsonOutput'
  - $ref: '#/definitions/listOutput'
  - $ref: '#/definitions/csvOutput'

outputGroups:
  type: array
  items:
    $ref: '#/definitions/outputGroup'

outputGroup:
  type: object
  required:
    - title
    - outputs
  properties:
    title:
      type: string
    outputs:
      type: array
      items:
type: string
additionalProperties: true

baseOutput:
  type: object
  properties:
    title:
      type: string
    description:
      type: string
    sensitive:
      type: boolean
      default: false
    format:
      type: string
    visible:
      type: boolean
      default: true
  additionalProperties: true

booleanOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [boolean]
        value:
          type: boolean
    additionalProperties: true

numberOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [number]
        value:
          type: number
    additionalProperties: true

stringOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [string]
        value:
          type: string
    additionalProperties: true

copyableStringOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [copyableString]
        value:
          type: string
    additionalProperties: true
mapOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [map]
        value:
          type: object
        additionalProperties: true

jsonOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [json]
        value:
          type: object
        additionalProperties: true

listOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [list]
        value:
          type: array
        additionalProperties: true

csvOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [csv]
        value:
          type: array
        additionalProperties: true

linkOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
        type:
          enum: [link]
        displayText:
          type: string
          minLength: 3
          maxLength: 45
        value:
          $ref: '#/definitions/url'
        additionalProperties: true

ocidOutput:
  allOf:
    - $ref: '#/definitions/baseOutput'
    - required: [type]
      properties:
Example Schema Document

Following is an example schema document.

Example

```
# Title shown in Application Information tab.
title: Sample input variable schema
# Sub Title shown in Application Information tab.
description: Sample description...
informationalText: Sample informational text to display in tab...
schemaVersion: 1.1.0
version: "20190304"

# URL of Logo Icon used on Application Information tab. Logo must be 130x130 pixels.
# (Optional)
logoUrl: https://cloudmarketplace.oracle.com/marketplace/content?
contentId=53066708

# Used in Application Information tab to Hyperlink Title and Logo to the Marketplace
# Listing.
# Also used to link to Listing Usage section for "View Instructions".
# (Optional) If it is missing, Application Information uses the "marketplace-listing-id" tag for the same purpose.
source:
  type: marketplace
  reference: 16132843

locale: "en"
variableGroups:
  - title: "Node Configuration"
    variables:
      - targetCompartment
      - ${nodeCount}
      - ${nodeShapes}
      - ${availability}
  - title: "Application Details"
    variables:
      - ${username}
      - ${password}
      - ${dnsServers}
  - title: "Subnet"
    variables:
      - ${vcnCompartment}
      - ${myVcn}
      - ${subnetCompartment}
      - ${mySubnet}
      - ${mySubnetWithFilter}
      - ${hide_public_subnet}
      - ${hide_private_subnet}
      - ${hide_regional_subnet}
      - ${hide_ad_subnet}
  - title: "Database"
    variables:
      - ${dbCompartment}
      - ${myDbSystem}
```
- `${myDbHome}`
- `${myDb}`
- `${myAutonomousDB}`
- title: "Advanced"
  variables:
  - `${myImageId}`
  - `${myShape}`
  - `${myCompatibleShape}`
  visible: true
- title: "Hidden"
  variables:
  - `${myRegion}`
  visible: false
- title: "Existing Vcn"
  variables:
  - `${myVcn}`
  visible:
    or:
      - `${useExistingVcn}`
      - and:
        - and:
          - true
          - true
        - not:
          - false
- title: "Password can't be 'password'!"
  variables:
  - `${password}`
- title: "Complex Conditional Section"
  variables:
  - `${myVcn}`
  visible:
    or:
      - `${useExistingVcn}`
      - and:
        - and:
          - true
          - true
        - not:
          - false
- title: "Equality Conditional Section"
  variables:
  - `${myVcn}`
  visible:
    eq:
      - `${objectStorageTier}`
      - standard

variables:
  # string field
  username:
    type: string
    minLength: 1
    maxLength: 255
    pattern: "^[a-z][a-zA-Z0-9]+$"
  # title is used as the label if present
title: Username
  # description used as the tooltip if present
description: Enter your username
default: admin
required: true

# password field
password:
description: Really Bad Password Field
type: password
pattern: "^[a-zA-Z]{1,8}$"
required: true

# integer field
defineCount:
  type: integer
description: Number of Nodes
minimum: 3
maximum: 12
multipleOf: 3

# non-integer number field
availability:
  type: number
default: 99.7
maximum: 100
minimum: 0

# string enum
objectStorageTier:
  type: enum
enum:
  - archive
  - standard

# input a list, each element must be an ip addresses
defineServer:
  type: array
  items:
    type: string
    pattern: "^\(?:(?:25[0-5]|2[0-4]\.[0-9]|1\?[0-9]\.[0-9])\.)\.(?:25[0-5]|2[0-4]\.[0-9]|1\?[0-9]\.[0-9])\)\(\?\:\?\:\?\:[0-9]\-[5]\)\|2\-[0-4]\|[0-9]\|[01]\?[0-9]\-[0-9]\)?\.|1\?[0-9]\-[0-9]\)?$"
  minItems: 1
  uniqueItems: true
default: [ 8.8.8.8, 8.8.4.4 ]

# datetime picker
defineDate:
  type: datetime

# compartmentId dynamic dropdown, targetCompartment present in input variables
targetCompartment:
  type: oci:identity:compartment:id

# subnet picker
useExistingVcn:
  type: boolean

vcnCompartment:
  type: oci:identity:compartment:id
  visible: ${useExistingVcn}

myVcn:
  type: oci:core:vcn:id
  dependsOn:
    compartmentId: ${vcnCompartment}
  visible:
  or:
    - ${useExistingVcn}
- and:
  - and:
    - true
    - true
    - not:
      - false

subnetCompartment:
  type: oci:identity:compartment:id
  visible: ${useExistingVcn}

mySubnet:
  type: oci:core:subnet:id
  dependsOn:
    compartmentId: ${subnetCompartment}
    vcnId: ${myVcn}
  visible: ${useExistingVcn}

mySubnetWithFilter:
  type: oci:core:subnet:id
  dependsOn:
    compartmentId: ${subnetCompartment}
    vcnId: ${myVcn}
    hidePublicSubnet: ${hide_public_subnet}
    hidePrivateSubnet: ${hide_private_subnet}
    hideRegionalSubnet: ${hide_regional_subnet}
    hideAdSubnet: ${hide_ad_subnet}
  visible: ${useExistingVcn}

hide_public_subnet:
  type: boolean
  default: false

hide_private_subnet:
  type: boolean
  default: false

hide_regional_subnet:
  type: boolean
  default: false

hide_ad_subnet:
  type: boolean
  default: false

myRegion:
  type: oci:identity:region:name
  visible: false

myImageId:
  type: oci:core:image:id
  dependsOn:
    compartmentId: ${targetCompartment}

myShape:
  type: oci:core:instanceshape:name
  dependsOn:
    compartmentId: ${targetCompartment}

myCompatibleShape:
  type: oci:core:instanceshape:name
  dependsOn:
    compartmentId: ${targetCompartment}
    imageId: ${myImageId}
visible:
  or:
   - ${useExistingVcn}
   - and:
     - and:
       - true
       - true
       - not:
         - false

myAvailabilityDomain:
  type: oci:identity:availabilitydomain:name
  dependsOn:
    compartmentId: ${targetCompartment}
  visible: complexExpression

myFaultDomain:
  type: oci:identity:faultdomain:name
  dependsOn:
    compartmentId: ${targetCompartment}
    availabilityDomainName: ${myAvailabilityDomain}

dbCompartment:
  type: oci:identity:compartment:id

myDbSystem:
  type: oci:database:dbsystem:id
  dependsOn:
    compartmentId: ${dbCompartment}

myDbHome:
  type: oci:database:dbhome:id
  dependsOn:
    dbSystemId: ${myDbSystem}
    compartmentId: ${dbCompartment}

myDbHomeVersion:
  type: oci:database:dbhome:dbversion
  dependsOn:
    dbHomeId: ${myDbHome}

myDb:
  type: oci:database:database:id
  dependsOn:
    dbHomeId: ${myDbHome}
    compartmentId: ${dbCompartment}

myAutonomousDB:
  type: oci:database:autonomousdatabase:id
  dependsOn:
    compartmentId: ${dbCompartment}

# Used to present outputs with more refinement on the Application
# Information tab.
# The Application Information tab is only shown if the schema has a "title",
# "description", and at least one output in this "outputs" section.
#
# type:
# - boolean
# - string
# - number
# - link - contains url that can be hyperlinked. If type is not specified
#   and the
# value is a proper url, this type is assumed.
#ócíd - contains an OCID. An attempt is made to hyperlink it to the designated resource in the console.
#csv - synonym for list. Array of values converted to a comma separated list.
#json - synonym for map. Map of key / values converted to JSON.
#list - array of values converted to a comma separated list.
#map - map of key / values converted to JSON.

#displayText: used in links to give text displayed instead of value
#title: friendly label
#visible: if false, this output is not shown in the outputs section of Application Information.

It can still be used as the `primaryOutputButton`.

```yaml
outputs:
  controlCenterUrl:
    type: link
    title: Control Center
    displayText: Control Center
    visible: false

  schemaRegistryUrl:
    type: link
    title: Schema Registry
    displayText: Schema Registry

  schemaRegistryPublicIps:
    type: csv
    title: Public IPs

  schemaRegistryLoadBalancer:
    type: ocid
    title: Load Balancer

  brokerPublicIps:
    type: csv

  connectUrl:
    type: link
    title: Connect
    displayText: Connect

  connectPublicIps:
    type: csv
    title: Public IPs

  restUrl:
    type: link
    title: Rest API
```

#primaryOutputButton is a reference to a link output that creates a primary button on the Application Information tab.
(Optional) if not provided, no primary button is shown. Also if the output referenced is not a link output, no button is shown.

```
primaryOutputButton: ${controlCenterUrl}
```

# Used to group Outputs. Any outputs not included in these defined groups, are included in a default group labelled "Outputs".
(Optional) if not groups are given, outputs are not grouped at all.

```
outputGroups:
  - title: Schema Registry
```
How to Control Console Items

This section provides instructions and examples for controlling the display of stack variables and stack details page items in the Oracle Cloud Infrastructure Console for stacks created from your Terraform configuration file. Using a schema document, you can define how variables look and behave during stack creation and what text is displayed in the Application Information tab for a created stack.

Following are Console display items that are controlled by the schema document.

Field label and description

To render a field label and description for a variable:

• Add the lines `title: <field_label>` and `description: <field_description>`.

Example image for a variable field label and description:

![Application Name](image)

Example declaration for a variable field label and description:

```yaml
functions_app_name:
  type: string
  # field label, displayed above field
title: "Application Name"
  # field description, displayed below field
description: "Do not use spaces."
```

Default value

To render a variable with a default value:

• Add the line `default: <default-value>`.

Example image for a variable with a default value:

![DataScienceApp](image)

Example declaration for a check box variable:

```yaml
functions_app_name:
  type: string
  title: "Application Name"
  description: "Do not use spaces."
  required: true
  # provide a default value
```
Group and order

To render a group (box) of variables, with the variables in a prescribed sequence:

- Add a `variableGroups` block.
- Add a `title` line to this block.
- Add a `variables` block to `variableGroups`.
- Add variables to the `variables` block in the order you want.

Example image for a group of variables:

```
Network Configuration
```

Example declaration for a group of variables with a prescribed order:

```
variableGroups:
  - title: "Network Configuration"
    variables:
      - ods_vcn_use_existing
      - ods_vcn_existing
      - ods_vcn_name
      - ods_vcn_cidr
      - ods_subnet_public_existing
      - ods_subnet_public_name
      - ods_subnet_public_cidr
      - ods_subnet_private_existing
      - ods_subnet_private_name
      - ods_subnet_private_cidr
```

SSH key control

To render a variable as an SSH key control:

- Add the line `type: oci:core:ssh:publickey`.

Example image for an SSH key control:
Example declaration for an SSH key control:

```yaml
ssh_public_key:
  title: SSH Public Key
  description: The public SSH key for the key-pair that you want to use, if you wish to log in to the instances over SSH
  # renders variable as an SSH key control
  type: oci:core:ssh:publickey
  required: true
  pattern: "((^ssh-rsa AAAAB3NzaC1yc2|ecdsa-sha2-nistp256
  AAAAE2VjZHNhLXNoYT1tbmlzdHAyNT|ecdsa-sha2-nistp384
  AAAAE2VjZHNhLXNoYT1tbmlzdHAzODQAAAAlbmldHAAzOD|ecdsa-sha2-nistp521
  AAAAE2VjZHNhLXNoYT1tbmlzdHA1MjEAAAAIbmldHAA1Mj|ssh-ed25519
  AAAAC3NzaC1lZDI1NTE5|ssh-dss AAAAB3NzaC1kc3}|0-9A-Za-z+\/[=]{0,3})
  (\[^,\]*)?)
  ,((ssh-rsa AAAAB3NzaC1yc2|ecdsa-sha2-nistp256
  AAAAE2VjZHNhLXNoYT1tbmlzdHAyNT|ecdsa-sha2-nistp384
  AAAAE2VjZHNhLXNoYT1tbmlzdHAzODQAAAAlbmldHAAzOD|ecdsa-sha2-nistp521
  AAAAE2VjZHNhLXNoYT1tbmlzdHA1MjEAAAAIbmldHAA1Mj|ssh-ed25519
  AAAAC3NzaC1lZDI1NTE5|ssh-dss AAAAB3NzaC1kc3}|0-9A-Za-z+\/[=]{0,3})
  (\[^,\]*)?)\)*$"
```

Dynamic prepopulation

To dynamically prepopulate variables with values based on dependencies:

- Add the lines `type: <supported-type>` and `dependsOn: <other_variable>`.

  `<supported-type>` is a type listed at Supported Types (Dynamic Prepopulation and Controls) on page 3596.

Example image for a dynamically prepopulated variable:

```
SELECT VCN  OPTIONAL

VCN-20200921-1967
```

Example declaration for a dynamically prepopulated variable:

```yaml
ods_vcn_existing:
  # prepopulates available values for VCN
  type: oci:core:vcn:id
  title: "Select VCN"
  # determines values for prepopulation from selected compartment
  dependsOn:
    compartmentId: compartment_ocid
```
Example declarations for VCN depending on compartment, subnet depending on both compartment and VCN:

```python
vcnCompartment:
    # prepopulates available values for compartment
type: oci:identity:compartment:id

myVcn:
    # prepopulates available values for VCN
type: oci:core:vcn:id
    # determines values for VCN prepopulation from selected compartment
dependsOn:
        compartmentId: ${vcnCompartment}

subnetCompartment:
    # prepopulates available values for compartment
type: oci:identity:compartment:id

mySubnet:
    # prepopulates available values for subnet
type: oci:core:subnet:id
    # determines values for subnet prepopulation from selected compartment
    and VCN
dependsOn:
        compartmentId: ${subnetCompartment}
        vcnId: ${myVcn}
```

Image example declaration 1, where image depends on compartment only (the one mandatory dependsOn field):

```python
instance_image:
    title: Image
description: Image
type: oci:core:image:id
required: true
dependsOn:
    compartmentId: ${compartment_ocid}
```

Image example declaration 2, where image depends on compartment, operating system, operating system version, and shape:

```python
instance_image:
    title: Image
description: Image
type: oci:core:image:id
required: true
dependsOn:
    compartmentId: ${compartment_ocid}
    operatingSystem: "Oracle Linux"
    operatingSystemVersion: "7.8"
    shape: "<shape name>"
```

**Enumerated values**

To render enumerated values for a variable:

- Add the lines `type: enum` and add an `enum` block.

Example image for a variable with enumerated values:
Example declaration for a variable with enumerated values:

```yaml
ods_vault_type:
  type: enum
  title: "Vault Type"
  default: "DEFAULT"
  # enumerated values
  enum:
    - DEFAULT
    - VIRTUAL_PRIVATE
```

Check box

To render a variable as a check box:

- Add the line `type: boolean`.

Example image for a check box variable:

![Check Box](image)

Example declaration for a check box variable:

```yaml
ods_vcn_use_existing:
  # renders variable as a check box
  type: boolean
  title: "Use Existing VCN?"
  required: true
  default: false
```

Visibility dependency

**Note:**

Supported operations include "eq", "and", "or", and "not". Groups have higher priority than the groups' constituent variables. For example, if a variable is visible within a group that is not visible, then the entire group is not visible.

To hide or show variables or variable groups depending on other variables:

- Add the line `visible: <other_variable>`.

Example image for a set of variables, where visibility of the "Application Name" and "API Gateway Name" fields is dependent on the "Provision Functions and API Gateway?" check box:

![Visibility Dependency](image)
Example declarations that show the "Application Name" and "API Gateway Name" fields (functions_app_name and apigateway_name) only when the "Provision Functions and API Gateway?" check box (enable_functions_apigateway) is selected:

```yaml
enable_functions_apigateway:
  type: boolean
  title: "Provision Functions and API Gateway?"
  required: true
  default: true

functions_app_name:
  type: string
  title: "Application Name"
  description: "Do not use spaces."
  required: true
  default: "DataScienceApp"
  pattern: "^[a-zA-Z0-9]+$"
  # show only when enable_functions_apigateway variable is selected
  visible: enable_functions_apigateway

apigateway_name:
  type: string
  title: "API Gateway Name"
  required: true
  default: "Data Science Gateway"
  # show only when enable_functions_apigateway variable is selected
  visible: enable_functions_apigateway
```

**Password**

To render a variable as a password:

- Add the line `type: password`.

To require re-entry for confirmation of the entered password:

- Add the line `confirmation: true`.

Example image for a password variable that requires confirmation:

![Example image for a password variable that requires confirmation](image_url)

Example declaration for a password variable, requiring confirmation:

```yaml
password:
  title: Repository Password
  description: Must match remote repository password
  # renders variable as a password field
  type: password
  # renders a second field to re-enter the password for confirmation
  confirmation: true
  pattern: "^[a-zA-Z-][a-zA-Z0-9]{1,8}$"
  required: true
```
Required variables

To require a value for a variable:
• Add the line required: true.

Example image for a required variable, with validation warning:

![Example declaration for a required variable:]

```yaml
availability_domain:
  type: oci:identity:availabilitydomain:name
  dependsOn:
    compartmentId: compartment_ocid
  # displays validation warning if no value is selected or entered
  required: true
  title: "Available Domain"
  description: "Available Domain"
  default: "tabw:PHX-AD-1"
```

Optional variable

To mark a variable as optional:
• Add the line required: false.

Example image for an optional variable:

![Example declaration for a variable with enumerated values:]

```yaml
volume_group_display_name:
  type: string
  # displays "Optional" marking to right of field label
  required: false
  title: "Block Volume Group Display Name"
  description: "Display name of the Block Volume Group"
```

Validation pattern

To validate the value entered for a variable against a regular expression pattern:
• Add the line pattern: <regular-expression>.
  
  <regular-expression> is the validation pattern specific to the value you want to validate.

  Hyperlink pattern example: ^https?:\/\/(www\.)?[-a-zA-Z0-9@:%._\+~#\=]{2,256}\.[a-z]{2,4}\b([-a-zA-Z0-9@:%_\+.~-?&//=]*)$

Example image for a validation error for an entered value:

![Example image for a validation error for an entered value:]

```yaml
APPLICATION_NAME

Specify a value that satisfies the following regular expression: %[-a-zA-Z0-9\-\=]*$```
Example declaration for a variable with a validation pattern:

```yaml
functions_app_name:
  type: string
  title: "Application Name"
  description: "Do not use spaces."
  required: true
  default: "DataScienceApp"
  # validate entered value against alphanumeric regular expression
  pattern: "^[a-zA-Z0-9]+$"
```

**Application Information tab**

To display the Application Information tab for a stack created from your Terraform configuration:

- Add lines for the schema `title` and `description`.
- Add at least one output in the `outputs` section.

To allow copying of an output variable field value displayed in the Application Information tab:

- Set the type: Add the line `type: copyableString`.

Example image for the Application Information tab:

![Example image for the Application Information tab](image-url)

Example declaration for a schema title, description, and outputs:

```yaml
# heading under Application Information tab
title: "OCI Developer Tools"
# text under heading
description: "OCI Developer Tools like CLI, SDK, Terraform and Ansible are pre-installed on the compute instance."
stackDescription: "OCI Developer Tools are pre-installed on the compute instance."
# text in blue information box
informationText: "The auto-generated SSH private key should not be used for production use, instead, the user should generate the SSH key-pair and upload the public key for the compute instance. To connect to the compute instance, copy the ssh private key pem content into a file on your machine. Run the following command from the terminal [ssh -i <path to the pem file> opc@<Public IP>] ."
```

...
GitHub and GitLab Connection Issues

This topic describes how to troubleshoot connection issues to GitHub and GitLab.

**Symptom**

Can't connect to GitHub or GitLab.

This symptom can occur in the following situations:

- Creating a configuration source provider.
- Creating a stack from a new or existing configuration source provider.
- Running a job on a stack that uses a configuration file stored in GitHub or GitLab.

**Possible causes**

- Your Personal Access Token (PAT) may have been revoked or the required permission scopes changed and are insufficient.
- Your GitHub or GitLab repository permissions may have changed and become insufficient.
- Your GitHub or GitLab server is not accessible over the Internet.

**Resolution**

- Recreate your Personal Access Token (PAT) and ensure the scope for the token includes the required permissions (scopes). See the relevant documentation:
  - GitHub: https://docs.github.com/en/free-pro-team@latest/github/authenticating-to-github/creating-a-personal-access-token
  - GitLab: https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html
- Ensure that your GitHub or GitLab repository permissions meet requirements (admin or owner).
- Review prerequisites to confirm that all requirements are satisfied. See Prerequisites for connecting to GitHub and GitLab on page 3582.
Chapter 31

Search

This chapter explains how to search for resources across compartments.

Overview of Search

Oracle Cloud Infrastructure Search lets you find resources within a tenancy, pages of the Console within services, and documentation within the Oracle Cloud Infrastructure Getting Started Guide and Oracle Cloud Infrastructure User Guide. Search sorts search results by resource, service, or documentation, helping you avoid navigating through menus, the latency associated with loading a long list of results onto a single page, or the inconvenience of viewing a long list that spans multiple pages. You can also filter results by criteria specific to the search category after results are found and sorted by category.

You might find it helpful to use Search to find related resources when creating or deleting another resource. For example, you might want to find what compartments already exist before creating a new one because compartments cannot be deleted. Or, if you want to delete a volume, you can use a query to verify that a backup exists.

Another benefit of Search is that you can find resources that require action. For example, you might want to delete terminated block volumes because you no longer need them and don’t want them to count against your service limits. Or, you can search for all resources that match a specific naming scheme, in case you want to act on a category of associated resources. Sometimes, resources in a specific lifecycle state, such as databases in a failed state, require troubleshooting. With Search, you can quickly identify those resources and resolve problems.

Search can also help you find pages within the Console, even if you can’t recall their location among services in the navigation menu. When you find a page, if you want to know more about its contents, you can use Search to find documentation to help you. For example, you might search for “create virtual cloud network” if you want to read documentation about creating a virtual cloud network.

Search Categories and Ways to Search Them

To search for a resource, you can use a free text search based on keywords. You can also use structured resource query language to build an advanced query based on as little as a single resource attribute, such as the resource's creation date. Results for resource searches are limited to the tenancy and the currently selected region.

To find a named page in the Console without knowing the service or to locate help in the documentation, you can use a free text search. Advanced queries don't work for these types of searches.

Supported Resources

Search supports queries for the Oracle Cloud Infrastructure services and resources listed in this section. The following table will be updated as query support is added for more resources. You can refer to each resource's object reference for information about the resource, including its attributes. In some cases, where indicated, a resource might not support all attributes for search. Often, services index only the required attributes for a given resource. For current information about supported resources and resource attributes, use the ListResourceTypes API.

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Migration</td>
<td>amsmigration</td>
<td>See Migration Reference</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Application Migration</td>
<td>amssource</td>
<td>See Source Reference.</td>
</tr>
<tr>
<td>Analytics Cloud</td>
<td>analyticsinstance</td>
<td>See AnalyticsInstance Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apideployment</td>
<td>See Deployment Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apigateway</td>
<td>See Gateway Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apigatewayapi</td>
<td>See Api Reference.</td>
</tr>
<tr>
<td>API Gateway</td>
<td>apigatewaycertificate</td>
<td>See Certificate Reference.</td>
</tr>
<tr>
<td>Big Data</td>
<td>bigdataservice</td>
<td>See BdsInstance Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>bootvolume</td>
<td>See BootVolume Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>bootvolumebackup</td>
<td>See BootVolumeBackup Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volume</td>
<td>See Volume Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumebackup</td>
<td>See VolumeBackup Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumegroup</td>
<td>See VolumeGroup Reference.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumegroupbackup</td>
<td>See VolumeGroupBackup Reference.</td>
</tr>
<tr>
<td>Blockchain Platform</td>
<td>blockchainplatforms</td>
<td>See BlockchainPlatform Reference.</td>
</tr>
<tr>
<td>Budgets</td>
<td>budget</td>
<td>See Budget Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguarddetectorrecipe</td>
<td>See DetectorRecipe Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguardmanagedlist</td>
<td>See ManagedList Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguardresponderrecipe</td>
<td>See ResponderRecipe Reference.</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>cloudguardtarget</td>
<td>See Target Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>autoscalingconfiguration</td>
<td>See AutoScalingConfiguration Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>clusternetwork</td>
<td>See ClusterNetwork Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>consolehistory</td>
<td>See ConsoleHistory Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>dedicatedvmhost</td>
<td>See DedicatedVmHost Reference.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compute</td>
<td>image</td>
<td>See Image Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>instance</td>
<td>See Instance Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Queries for the <code>privateIp</code> or <code>publicIp</code> attribute of a <code>vnic</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>will include the related <code>instance</code>, if one exists, and is running, in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>query results.</td>
</tr>
<tr>
<td>Compute</td>
<td>instanceconfiguration</td>
<td>See InstanceConfiguration Reference.</td>
</tr>
<tr>
<td>Compute</td>
<td>instancepool</td>
<td>See InstancePool Reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Queries for the <code>primarySubnetId</code>, <code>faultDomains</code>, <code>secondaryVnicSubnets</code>, and <code>loadBalancers</code> attributes are not supported.</td>
</tr>
<tr>
<td>Content and Experience</td>
<td>oceinstance</td>
<td>See OceInstance Reference.</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>datacatalog</td>
<td>See Catalog Reference.</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>datacatalogprivateendpoint</td>
<td>See CatalogPrivateEndpoint Reference.</td>
</tr>
<tr>
<td>Data Flow</td>
<td>application</td>
<td>See Application Reference.</td>
</tr>
<tr>
<td>Data Flow</td>
<td>run</td>
<td>See Run Reference.</td>
</tr>
<tr>
<td>Data Integration</td>
<td>disworkspace</td>
<td>See Workspace Reference.</td>
</tr>
<tr>
<td>Data Safe</td>
<td>datasafeprivateendpoint</td>
<td>See DataSafePrivateEndpoint Reference.</td>
</tr>
<tr>
<td>Data Science</td>
<td>datasciencemodel</td>
<td>See Model Reference.</td>
</tr>
<tr>
<td>Data Science</td>
<td>datasciencenotebooksession</td>
<td>See NotebookSession Reference.</td>
</tr>
<tr>
<td>Data Science</td>
<td>datascienceproject</td>
<td>See Project Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomouscontainerdatabase</td>
<td>See AutonomousContainerDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomousdatabase</td>
<td>See AutonomousDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomoussexadatanirastructure</td>
<td>See AutonomousExadataInfrastructure Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>autonomousvmcluster</td>
<td>See AutonomousVmCluster Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>backupdestination</td>
<td>See BackupDestination Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>cloudexadatanirastructure</td>
<td>See CloudExadataInfrastructure Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>cloudvmcluster</td>
<td>See CloudVmCluster Reference.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Database</td>
<td>database</td>
<td>See Database Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>dbhome</td>
<td>See DbHome Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>dbsystem</td>
<td>See DbSystem Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>exadatainfrastructure</td>
<td>See ExadataInfrastructure Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externalcontainerdatabase</td>
<td>See ExternalContainerDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externaldatabaseconnector</td>
<td>See ExternalDatabaseConnector Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externalnoncontainerdatabase</td>
<td>See ExternalNonContainerDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>externalpluggabledatabase</td>
<td>See ExternalPluggableDatabase Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>vmcluster</td>
<td>See VmCluster Reference.</td>
</tr>
<tr>
<td>Database</td>
<td>vmclusternetwork</td>
<td>See VmClusterNetwork Reference.</td>
</tr>
<tr>
<td>Digital Assistant</td>
<td>odainstance</td>
<td>See OdaInstance Reference.</td>
</tr>
<tr>
<td>Email Delivery</td>
<td>emailsender</td>
<td>See Sender Reference.</td>
</tr>
<tr>
<td>Events</td>
<td>eventrule</td>
<td>See Rule Reference.</td>
</tr>
<tr>
<td>File Storage</td>
<td>filesystem</td>
<td>See FileSystem Reference.</td>
</tr>
<tr>
<td>File Storage</td>
<td>mounttarget</td>
<td>See MountTarget Reference.</td>
</tr>
<tr>
<td>Functions</td>
<td>functionsapplication</td>
<td>See Application Reference.</td>
</tr>
<tr>
<td>Functions</td>
<td>functionsfunction</td>
<td>See Function Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>compartment</td>
<td>See Compartment Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>group</td>
<td>See Group Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>identityprovider</td>
<td>See IdentityProvider Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>policy</td>
<td>See Policy Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>tagdefault</td>
<td>See TagDefault Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>tagnamespace</td>
<td>See TagNamespace Reference.</td>
</tr>
<tr>
<td>IAM</td>
<td>user</td>
<td>See User Reference.</td>
</tr>
<tr>
<td>Integration Cloud</td>
<td>integrationinstance</td>
<td>See IntegrationInstance Reference.</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>loadbalancer</td>
<td>See LoadBalancer Reference.</td>
</tr>
<tr>
<td>Management Agent</td>
<td>management-agents</td>
<td>See ManagementAgent Reference.</td>
</tr>
<tr>
<td>Management Agent</td>
<td>management-agent-install-keys</td>
<td>See ManagementAgentInstallKey Reference.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>alarm</td>
<td>See Search-Supported Attributes for Alarms on page 2664.</td>
</tr>
<tr>
<td>MySQL Database</td>
<td>dbsystem</td>
<td>See DBSystem Reference.</td>
</tr>
<tr>
<td>Service</td>
<td>Resource Type</td>
<td>Attributes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Networking</td>
<td>byoiprange</td>
<td>See ByoipRange Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>cpe</td>
<td>See Cpe Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>crossconnect</td>
<td>See CrossConnect Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>crossconnectgroup</td>
<td>See CrossConnectGroup Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>dhcpoptions</td>
<td>See DhcpOptions Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>drg</td>
<td>See Drg Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>internetgateway</td>
<td>See InternetGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>ipseccomconnection</td>
<td>See IPSecConnection Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>ipv6</td>
<td>See IPv6 Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>localpeeringgateway</td>
<td>See LocalPeeringGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>natgateway</td>
<td>See NatGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>networksecuritygroup</td>
<td>See NetworkSecurityGroup Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>publicip</td>
<td>See PublicIp Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>publicippool</td>
<td>See PublicIpPool Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>privateip</td>
<td>See Privatelp Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>remotepeeringconnection</td>
<td>See RemotePeeringConnection Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>routetable</td>
<td>See RouteTable Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>servicegateway</td>
<td>See ServiceGateway Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>subnet</td>
<td>See Subnet Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>vcn</td>
<td>See Vcn Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>virtualcircuit</td>
<td>See VirtualCircuit Reference.</td>
</tr>
<tr>
<td>Networking</td>
<td>vnic</td>
<td>See Vnic Reference.</td>
</tr>
<tr>
<td>NoSQL Database Cloud</td>
<td>table</td>
<td>See Table Reference.</td>
</tr>
<tr>
<td>Notifications</td>
<td>onssubscription</td>
<td>See Subscription Reference.</td>
</tr>
<tr>
<td>Notifications</td>
<td>onstopic</td>
<td>See NotificationTopic Reference.</td>
</tr>
</tbody>
</table>

**Note:** Queries for the `privateIp` or `publicIp` attribute of a `vnic` will include the related instance, if one exists and is running, in the query results.
<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Storage</td>
<td>bucket</td>
<td>See Bucket Reference.</td>
</tr>
<tr>
<td>OS Management</td>
<td>osmsmanagedinstancegroup</td>
<td>See ManagedInstanceGroup Reference.</td>
</tr>
<tr>
<td>OS Management</td>
<td>osmsscheduledjob</td>
<td>See ScheduledJob Reference.</td>
</tr>
<tr>
<td>OS Management</td>
<td>osmssoftwareresource</td>
<td>See SoftwareSource Reference.</td>
</tr>
<tr>
<td>Registry</td>
<td>containerimage</td>
<td>See ContainerImage Reference.</td>
</tr>
<tr>
<td>Registry</td>
<td>containerrepository</td>
<td>See ContainerRepository Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormconfigsourceprovider</td>
<td>See ConfigurationSourceProvider Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormjob</td>
<td>See Job Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormstack</td>
<td>See Stack Reference.</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>ormtemplate</td>
<td>See Template Reference.</td>
</tr>
<tr>
<td>Service Connector Hub</td>
<td>serviceconnector</td>
<td>See ServiceConnector Reference.</td>
</tr>
<tr>
<td>Service Limits</td>
<td>quota</td>
<td>See Quota Reference.</td>
</tr>
<tr>
<td>Streaming</td>
<td>connectharness</td>
<td>See ConnectHarness Reference.</td>
</tr>
<tr>
<td>Streaming</td>
<td>stream</td>
<td>See Stream Reference.</td>
</tr>
<tr>
<td>Vault</td>
<td>key</td>
<td>See Key Reference.</td>
</tr>
<tr>
<td>Vault</td>
<td>vault</td>
<td>See Vault Reference.</td>
</tr>
<tr>
<td>Vault</td>
<td>vaultsecret</td>
<td>See Secret Reference.</td>
</tr>
<tr>
<td>VMware solution</td>
<td>vmwareesxihost</td>
<td>See EsxiHost Reference.</td>
</tr>
<tr>
<td>VMware solution</td>
<td>vmwaresddc</td>
<td>See Sddc Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>httpredirect</td>
<td>See HttpRedirect Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waasaddresslist</td>
<td>See AddressList Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waascertificate</td>
<td>See Certificate Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waascustomprotectionrule</td>
<td>See CustomProtectionRule Reference.</td>
</tr>
<tr>
<td>WAF</td>
<td>waaspolicy</td>
<td>See WaasPolicy Reference.</td>
</tr>
</tbody>
</table>

**Common Resource Attributes**

Although you can use the query language to search fields and values for any supported attribute, query results only provide information about the following resource attributes:

- Resource type
- Oracle Cloud Identifier (OCID)
- Compartment
- Availability domain
- Display name
- Creation date and time
- Lifecycle state
- Tags (visible in the API only)

The preceding attributes are common to most Oracle Cloud Infrastructure resources. Their meaning is consistent across resource types, so they're provided by default for each result when you view a list of query results. Query results do not contain information specific to any resource type except where a matching search term appears. Meaning, you can query for volumes of a certain size. If there's a match, then the search result will display the attribute with the value that matches. In this example, in addition to the common attributes, the result also provides the `Size` attribute if that's where the match was found. You must view the details of a resource to see other resource-specific information.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use the Console, neither query results nor resource details will include either defined tags or free-form tags, due to display constraints. Any given resource might contain hundreds of tags. If you want to see tags, use the API to view resource details.</td>
</tr>
</tbody>
</table>

### Required IAM Permissions

The resources that you see in search or query results depend on the permissions you have in place for the resource type. You do not necessarily see results for every resource in the compartment or tenancy. For example, if your user account is not associated with a policy that grants you the ability to, at a minimum, inspect the `dbsystem` resource type, then you can’t query for DB systems. (The verb `inspect` lets you list and get resources.) Instead, Search will show no results for queries of DB system resources.

Permissions and policy language applies to resources. Searching for pages across services in the Console or documentation requires no special permissions because they aren't resources. An administrator cannot restrict access to search results of services or documentation.

For more information about policies, see [How Policies Work](#) on page 2136. For information about the specific permissions required for the list API operation for your desired resource type, see the [Policy Reference](#) on page 2167 for the appropriate service.

### Free Text Search

This topic describes how Search handles the search terms that you submit as a free text search.

By default, text entered in the Console search box is interpreted as a free text search. You can use a free text search to conduct a search of any category that Search supports. This includes searches for resources, pages across services in the Console, and documentation.

**Matching**

Search tries to match search terms against the values of indexed fields. For resources, this means that Search evaluates the value of all indexed resource attributes, from [common attributes](#) (except the resource type attribute) to attributes specific to a resource type. For services, this includes all page display names and service groups. For documentation, this includes the title and the contents of the topic. (Search does not query the topic description, topic category, or keyword metadata.)

To provide matching results to the text given in a free text search, Search queries all indexed fields by applying the `=` (equals) operator to text that you specified. If you're familiar with advanced queries, the effect is the same as using a `matching` clause. For example, a free text search for the term "net" queries all resource types, service pages, and documentation for the string "net" in any indexed field. If the string appears as part or the whole of a value anywhere in an indexed field, Search considers the found item a matching result. Search does not require exact matching, but an exact match does improve a result's ranking.

If the free text search includes a delimiting character (for example, a hyphen), the delimiter causes Search to treat the text on either side of the delimiter as an independent search term. For example, a free text search for "2020-04" looks for the string "2020" and the string "04". If a potential result contains either string, then it's a match.
Free text search matches individual terms from the provided text. Search does not try to match specific combinations of characters that you might group by using quotes or by presenting terms in a specific order. Likewise, proximity of search terms does not matter. However, if you have multiple search terms in a free text search, results that contain multiple matches to the search terms have a higher ranking in the search results.

**Ranking of Results**

To rank results, Search evaluates each potential result for how closely it can match the search term or terms provided. Exact matches occupy a higher rank in the results than partial matches. Search also considers how many matches for the exact search term the result contains. Either a close match or multiple matching terms improves the result's ranking.

**Search Language Syntax**

This topic describes the basics of the query language for Search, including an explanation of syntax and rules so you can create your own queries. Queries apply search conditions to specific resource types and let you sort results. If you want to search across all supported resource types and resource attributes and do not need ordered search results, you do not need to construct a query. Instead, you can search for a partial or exact match of free-form text without applying query language syntax to your search.

When you are ready to run a query, see [Querying Resources, Services, and Documentation](#) on page 3642 for instructions.

**Query Basics**

The following examples show the basic syntax of a query:

```plaintext
query <resourceType> resources where <conditions> sorted by <fieldName> <order>
```

Or:

```plaintext
query <resourceType> resources matching <keywords>
```

Search ignores white space, indentation, and line breaks. Sample queries include indentation to improve readability. For the purposes of demonstrating syntax only, angle brackets (<> ) and italicized text indicate variables, which can consist of one or more keywords.

In a query, clauses include the following:

- **query** - (Required) Selects which resources to return based on subsequent clauses. Query statements always begin with the word `query`.
- **where** - Matches resources to the specified `conditions`.
- **matching** - Matches resources to the specified text regardless of whether the text matches exactly, matches the resource type, or appears in an indexed resource attribute.
- **sorted by** - Orders resources according to `fieldName` in the order specified by `order`. If you do not include this clause, Search lists results by creation date in descending order, with the newest resources listed first.

Clauses are optional unless indicated otherwise. For matching purposes, you can use the `where` clause and the `matching` clause either separately or together.

In the `query` clause, you specify the following information:

- **resourceType** - (Required) Specifies the resource type to which the subsequent clauses apply when you run the query. You can specify either the resource type name (for example, `database` or `group`) or `all`. If you specify `all`, Search searches for the `conditions` against all resource types. You can query for individual resource types, but not family types. For a list of supported resource types, see the [Supported Resources](#) section of [Overview of Search](#).
- **resources** - (Required) Specifies that this is a resource query.
**Conditions**

The `where` clause applies conditions that filter the results returned by Search. You can specify one or more condition statements. For more information about multiple conditions, see Grouping Conditions.

In a query, conditions consist of the following:

```
<fieldName> <operation> <value>
```

The `fieldName` keyword is the resource attribute against which the operation and chosen value of that attribute are evaluated. Each field is associated with a field type. The field type tells you the expected format for any value in that field. What kind of operation you can use in a conditions statement depends on the field type.

In query conditions, an operation is a comparison operator that applies to the value in the statement. The `value` keyword refers to the value of the `fieldName` you specified. Search evaluates whether the specified attribute of the chosen resource type matches or does not match the value, according to the operation. In a query, you must enclose any string or date-time value in opening and closing straight single quotes (#) or double quotes (").

The following table describes supported operations for resource queries:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Supported Field Types</th>
<th>Case-sensitive?</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equals, or exact matching for strings</td>
<td>String, integer, rational, Boolean, date-time</td>
<td>No</td>
<td>If the value was #backUp#, it would match &quot;backup&quot;, &quot;BACKUP&quot;, &quot;BackUp&quot;, &quot;backUp&quot;, or any other variation in casing.</td>
</tr>
<tr>
<td>!=</td>
<td>Does not equal</td>
<td>String, integer, rational, Boolean, date-time</td>
<td>No</td>
<td>If the value was #backUp#, it would match anything that does not equal &quot;backUp&quot;, &quot;backup&quot;, or any other variation in casing. It also would match anything that does not contain the characters 'backup' in that order.</td>
</tr>
<tr>
<td>==</td>
<td>Strictly equals</td>
<td>String</td>
<td>Yes</td>
<td>If the value was #backUp#, it would only match &quot;backUp&quot; and no other variation in casing.</td>
</tr>
<tr>
<td>!==</td>
<td>Strictly does not equal</td>
<td>String</td>
<td>Yes</td>
<td>If the value was #backUp#, it would match &quot;backup&quot;, &quot;BACKup&quot;, or anything except &quot;backUp&quot;, with that exact casing.</td>
</tr>
</tbody>
</table>
The following table lists some examples of resource attributes that belong to each category of supported field types. (As previously described, the field type tells you the expected format for a given field and the kind of operation you can pair it with in a conditions statement.)

The table does not include every possible example for a given field type nor does it include examples from every resource-type. If you want to know what format the Search service expects for a specific resource attribute, you can use the command line interface or API to find out more about resource attributes. You can also consult the API documentation. The API documentation includes a reference for each supported resource type that specifies attributes, their field types, and any restrictions. For more information, see the Supported Resources section of Overview of Search.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Supported Field Types</th>
<th>Case-sensitive?</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>=~</td>
<td>Contains</td>
<td>String</td>
<td>No</td>
<td>If the value was #backUp#, it would match anything that equals &quot;backup&quot;, &quot;BACKUP&quot;, &quot;BackUp&quot;, &quot;backUp&quot;, or any other variation in casing, or contains those characters in that order, alongside other characters.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to</td>
<td>Integer, rational, date-time</td>
<td>Not applicable</td>
<td>For a query where you have size &gt;= 5 as the condition, all results have a value of 5 or greater in the field named size.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than</td>
<td>Integer, rational, date-time</td>
<td>Not applicable</td>
<td>For a query where you have size &gt; 5 as the condition, all results have a value of greater than 5 in the field named size.</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
<td>Integer, rational, date-time</td>
<td>Not applicable</td>
<td>For a query where you have size &lt;= 5 as the condition, all results have a value of 5 or less in the field named size.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than</td>
<td>Integer, rational, date-time</td>
<td>Not applicable</td>
<td>For a query where you have size &lt; 5 as the condition, all results have a value of 5 or less in the field named size.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Example Resource Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Display names, lifecycle states, availability domains, tags, CIDR blocks, and URLs</td>
</tr>
<tr>
<td>Type</td>
<td>Example Resource Attributes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Integer</td>
<td>Size or length of a resource</td>
</tr>
<tr>
<td>Rational</td>
<td>Available data storage</td>
</tr>
<tr>
<td>Boolean</td>
<td>Whether a feature is enabled or configured, whether a resource is healthy, whether a resource is public or private, whether something is the latest version, and whether something is allowed</td>
</tr>
<tr>
<td>Date-time</td>
<td>Creation dates, last-updated dates, last-indexed dates, and scheduled maintenance reboots</td>
</tr>
</tbody>
</table>

**Grouping Conditions**

By including more than one condition statement in a query, you can refine results according to multiple criteria. You can group multiple conditions by using either the logical operators && (ampersands, to indicate a logical AND) or || (vertical bars, to indicate a logical OR). For example:

```plaintext
licenseModel = 'LICENSE_INCLUDED' && dataStoragePercentage > 40 && lifecycleState != 'FAILED'
```

You cannot combine two different logical operators in the same query unless you wrap parentheses around one group of predicates. (Multiple conditions can only use the same logical operator otherwise.) For example:

```plaintext
(licenseModel = 'LICENSE_INCLUDED' && dataStoragePercentage > 40) || lifecycleState != 'FAILED'
```

In the preceding example, all results returned will have either “LICENSE_INCLUDED” as the value in the field named “licenseModel” and a value greater than 40 for the field named “dataStoragePercentage” or the value of their “lifecycleState” field name is anything other than “FAILED”.

The following group is also acceptable:

```plaintext
licenseModel = 'LICENSE_INCLUDED' && (dataStoragePercentage > 40 || lifecycleState != 'FAILED')
```

In the preceding example, all results returned will have “LICENSE_INCLUDED” as the value in the field named “licenseModel” and either a value greater than 40 as the value for the field named “dataStoragePercentage” or anything that is not “FAILED” for the value of the field named “lifecycleState”.

Search does not perform left-to-right evaluation to reduce ambiguity or clarify intent.

**Date and Time Values**

You can specify date and time values by using any of the following pattern string formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Examples</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;yyyy&gt;</code>-<code>&lt;MM&gt;</code>-<code>&lt;dd&gt;</code></td>
<td>'2018-06-19 16:15:41 PDT',</td>
<td>Time Zone is optional. If Time Zone is omitted, UTC is used.</td>
</tr>
<tr>
<td><code>&lt;HH&gt;</code>: <code>&lt;mm&gt;</code>: <code>&lt;ss&gt;</code> <code>&lt;TimeZone&gt;</code></td>
<td>'2018-06-19 16:15:41 -08:00'</td>
<td></td>
</tr>
<tr>
<td><code>&lt;EEE&gt;</code>, <code>&lt;d&gt;</code>, <code>&lt;MM&gt;</code> <code>&lt;yyyy&gt;</code></td>
<td>'Tue, 19 Jun 2018 16:15:41 +0300',</td>
<td>EEE is optional. MMM can also be expressed as MMMM. Time Zone</td>
</tr>
<tr>
<td><code>&lt;HH&gt;</code>: <code>&lt;mm&gt;</code>: <code>&lt;ss&gt;</code> <code>&lt;TimeZone&gt;</code></td>
<td>'19 June 2018 16:15:41'</td>
<td>is also optional. If Time Zone is omitted, UTC is used.</td>
</tr>
</tbody>
</table>
You must observe spacing. Interpret dashes, colons, commas, and the characters 'T' and 'Z' literally. To interpret placeholder values in the preceding table, you can refer to the following pattern syntax:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Date or Time Component</th>
<th>Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Year</td>
<td>Year</td>
</tr>
<tr>
<td>M</td>
<td>Month in year</td>
<td>Month</td>
</tr>
<tr>
<td>d</td>
<td>Day in month</td>
<td>Day</td>
</tr>
<tr>
<td>H</td>
<td>Hour in day (from 00-23)</td>
<td>Number</td>
</tr>
<tr>
<td>m</td>
<td>Minute in hour</td>
<td>Number</td>
</tr>
<tr>
<td>s</td>
<td>Seconds in minute</td>
<td>Number</td>
</tr>
<tr>
<td>E</td>
<td>Day in week</td>
<td>Text</td>
</tr>
</tbody>
</table>

Repeating pattern letters indicate their exact presentation. For example, 'HH' means you must use '00' and not '0' to represent midnight. Similarly, 'EEE' means 'Tue' and not 'Tuesday'. Likewise, 'MM' requires '09' instead of '9' to represent the month of September.

TimeZone is optional, but in your chosen format, you can specify TimeZone in any of the following ways:

- **Name.** You can specify a time zone by its name, such as GMT or PDT. Values are case-insensitive.
- **GMT offset value.** You can specify a time zone according to its GMT offset. For example, GMT-08:00. Values are case-insensitive.
- **ISO 8601 time zone.** You can specify a time zone according to ISO 8601 standards. For example, -08, -0800, or -08:00.

Instead of using one of the preceding formats, you can also specify a date-time value as the constant now. The constant now represents the current time to the level of granularity of seconds in a minute.

Lastly, you can add or subtract time intervals from any date-time values. For example, you can query for resources that were created within five minutes of a specific time. Search supports the following time intervals:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Date or Time Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>Seconds</td>
</tr>
<tr>
<td>m</td>
<td>Minutes</td>
</tr>
<tr>
<td>h</td>
<td>Hours</td>
</tr>
<tr>
<td>d</td>
<td>Days</td>
</tr>
<tr>
<td>w</td>
<td>Weeks</td>
</tr>
</tbody>
</table>

To specify a time interval in relation to a date-time value, use one of the following formats:

- now - 3h
- 2018-06-19 16:15:41 PDT + 1h

**Matching**

For matching purposes, instead of or in addition to using a where clause with conditions, you might want to use the matching clause. The matching clause obviates the need to specify conditions (that contain a field name, operation, and value). A matching clause effectively queries all indexed fields by applying the = (equals) operator along with the text you specify. However, it does so without strictly requiring an exact match. For example, the following query uses a matching clause to behave the same way as a free text search: query all resources
matching 'instance'. The query produces results that match all resources and resource attributes that contain the word "instance".

The matching clause queries all indexed fields for matches, but ignores special characters, including any punctuation.

**Sorting**

The last clause of a resource query is the sorted by clause and is optional. The sorted by clause orders the results returned by Search based on the field name and lists them according to the order you specify. By default, if you do not specify sort order, results are always sorted by date-time created in descending order.

In the sorted by clause, you can specify the following:

- **fieldName** - The field that Search uses to sort results. You can specify any field of any resource. Resources that do not contain the field you specify are listed after the resources that do.
- **order** - You can specify either asc or desc. Specifying asc lists results in ascending order. Specifying desc lists results in descending order.

**Querying Multiple Resource Types**

You can query multiple resource types at once by joining queries. Each query can have its own conditional clause. If the queries that you want to join have different "where" conditions, then the syntax is different from when you have queries for multiple resource types that share the same "where" condition.

The basic syntax for a query for multiple resource types is as follows:

```
query <resourceType>,<resourceType> resources
```

For example:

```
query group, user resources
```

The preceding example query returns all groups and all users in the tenancy.

The following shows the syntax for a query for multiple resource types with conditions, but where the conditions are the same for all resource types:

```
query <resourceType>,<resourceType> resources where <conditions>
```

For example:

```
query group, user resources where displayName = 'administrator'
```

The preceding example query returns all groups with the display name "administrator" and all users with the display name "administrator," with any variation in casing.

If you need to apply differing conditions to any resource type, you must use a union keyword instead of comma separation between the joined queries. The following shows the syntax for a query for multiple resource types where some of the resource types share conditions while others do not:

```
query <resourceType>,<resourceType> resources where <conditions>
union <resourceType> resources
```

For example:

```
query group, user resources where displayName = 'administrator' union compartment resources
```
The preceding example returns all groups with the display name "administrator" and all users with the display name "administrator," with any variation in casing, and all compartment resources.

Or, for example:

```
query group resources union user resources where displayName = 'administrator' union compartment resources
```

The preceding example returns all groups and all compartments. It also returns all users with the display name "administrator," with any variation in casing.

Optionally, you can add the `sorted by` clause to the end of the query to order all results in ascending or descending order.

### Sample Queries

This topic provides an explanation of sample queries, including what results to expect from a given sample query. For more information about the syntax for constructing a query, see Search Language Syntax on page 3633.

**Note:**

**Example Values**

Sample queries show example values for resource attributes. Replace those examples with values from your own tenancy.

Search provides the following sample queries in the Console:

- Query for everything
- Query for everything, sorted by time created
- Query for volumes and users
- Query for volumes and users, sorted by time created
- Query for volumes and users that have any indexed field matching “production,” sorted by time created
- Query for all resources that have a specific freeform tag
- Query for all resources that have one of two specific defined tags
- Query for instances in a "Running" state
- Query for instances in either a "Terminated" or "Terminating" state
- Query for all resources in a specific compartment
- Query for all instances due for a maintenance reboot
- Query for all resources that are Always Free

### Query All Resources

**Query name:** Query for everything

**Expected results:** Returns all supported resources in the tenancy across all compartments. Lists results, by default, in order of time created, from newest to oldest.

**Sample query language:**

```
query all resources
```

### Query All Resources, Sort by Time Created

**Query name:** Query for everything, sorted by timeCreated

**Expected results:** Returns all supported resources in the tenancy across all compartments, listed in order of time created, from newest to oldest.
Sample query language:
```sql
query
  all resources
  sorted by timeCreated desc
```

**Query Volumes and Users**

**Query name:** Query for volumes and users

**Expected results:** Returns all block volumes and users in the tenancy. Lists results, by default, in order of time created, from newest to oldest.

**Sample query language:**
```sql
query
  volume, user resources
```

**Query All Volumes and Users, Sort by Time Created**

**Query name:** Query for volumes and users, sorted by timeCreated

**Expected results:** Returns all block volumes and users in the tenancy, listed in order of time created, from newest to oldest

**Sample query language:**
```sql
query
  volume, user resources
  sorted by timeCreated desc
```

**Query Volumes and Users Matching "Production," Sorted by Time Created**

**Query name:** Query for volumes and users, with anything matching production, sorted by timeCreated

**Expected results:** Returns all block volumes and users in the tenancy that have any indexed fields that exactly or partially match the search string "production", irrespective of casing. Lists results, by default, in order of time created, from newest to oldest.

**Sample query language:**
```sql
query
  volume, user resources
  matching 'production'
  sorted by timeCreated desc
```

**Query All Resources With Specific Freeform Tags**

**Query name:** Query for all resources that have specific freeform tags

**Expected results:** Returns all resources in the tenancy that have a freeform tag of "costcenter" with a value of "1234."

**Sample query language:**
```sql
query
  all resources
  where
    (freeformTags.key = 'costcenter' && freeformTags.value = '1234')
```
Query All Resources According to Defined Tags

Query name: Query for all resources that have one of two specific defined tags

Expected results: Returns all resources in the tenancy that have either a tag with the key “region” and value “phx” in the tag namespace “categorization,” or all resources in the tenancy that have a tag with the key “region” and value “iad” in the namespace “categorization.” Ignores casing for all keys and values.

Sample query language:

```sql
query
  all resources
  where
    (definedTags.namespace = 'categorization' && definedTags.key = 'region' && definedTags.value = 'phx') ||
    (definedTags.namespace = 'categorization' && definedTags.key = 'region' && definedTags.value = 'iad')
```

Query Instances According to Specific Lifecycle State

Query name: Query for running instances

Expected results: Returns all instances in the tenancy in a "Running" state. Lists results, by default, in order of time created, from newest to oldest.

Sample query language:

```sql
query
  instance resources
  where lifeCycleState = 'RUNNING'
```

Query Instances According to One of Two Lifecycle States

Query name: Query for instances terminated or terminating

Expected results: Returns all instances in the tenancy in either a "Terminated" or "Terminating" state. Lists results, by default, in order of time created, from newest to oldest.

Sample query language:

```sql
query
  instance resources
  where lifeCycleState = 'TERMINATED' || lifeCycleState = 'TERMINATING'
```

Query All Resources According to Compartment ID

Query name: Query for all resources in a compartment

Expected results: Returns all resources in the tenancy with a specific compartment ID. Lists results, by default, in order of time created, from newest to oldest.

Sample query language:

```sql
query
  all resources
  where compartmentId = 'compartmentOcid'
```

Query All Instances Due for Maintenance Reboot

Query name: Query for all instances which have an upcoming scheduled maintenance reboot
Expected results: Returns all instances in the tenancy with a scheduled maintenance reboot time value of "now."
Lists results, by default, in order of time created, from newest to oldest.

Sample query language:

```
query
  instance resources
  where timeMaintenanceRebootDue = 'now'
```

Query All Always Free Resources

Query name: Query for all resources that are Always Free

Expected results: Returns all existing resources in the tenancy that are free of charge for the life of the account. Lists results, by default, in order of time created, from newest to oldest.

Sample query language:

```
query
  all resources
  where
    systemTags.namespace = 'orcl-cloud' &&
    systemTags.key = 'free-tier-retained' &&
    systemTags.value = 'true'
```

Querying Resources, Services, and Documentation

This topic describes different ways you can use Search.

You can find Oracle Cloud Infrastructure resources in your tenancy by performing a free text search or running a query. A free text search locates resources with the desired text anywhere in the resource metadata. An advanced query lets you find resources according to specific fields and conditions. When finding resources, both free text searches and queries rely on resource indexing and the indexed attributes for a given resource type. Search also scopes resource results to the currently selected region.

Although queries can only be used to find resources, you can use free text searches to help you locate pages in the Console or help in the documentation. A free text search looks for search terms in the display names of Console pages and lists pages according to where they appear within services in the tenancy. A free text search can also find search terms in the Oracle Cloud Infrastructure Getting Started Guide and Oracle Cloud Infrastructure User Guide documentation. The results for both these types of searches depend on the language, but not the region.

Note:

Supported Resources and Using Advanced Resource Queries

The search results that you see reflect what Search considers supported resources. To see what Oracle Cloud Infrastructure services and resources Search supports, see the Supported Resources section of Overview of Search.

Furthermore, if you don't find the resource you want or expect when you submit a free text search, you might need to run a query constructed using query language syntax. For more information about syntax for advanced queries, see Search Language Syntax on page 3633. (For a documentation search, if a free text search doesn't produce the content results you expect, you might try a plural or singular form of one or more search terms or a different, supported language.)

Using the Console

You can find resources, services, or documentation by doing one of the following:

- typing free-form text for a free text search
• reusing recent search terms
• typing a query (for resources only)
• modifying a sample query

By default, text entered into the Search for resources, services, and documentation box is interpreted as a free text search.

To perform a free text search

1. In the top navigation bar, click Search for resources, services, and documentation.
2. Type the free-form text you want to search for.
3. Under one of the categories of search results, click a result. (To see all results on a full page instead, click View all next to the category name.)
4. (Optional) If you do not see the results that you expect, you can change to a different region (if searching for a resource), change to a different language (if searching for a service or documentation), view a different category of search results, or edit your search terms. If searching for a resource, you can also refine your search with a query by clicking Advanced Resource Query. Then, follow the instructions in To run a custom, free-form query or To run a sample query.
5. (Optional) If you chose to view results on a full page, the list shows results with the best matches at the beginning of the list. However, you can also do the following:
   • If you chose the Resources category specifically, you can sort results, expand individual results to see the matching text, or you can filter results more specifically. To filter results more specifically, click Choose one or more resource types to filter the results, and then type or choose one or more resource types to include.
   • For the Services category, you can only filter or sort results. To filter results more specifically, click Choose one or more service groups to filter the results, and then type or choose the service group to include.
   • Similarly, for the Documentation category, you can only filter or sort results. To filter results more specifically, click Choose one or more topics to filter the results. (Here, "topic" refers to the subject matter rather than the topic title.)

For any category, filter options only include resource types, service groups, or documentation presented in the full list of results.

Results are eventually consistent, but might not immediately include resources that you created very recently.

To run a custom, free-form query to find a resource

1. In the top navigation bar, click Search for resources, services, and documentation, and then click Advanced Resource Query.
2. In the query text box, type a query using query language syntax, and then click Search.
3. The list shows results in groupings. From here, you can filter results more specifically: click Choose one or more resource types to filter the results, and then type or choose one or more resource types to include in filtered results. Filter options only include resource types present in the full list of results.
4. (Optional) If you do not see the results that you expect, you can change to a different region or edit your query.

Results are eventually consistent, but might not immediately include resources that you created very recently.

To run a sample query to find a resource

1. In the top navigation bar, click Search for resources, services, and documentation, and then click Advanced Resource Query.
2. Click Select Sample Query, and then click one of the listed sample queries. For an explanation of sample queries, see Sample Queries on page 3639.
3. Verify that the query language in the query text box satisfies your needs. Change all example values. Add, delete, or modify clauses, as appropriate, and then click Search.
4. The list shows results in groupings. From here, you can filter results more specifically: click Choose one or more resource types to filter the results, and then type or choose one or more resource types to include in filtered results. Filter options only include resource types present in the full list of results.
5. (Optional) If you do not see the results that you expect, you can change to a different region or edit your query.
Results are eventually consistent, but might not immediately include resources that you created very recently.

**To reuse recent search terms**

1. In the top navigation bar, click **Search for resources, services, and documentation**.
2. Under **Recent searches**, click one of five recent search terms. (Recent searches only include the five most recent free text searches, not advanced searches that use the structured query language.)
3. Under one of the categories of search results, click a result. (To see all results on a full page instead, click **View all** next to the category name.)
4. (Optional) If you do not see the results that you expect, you can change to a different region (if searching for a resource), change to a different language (if searching for a service or documentation), view a different category of search results, or edit your search terms. If searching for a resource, you can also refine your search with a query by clicking **Advanced Resource Query**. Then, follow the instructions in To run a custom, free-form query or To run a sample query.
5. (Optional) If you chose to view results on a full page, the list shows results with the best matches at the beginning of the list. However, you can also do the following:
   - If you chose the **Resources** category specifically, you can sort results, expand individual results to see the matching text, or you can filter results more specifically. To filter results more specifically, click **Choose one or more resource types to filter the results**, and then type or choose one or more resource types to include.
   - For the **Services** category, you can only filter or sort results. To filter results more specifically, click **Choose one or more service groups to filter the results**, and then type or choose the service group to include.
   - Similarly, for the **Documentation** category, you can only filter or sort results. To filter results more specifically, click **Choose one or more topics to filter the results**. (Here, "topic" refers to the subject matter rather than the topic title.)

For any category, filter options only include resource types, service groups, or documentation presented in the full list of results.

Results are eventually consistent, but might not immediately include resources that you created very recently.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see [Command Line Interface (CLI)](https://docs.oracle.com/en/cloud incontras/oci/service-configuration/ocisearch.html). For a complete list of flags and options available for CLI commands, see the [Command Line Reference](https://docs.oracle.com/en/cloud incontras/oci/service-configuration/ocisearch.html).

**To see what resource-types you can run a query for**

Open a command prompt and run `oci search resource-type list` to see what resource-types you can run a query for:

```bash
oci search resource-type list
```

For example:

```bash
oci search resource-type list --all
```

**To see what resource attributes you can query for a given resource-type**

Open a command prompt and run `oci search resource-type get` to see what attributes you can search for a given resource-type:

```bash
oci search resource-type get --name <resource-type_name>
```

You must specify the resource-type by its indexed name. Pay attention to capitalization. For example:

```bash
oci search resource-type get --name VolumeBackup
```
To perform a free text search

Open a command prompt and run `oci search resource free-text-search` to search the text of all searchable resource-types:

`oci search resource free-text-search`

For example:

`oci search resource free-text-search --text <text_to_search_for>

To run a custom, free-form query to find a resource

Open a command prompt and run `oci search resource structured-search` to run an advanced resource query:

`oci search resource structured-search --query-text "<query_text_using_query_language_syntax>"

For example:

`oci search resource structured-search --query-text "query user resources"

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to search for resources or find out what resources you can search for:

- SearchResources
- ListResourceTypes

In addition to finding supported resources with ListResourceTypes, you can also find what attributes each resource supports for search.

Example: Finding Instance Resources With a Specific Defined Tag

This section describes how to use the API to query for a specific type of resource based on the resource's defined tags.

The following query will find instances with a defined tag within the namespace "rqs", where the tag's key is "costcenter" and the key's value is "1234".

```sql
query
  instance resources
where
  (definedTags.namespace = 'rqs' && definedTags.key = 'costcenter' &&
  definedTags.value = '1234')
```

When you use the SearchResources operation to issue the query, the request will look similar to the following. (This example purposefully omits the authorization header and other headers.)

```json
POST /20180409/resources
Host: query.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
  "type": "Structured",
  "query": "query instance resources where (definedTags.namespace = 'rqs' &&
  definedTags.key = 'costcenter' &&
  definedTags.value = '1234')",
  "matchingContextType": "HIGHLIGHTS"
}
```
If your query produces results, the response will list the resources that match the resource type and tag that you specified. The response will look similar to the following:

```json
{
    "items" : [
        {
            "resourceType" : "Instance",
            "identifier" : "ocid1.instance.oc1.phx.exampleawcbfhncvbh3siw2svbprg3bopovy6hgnywfauxq037ckdmr6hjya",
            "compartmentId" : "ocid1.tenancy.oc1..examplea46vssm715wsk5qa7cvb163ctajep4bh61v4vaifauxz6ec7jzg4q",
            "displayName" : "service-pkgs",
            "availabilityDomain" : "ABCd:PHX-AD-1",
            "lifecycleState" : "RUNNING",
            "freeformTags" : {},
            "definedTags" : {
                "rqs" : {
                    "costcenter" : "1234"
                }
            },
            "searchContext" : null
        },
        {
            "resourceType" : "Instance",
            "identifier" : "ocid1.instance.oc1.phx.exampleanb3poce6z4omcvbzw66epp3pvbbww6hz7e2jfaux2lxvi3daxhra",
            "compartmentId" : "ocid1.compartment.oc1..examplea43m3udlwrzwmbcvbk5hm3umk2khgfhhjgcdttawjlfiauxuqwsjiya",
            "timeCreated" : "2018-10-09T23:35:30.167Z",
            "displayName" : "prod-test",
            "availabilityDomain" : "ABCd:PHX-AD-2",
            "lifecycleState" : "RUNNING",
            "freeformTags" : {},
            "definedTags" : {
                "rqs" : {
                    "costcenter" : "1234"
                }
            },
            "searchContext" : null
        },
        {
            "resourceType" : "Instance",
            "identifier" : "ocid1.instance.oc1.phx.exampleanb3poce6z4omcvbzw66epp3pvbbww6hz7e2jfaux2lxvi3daxhra",
            "compartmentId" : "ocid1.compartment.oc1..examplea43m3udlwrzwmbcvbk5hm3umk2khgfhhjgcdttawjlfiauxuqwsjiya",
            "timeCreated" : "2018-10-09T23:35:30.167Z",
            "displayName" : "prod-test",
            "availabilityDomain" : "ABCd:PHX-AD-2",
            "lifecycleState" : "RUNNING",
            "freeformTags" : {},
            "definedTags" : {
                "rqs" : {
                    "costcenter" : "1234"
                }
            },
            "searchContext" : null
        },
        {
            "resourceType" : "Instance",
            "identifier" : "ocid1.compartment.oc1..exampleaexfjsiad7gba6ri4hovmcbk3a5h6k5vulswf544ufauxks4p2jasq",
            "compartmentId" : "ocid1.tenancy.oc1..examplea46vssm715cvb5qa7gg563ctajep4bh61v4vauxf4iz6ec7jzg4q",
            "timeCreated" : "2018-06-12T19:45:24.945Z",
            "displayName" : "BackupTest",
            "availabilityDomain" : "ABCd:PHX-AD-3",
            "lifecycleState" : "STOPPED",
            "freeformTags" : {},
            "definedTags" : {
                "rqs" : {
                    "costcenter" : "1234"
                }
            },
            "searchContext" : null
        },
        {
            "resourceType" : "Instance",
            "identifier" : "ocid1.compartment.oc1..exampleaexfjsiad7gba6ri4hovmcbk3a5h6k5vulswf544ufauxks4p2jasq",
            "compartmentId" : "ocid1.tenancy.oc1..examplea46vssm715cvb5qa7gg563ctajep4bh61v4vauxf4iz6ec7jzg4q",
            "timeCreated" : "2018-06-12T19:45:24.945Z",
            "displayName" : "BackupTest",
            "availabilityDomain" : "ABCd:PHX-AD-3",
            "lifecycleState" : "STOPPED",
            "freeformTags" : {},
            "definedTags" : {
                "rqs" : {
                    "costcenter" : "1234"
                }
            },
            "searchContext" : null
        }
    ]
}
With these results, you can take additional action, if needed. For more information about a resource type, such as its attributes, see its reference page in the API Reference Guide. For the reference pages of resource types that have been indexed for Search, see Supported Resources on page 3626.

Troubleshooting Search

This topic covers common issues related to Search and how you can address them:

- Query or Search Results are Not as Expected on page 3647

Query or Search Results are Not as Expected

There are several reasons why you might not see results that you expect from a search or query.

Not all resource types have been indexed for Search. For a list of currently supported resource types, see Supported Resources on page 3626.

You might not have the required permissions for the resource type that you want to view in search or query results. If there's no policy that grants you the permissions you need, then an administrator must create one for you or add you to a group that's already named in a policy. For more information, see Details for Search.

The query syntax you used might need adjustment. Verify that the conditions in your query language haven't restricted the results to a narrower set than you intended.

If you recently created a resource, it might not show up in search results immediately. Similarly, if you recently updated a resource, your changes might not immediately appear. At times, you might see a resource in a list view before you can see it in search results. The Search service is eventually consistent. Wait, and then try again.
This chapter explains how to use Security Zones.

Security Zones

Security Zones let you be confident that your resources in Oracle Cloud Infrastructure, including Compute, Networking, Object Storage, and Database resources, comply with Oracle security principles.

A security zone is associated with a compartment and a security zone recipe. When you create and update resources in a security zone, Oracle Cloud Infrastructure validates these operations against the list of policies defined in the security zone recipe. If any security zone policy is violated, then the operation is denied.

For example, a security zone policy forbids the creation of public buckets in Object Storage. If you try to create a public bucket in a security zone that has this policy, or if you try to modify an existing storage bucket and make it public, you receive an error message. Similarly, you can't move an existing resource from a standard compartment to a security zone unless all policies are met.

Security zone

An association between a compartment and a security zone recipe. Resource operations in a security zone are validated against all policies in the recipe.

Security zone recipe

A collection of security zone policies.

Security zone policy

A security requirement for resources in a security zone.

Your tenancy has a predefined recipe named Maximum Security Recipe, which includes all available security zone policies. Oracle manages this recipe and you can't modify it.

In general, security zone policies align with these security principles:

• Resources can't be moved from a security zone to a standard compartment because it might be less secure.
• Data in a security zone can't be copied to a standard compartment because it might be less secure.
• All the required components for a resource in a security zone must also be located in a security zone. Resources that are not in a security zone might be vulnerable. For example, a compute instance in a security zone can't use a boot volume that is not in a security zone.
• Resources in a security zone must not be accessible from the public internet.
• Resources in a security zone must be encrypted using customer-managed keys.
• Resources in a security zone must be regularly and automatically backed up.
• Resources in a security zone must use only configurations and templates approved by Oracle.

To learn more, see Security Zone Policies on page 3651.

A security zone policy differs from an IAM policy in the following ways:

• Administrators create IAM policies to grant users the ability to manage certain resources in a compartment.
Security Zones

- A security zone policy ensures that these management operations comply with the Oracle maximum security architecture and best practices.
- A security zone policy is validated regardless of which user is performing the operation.
- A security zone policy denies certain actions; it doesn't grant capabilities.
- Administrators can't create, modify, or disable security zone policies.

To create a security zone, see Managing Security Zones on page 3649.

Managing Security Zones

You can create and delete security zones, and identify the policies enforced in your security zone.

A security zone has the following characteristics:

- Associated with a single compartment that has the same name as the security zone
- Assigned a security zone recipe

As resources are created or modified in the compartment, Oracle Cloud Infrastructure validates these operations against all policies in the security zone recipe.

Your tenancy has a predefined recipe named Maximum Security Recipe, which includes all available security zone policies. Oracle manages this recipe, and you can't modify it.

A security zone compartment can only have subcompartments that are also security zone compartments.

- You can create a security zone in an existing security zone compartment.
- You can move a security zone compartment to another security zone compartment.
- You can't create a standard compartment in a security zone compartment.
- You can't move a standard compartment to a security zone compartment.

**Caution:**

To ensure the integrity of your data, you can't move certain resources from a compartment in a security zone to a compartment that isn't in a security zone.

Required IAM Policy

To work with Security Zones, an administrator must grant you access in an IAM policy.

If you try to perform an action and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted.

For example, the following IAM policy allows users in the group SecurityAdmins to manage security zones in the entire tenancy.

```text
Allow group SecurityAdmins to manage security-zone in tenancy
```

See Security Zone IAM Policies on page 3655.

Creating a Security Zone

Create a security zone by using the Console.

All security zones are assigned the Maximum Security Recipe.

2. Click Create Security Zone.
3. Enter a name and description for the security zone.

Oracle Cloud creates a compartment with the same name and assigns it to this security zone.

Avoid entering confidential information.

4. For Create in Compartment, navigate to the compartment that you want to create the new compartment in.
5. Click Create Security Zone.
To create resources such as networks or compute instances in the new security zone, select the compartment with the same name when you create the resources.

**Viewing the Policies for a Security Zone**

Identify the recipe for an existing security zone, and then view its policies.

1. Open the navigation menu and click **Governance and Administration**. Under **Security**, click **Security Zones**.
2. Click the name of the security zone.
3. Click the recipe for the security zone.

To learn more about a security zone policy in the recipe, see **Security Zone Policies** on page 3651.

**Deleting a Security Zone**

Delete a security zone by using the Console.

To delete a security zone, you delete the compartment that's associated with the security zone.

Before you can delete a compartment, it must be empty of all resources. Ensure that all the compartment's resources have been moved, deleted, or terminated, including any policies attached to the compartment.

- **Note:**
  
  To ensure the integrity of your data, you can't move certain resources from a compartment in a security zone to a compartment that isn't in a security zone.

1. Open the navigation menu and click **Governance and Administration**. Under **Security**, click **Security Zones**.
2. Locate the compartment whose name is the same as the security zone.
3. Click the **Actions** icon (three dots) for this compartment, and then click **Delete Compartment**.
4. At the prompt, click **OK**.

For more information, see **Deleting Compartments**.

**Managing Recipes**

When you create a security zone you assign a recipe to it. A recipe is a collection of security zone policies.

When you perform certain resource operations in a security zone, such as creating a compute instance or a subnet, Oracle Cloud Infrastructure automatically validates the policies within the recipe that is assigned to the security zone.

Your tenancy has a predefined recipe named Maximum Security Recipe, which includes all available security zone policies. Oracle manages this recipe, and you can’t modify it.

**Required IAM Policy**

To work with Security Zones, an administrator must grant you access in an **IAM policy**.

If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted.

For example, the following IAM policy allows users in the group **SecurityAdmins** to manage security zones in the entire tenancy.

```
Allow group SecurityAdmins to manage security-zone in tenancy
```

See **Security Zone IAM Policies** on page 3655.

**Viewing the Policies in a Recipe**

Identify the policies in a security zone recipe by using the Console.

1. Open the navigation menu and click **Governance and Administration**. Under **Security**, click **Security Zones**.
2. Click **Recipes**.
3. Click the name of a recipe.
To learn more about a security zone policy in the recipe, see Security Zone Policies on page 3651.

**Viewing the Security Zones Associated with a Recipe**
Identify the security zones that are associated with a recipe by using the Console.

2. Click Recipes.
3. Click the name of a recipe.
4. Click Associated Security Zones.
To create a security zone, see Managing Security Zones on page 3649.

**Security Zone Policies**
When you create and update resources in a security zone, Oracle Cloud Infrastructure validates these operations against the policies associated with the security zone. If any policy is violated, then the operation is denied.

Security zone policies are categorized by security principle. Each policy impacts one or more resources, such as Compute, Networking, Object Storage, and Database resources.

**Note:**
Database policies do not apply to Oracle Exadata Cloud@Customer.

**Restrict Resource Movement**
To ensure the integrity of your data, you can't move certain resources from a security zone to a standard compartment because it might be less secure. You also can't move an existing resource from a standard compartment to a security zone unless all security zone policies are met.

The following table describes the security zone policies that restrict resource movement.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny block_volume_in_security_zone_move_to_compartment_not_in_security_zone</td>
<td>Block Volume</td>
<td>You can't move a block volume from a security zone to a standard compartment.</td>
</tr>
<tr>
<td>deny boot_volume_in_security_zone_move_to_compartment_not_in_security_zone</td>
<td>Block Volume</td>
<td>You can't move a boot volume from a security zone to a standard compartment.</td>
</tr>
<tr>
<td>deny instance_in_security_zone_move_to_compartment_not_in_security_zone</td>
<td>Compute</td>
<td>You can't move a compute instance from a security zone to a standard compartment.</td>
</tr>
<tr>
<td>deny instance_not_in_security_zone_move_to_compartment_in_security_zone</td>
<td>Compute</td>
<td>You can't move a compute instance from a standard compartment to a compartment that is in a security zone.</td>
</tr>
<tr>
<td>deny subnet_in_security_zone_move_to_compartment_not_in_security_zone</td>
<td>Networking</td>
<td>You can't move a subnet from a security zone to a standard compartment.</td>
</tr>
<tr>
<td>deny bucket_in_security_zone_move_to_compartment_not_in_security_zone</td>
<td>Object Storage</td>
<td>You can't move a bucket from a security zone to a standard compartment.</td>
</tr>
</tbody>
</table>
### Security Zones

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny <code>db_instance_move_to_compartment_not_in_security_zone</code></td>
<td>Database (all types)</td>
<td>You can't move a database from a security zone to a standard compartment.</td>
</tr>
<tr>
<td>deny <code>database_with_dataguard_association_move_to_compartment_in_security_zone</code></td>
<td>Database (Bare metal and virtual machine DB systems, Exadata DB systems)</td>
<td>You can't move a database from a standard compartment to a security zone if its Data Guard association isn't in a security zone.</td>
</tr>
</tbody>
</table>

### Restrict Resource Association

The components of a resource that impact its security posture must also be located in a security zone. Resources that aren't in a security zone might be vulnerable.

The following table describes the security zone policies that restrict resource association.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny <code>block_volume_not_in_security_zone_attach_to_instance_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>All block storage volumes attached to a compute instance in a security zone must themselves be in a security zone.</td>
</tr>
<tr>
<td>deny <code>block_volume_in_security_zone_attach_to_instance_not_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>A compute instance that isn't in a security zone can't be attached to block storage volumes that are in a security zone.</td>
</tr>
<tr>
<td>deny <code>boot_volume_not_in_security_zone_attach_to_instance_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>The boot volume for a compute instance in a security zone must also be in a security zone.</td>
</tr>
<tr>
<td>deny <code>boot_volume_in_security_zone_attach_to_instance_not_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>A compute instance that isn't in a security zone can't be attached to a boot volume that is in a security zone.</td>
</tr>
<tr>
<td>deny <code>instance_in_security_zone_launch_from_boot_volume_not_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>The boot volume for a compute instance in a security zone must also be in a security zone.</td>
</tr>
<tr>
<td>deny <code>instance_not_in_security_zone_launch_from_boot_volume_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>A compute instance that isn't in a security zone can't use a boot volume that is in a security zone.</td>
</tr>
<tr>
<td>deny <code>attached_block_volume_not_in_security_zone_move_to_compartment_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>A block volume can't be moved to a security zone if it's attached to a compute instance that isn't in a security zone.</td>
</tr>
<tr>
<td>deny <code>attached_boot_volume_not_in_security_zone_move_to_compartment_in_security_zone</code></td>
<td>Compute, Block Volume</td>
<td>A boot volume can't be moved to a security zone if it's attached to a compute instance that isn't in a security zone.</td>
</tr>
<tr>
<td>deny <code>instance_in_security_zone_in_subnet_not_in_security_zone</code></td>
<td>Compute, Networking</td>
<td>A compute instance in a security zone must use subnets that are also in a security zone.</td>
</tr>
<tr>
<td>Policy</td>
<td>Services</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>deny dataguard_association_with_db_instances_not_in_security_zones</td>
<td>Database (Bare metal and virtual machine DB systems, Exadata DB systems)</td>
<td>A database in a security zone can have a Data Guard association with another database (primary/standby) only if it's also in a security zone.</td>
</tr>
<tr>
<td>deny db_instance_subnet_not_in_security_zone</td>
<td>Database (all types)</td>
<td>A database in a security zone must use subnets that are also in a security zone.</td>
</tr>
<tr>
<td>deny db_resource_association_not_in_security_zone</td>
<td>Database (Exadata DB systems)</td>
<td>Exadata Infrastructure resources in a security zone can't be associated with Container Databases or VM clusters that aren't in security zones.</td>
</tr>
</tbody>
</table>

### Deny Public Access

Resources in a security zone must not be accessible from the public internet.

When you create a private subnet, compute instances launched in that subnet can't have public IP addresses. This restriction ensures that compute instances in the subnet have no internet access. For compute instances in a private subnet, a *service gateway* enables private access to public services such as Object Storage. See [Overview of Networking](#).

The following table describes the *security zone policies* that restrict network access.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny public_subnets</td>
<td>Networking</td>
<td>Subnets in a security zone can't be public. All subnets must be private.</td>
</tr>
<tr>
<td>deny internet_gateway</td>
<td>Networking</td>
<td>You can't add an <em>internet gateway</em> to a <em>VCN</em> within the security zone.</td>
</tr>
<tr>
<td>deny public_buckets</td>
<td>Object Storage</td>
<td>Object Storage buckets in a security zone can't be public.</td>
</tr>
<tr>
<td>deny db_instance_public_access</td>
<td>Database (all types)</td>
<td>Databases in a security zone can't be assigned to public subnets. They must use private subnets.</td>
</tr>
</tbody>
</table>

### Require Encryption

Resources in a security zone must be encrypted using customer-managed keys. Data must be encrypted while in transit and at rest.

[Oracle Cloud Infrastructure Vault](#) lets you manage the master encryption keys that protect your data and the secret credentials that you use to securely access resources. You can also regularly rotate encryption keys.

Many services integrate with the Vault service for encryption, including Object Storage and Block Volume.

The following table describes the *security zone policies* that enforce encryption.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny_block_volume_without_vault_key</td>
<td>Block Volume</td>
<td>Block <em>volumes</em> in a security zone must use a customer-managed master encryption key in the Vault service. They can't use the default encryption key managed by Oracle.</td>
</tr>
</tbody>
</table>
Security Zones

<table>
<thead>
<tr>
<th>Policy</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny boot_volume_without_vault_key</td>
<td>Block Volume</td>
<td>Boot volumes in a security zone must use a customer-managed master encryption key in the Vault service. They can't use the default encryption key managed by Oracle.</td>
</tr>
<tr>
<td>deny buckets_without_vault_key</td>
<td>Object Storage</td>
<td>Object Storage buckets in a security zone must use a customer-managed master encryption key in the Vault service. They can't use the default encryption key managed by Oracle.</td>
</tr>
</tbody>
</table>

Ensure Data Durability

Automatic backups must be performed regularly for resources in a security zone.

The following table describes the security zone policy that enforces data durability.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny database_without_backup</td>
<td>Database (Bare metal and virtual machine DB systems, Exadata DB systems)</td>
<td>Databases in a security zone must be configured to perform automatic backups. See Backing Up a Database to Oracle Cloud Infrastructure Object Storage.</td>
</tr>
</tbody>
</table>

Ensure Data Security

Data in a security zone is considered privileged and can't be copied to a standard compartment.

The following table describes the security zone policies that enforce data security.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny database_not_in_security_zone_create_from_backup_in_security_zone</td>
<td>Database (Bare metal and virtual machine DB systems, Exadata DB systems)</td>
<td>You can't use a database backup in a security zone to create a database that isn't in a security zone.</td>
</tr>
<tr>
<td>deny database_in_security_zone_create_clone_not_in_security_zone</td>
<td>Database (Virtual machine DB systems, Autonomous Database)</td>
<td>You can't clone a database in a security zone to create a database that isn't in a security zone.</td>
</tr>
</tbody>
</table>

Use Only Configurations Approved by Oracle

Oracle requires certain security features to be enabled and configured for the resources within a security zone. One example is the operating system configuration for a compute instance.

The following table describes the security zone policies that require configurations that are approved by Oracle.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Policy Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny instance_without_sanctioned_image</td>
<td>Compute</td>
<td>All compute instances in a security zone must be created using an Oracle-provided image. You can't create a compute instance from a custom image in a security zone.</td>
</tr>
</tbody>
</table>
Security Zones

<table>
<thead>
<tr>
<th>Policy</th>
<th>Services</th>
<th>Policy Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny free_database_creation</td>
<td>Database (all types)</td>
<td>You can’t create an <em>Always Free database</em> in a security zone.</td>
</tr>
</tbody>
</table>

Security Zone IAM Policies

Create IAM policies to control who has access to security zones and recipes, and to control the type of access for each group of users.

By default, only users in the Administrators group have access to all security zone resources. If you are new to IAM policies, see Getting Started with Policies.

For a complete list of policies in Oracle Cloud Infrastructure, see the Policy Reference.

Resource-Types

The following resource types are related to security zones.

- security-zone

Supported Variables

Security zone IAM policies support all the general policy variables.

See General Variables for All Requests.

Details for Verb + Resource-Type Combinations

Identify the permissions and API operations covered by each verb for security zones.

The level of access is cumulative as you go from inspect to read to use to manage.

security-zone

<table>
<thead>
<tr>
<th>Verb</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>SECURITY_ZONE_INSPECT</td>
</tr>
<tr>
<td>read</td>
<td>SECURITY_ZONE_READ</td>
</tr>
<tr>
<td>use</td>
<td>SECURITY_ZONE_ATTACH, SECURITY_ZONE_UPDATE</td>
</tr>
<tr>
<td>manage</td>
<td>SECURITY_ZONE_CREATE, SECURITY_ZONE_DELETE</td>
</tr>
</tbody>
</table>

Policy Examples

Learn about security zone IAM policies using examples.

Allow users in the group SecurityAdmins to create, update, and delete security zones in the entire tenancy:

Allow group SecurityAdmins to manage security-zone in tenancy

Allow users in the group SecurityAuditors to view security zones in the compartment SalesApps:

Allow group SecurityAuditors to read security-zone in compartment SalesApps
Chapter 33

Security Guide and Announcements

This section of the Oracle Cloud Infrastructure documentation provides a guide to help you securely configure services and resources, and timely announcements relevant to emerging security issues.

• Oracle Cloud Infrastructure Security Guide on page 3656
• Oracle Cloud Security Response to Intel L1TF Vulnerabilities on page 3725
• Oracle Cloud Security Response to Intel Microarchitectural Data Sampling (MDS) Vulnerabilities on page 3731

Oracle Cloud Infrastructure Security Guide

Oracle Cloud Infrastructure enables enterprises to maximize the number of mission-critical workloads that they can migrate to the cloud while continuing to maintain their desired security posture and reduce the overhead of building and operating data-center infrastructure. With Oracle Cloud Infrastructure, enterprise customers get unparalleled control of and transparency into their applications running in the cloud, including:

• Customer isolation that allows you to deploy your application and data assets in an environment that commits full isolation from other tenants and Oracle’s staff, as well as between the same tenant’s workloads.
• Always-on encryption that protects customer data at-rest and HTTPS-only public APIs.
• Easy-to-use IAM policies that allows you to constrain access to your services and segregate operational responsibilities to reduce risk associated with malicious and accidental user actions.
• Security zone policies that allow you to be confident that your resources comply with security principles and best practices related to encryption, network access, and so on.
• Comprehensive log data that allows you to audit and monitor actions on your resources, helping you to meet your audit requirements while reducing security and operational risk.
• Identity federation that allows you to use your existing users and groups in the cloud.
• Support for bringing in third-party software solutions for protecting customer data and resources in the cloud.
• Fault-independent data centers that enable high availability scale-out architectures and are resilient against network attacks, ensuring constant uptime in the face of disaster and security attack.
• Rigorous internal processes and use of effective security controls in all phases of cloud service development and operation.
• Adherence to Oracle’s strict security standards through third-party audits, certifications, and attestations. Oracle helps customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors, and regulators.

All of the Oracle Cloud Infrastructure security capabilities have been designed with one goal in mind: allowing you to run your mission-critical workloads in the cloud with complete control and confidence. Oracle continues to invest in the above areas and more to offer unmatched security and assurance to enterprise customers.

For an overview of Oracle Cloud Infrastructure's security, see Security Overview on page 3657.

Security Overview

Oracle’s mission is to build cloud infrastructure and platform services for your business to have effective and manageable security to run your mission-critical workloads and store your data with confidence.

Oracle Cloud Infrastructure’s security approach is based on seven core pillars. Each pillar has multiple solutions designed to maximize the security and compliance of the platform.

CUSTOMER ISOLATION

Allow customers to deploy their application and data assets in an environment that commits full isolation from other tenants and Oracle’s staff.

DATA ENCRYPTION

Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements for cryptographic algorithms and key management.

SECURITY CONTROLS

Offer customers effective and easy-to-use security management solutions that allow them to constrain access to their services and segregate operational responsibilities to reduce risk associated with malicious and accidental user actions.

VISIBILITY

Offer customers comprehensive log data and security analytics that they can use to audit and monitor actions on their resources, allowing them to meet their audit requirements and reduce security and operational risk.

SECURE HYBRID CLOUD

Enable customers to use their existing security assets, such as user accounts and policies, as well as third-party security solutions when accessing their cloud resources and securing their data and application assets in the cloud.

HIGH AVAILABILITY

Offer fault-independent data centers that enable high availability scale-out architectures and are resilient against network attacks, ensuring constant uptime in the face of disaster and security attack.

VERIFIABLY SECURE INFRASTRUCTURE

Follow rigorous processes and use effective security controls in all phases of cloud service development and operation. Demonstrate adherence to Oracle’s strict security standards through third-party audits, certifications, and attestations. Help customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors, and regulators.

Also, Oracle employs some of the world’s foremost security experts in information, database, application, infrastructure, and network security. By using Oracle Cloud Infrastructure, our customers directly benefit from Oracle’s deep expertise and continuous investments in security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- Keep software up-to-date. This includes the latest product release and any patches that apply to it.
- Limit privileges as much as possible. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Learn about and use the Oracle Cloud Infrastructure security features. For more information, see Security Services and Features on page 3663.
- Use secure best practices. For more information, see Security Best Practices on page 3673.
- Keep up-to-date on security information. Oracle regularly issues security-related patch updates and security alerts. Install all security patches as soon as possible. See the Critical Patch Updates and Security Alerts website.
Understanding the Oracle Cloud Infrastructure Environment

When planning your Oracle Cloud Infrastructure deployment, consider the following:

**Which resources must be protected?**
- Protect customer data, such as credit card numbers.
- Protect internal data, such as proprietary source code.
- Protect system components from being disabled by external attacks or intentional system overloads.

**Who are you protecting data from?**
For example, you must protect your subscribers’ data from other subscribers, but someone in your organization needs to access that data to manage it. Analyze your workflows to determine who needs access to the data. Consider carefully how much access to give a system administrator; it is possible that a system administrator can manage your system components without needing to access the system data.

**What will happen if protections on a strategic resource fail?**
Sometimes, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

**Shared Security Model**
Oracle Cloud Infrastructure offers best-in-class security technology and operational processes to secure its enterprise cloud services. However, for you to securely run your workloads in Oracle Cloud Infrastructure, you must be aware of your security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), and you are responsible for securely configuring your cloud resources. Security in the cloud is a shared responsibility between you and Oracle.

In a shared, multi-tenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data-center facilities, and hardware and software systems) and you are responsible for securing your workloads and configuring your services (such as compute, network, storage, and database) securely.

In a fully isolated, single-tenant, bare metal server with no Oracle software on it, your responsibility increases as you bring the entire software stack (operating systems and above) on which you deploy your applications. In this environment, you are responsible for securing your workloads, and configuring your services (compute, network, storage, database) securely, and ensuring that the software components that you run on the bare metal servers are configured, deployed, and managed securely.

More specifically, your and Oracle's responsibilities can be divided into the following areas:
- **Identity and Access Management (IAM):** As with all Oracle cloud services, you should protect your cloud access credentials and set up individual user accounts. You are responsible for managing and reviewing access for your own employee accounts and for all activities that occur under your tenancy. Oracle is responsible for providing effective IAM services such as identity management, authentication, authorization, and auditing.
- **Workload Security:** You are responsible for protecting and securing the operating system and application layers of your compute instances from attacks and compromises. This protection includes patching applications and operating systems, operating system configuration, and protection against malware and network attacks. Oracle is responsible for providing secure images that are hardened and have the latest patches. Also, Oracle makes it simple for you to bring the same third-party security solutions that you use today.
- **Data Classification and Compliance:** You are responsible for correctly classifying and labeling your data and meeting any compliance obligations. Also, you are responsible for auditing your solutions to ensure that they meet your compliance obligations.
- **Host Infrastructure Security:** You are responsible for securely configuring and managing your compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform (database configuration) services. Oracle has a shared responsibility with you to ensure that the service is optimally configured and secured. This responsibility includes hypervisor security and the configuration of the permissions and network access controls.
required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices.

- **Network Security:** You are responsible for securely configuring network elements such as virtual networking, load balancing, DNS, and gateways. Oracle is responsible for providing a secure network infrastructure.

- **Client and Endpoint Protection:** Your enterprise uses various hardware and software systems, such as mobile devices and browsers, to access your cloud resources. You are responsible for securing all clients and endpoints that you allow to access Oracle Cloud Infrastructure services.

- **Physical Security:** Oracle is responsible for protecting the global infrastructure that runs all of the services offered in Oracle Cloud Infrastructure. This infrastructure consists of the hardware, software, networking, and facilities that run Oracle Cloud Infrastructure services.

For information about using security credentials to access Oracle Cloud Infrastructure, see Security Credentials on page 179.

**Infrastructure Security**

Our security model is built around people, process, tooling, and a common security “platform” of methodologies and approaches from which we build our products. We apply this model to our core security components of Security Culture, Security Design and Controls, Secure Software Development, Personnel Security, Physical Security, and Security Operations that we use to protect and secure our customers and business.

**Security Culture**

We believe that a dynamic security-first culture is vital to building a successful security-minded organization. We have cultivated a holistic approach to security culture in which all our team members internalize the role that security plays in our business and are actively engaged in managing and improving our products' security posture. We have also implemented mechanisms that assist us in creating and maintaining a security-aware culture.

- **Security-minded leadership:** Our senior leadership is actively involved in our security planning, monitoring and management. We define and measure ourselves against security metrics and include security as a component of our team evaluation processes.

- **Embedded expertise:** To help with driving security practices within our team, we have an embedded security-engineering model with security team members sitting and working with our product development teams. This approach enables our security organization to build deep understanding of the product-development processes and system architectures. We are also able to better assist teams in solving security challenges in real time and drive security initiatives more effectively.

- **Common security standards:** We actively work to integrate security into our products and operations. One way we have done this is to establish a security standards baseline. Our objective in creating this baseline is to provide a single security point of reference for business that establishes clear and actionable guidelines. The security baseline is updated frequently to incorporate learned lessons and reflect emerging business factors. We have also created a series of support materials to assist our teams in implementing security controls including reference architectures, implementation guides, and access to security experts.

- **Values of openness, constructive debate, and encouraged escalation:** Security issues can be addressed only when the people who can fix them are aware of them. We believe that openness and transparency, constructive debate, and encouraged escalation make us stronger. We encourage escalation, and we work to create an environment where raising issues early and often is rewarded.

- **Security training awareness:** We maintain robust security and awareness training programs that raise awareness and reinforce our security culture. We require in-depth security training sessions for all new employees as well as annual refresher trainings, and we provide security training that is tailored to our employees’ specific job roles. All our software developers undergo a secure development training that establishes baseline security requirements for product development and provides best practices. We also work to provide engaging and innovative forms of security awareness training such as guest speakers and interactive forums (and we're not above providing food, drinks, or swag to drive attendance).
Security Designs and Controls

Security is integrated into our products and operations through our Oracle Cloud Infrastructure Methodology. This centralized methodology defines our approach for the core security areas that form the security foundation from which we build our products. This approach lends itself to agility and helps us apply best practices and lessons learned from one product across the business, thus raising the security of all our products.

• **User authentication and access control**: Least-privilege access is used to grant access to production systems, and the approved lists of service team members are periodically reviewed to revoke access when there is no justifiable need. Access to production environments requires multi-factor authentication (MFA). The MFA tokens are granted by the security team, and tokens of inactive members are disabled. All access to production systems is logged, and the logs are stored for security analysis.

• **Change management**: Oracle Cloud Infrastructure follows a defined and rigorous change management and deployment process that uses purpose-built proprietary testing and deployment tools. All changes deployed into our production environment follow a testing and approval process prior to release. This process is designed to ensure that changes operate as intended, and can otherwise be rolled back to a previous known good state to recover gracefully from unforeseen bugs or operational issues. We also track the integrity of critical system configurations to ensure that they align with expected state.

• **Vulnerability management**: We use both internal penetration testing teams and external industry experts to help us identify potential vulnerabilities in our products. These exercises help us improve the security of our products, and we work to incorporate the lessons that we learn into our future development work. Oracle Cloud Infrastructure hosts undergo periodic vulnerability scanning using industry-standard scanners. Scan results are triaged to validate applicability of findings to the Oracle Cloud Infrastructure environment, and that applicable findings are patched by our product teams.

• **Incident response**: We have developed strong processes and mechanisms to enable us to respond to and address incidents as they arise. We maintain 24/7 incident response teams ready to detect and respond to events. Our critical staff members carry paging devices that enable us to call on the expertise needed to bring issues to resolution. We have also built a process to help us learn from our incidents. We perform root cause analysis through our Corrective Action/Preventative Action (CAPA) process. CAPAs are intended to discover process gaps and changes that should be made by the business after an incident. CAPAs act as a common language that we can use to reflect on an issue and capture concrete steps to improve future operational readiness. CAPAs capture the root cause of an issue, what is required to contain or fix the issue, and what steps we must take to ensure that the issue does not recur. Our leadership team reviews all CAPAs, looks for cross-organizational applications for learned lessons, and ensures that actions are implemented in a timely manner.

• **Security logging and monitoring**: We have created automated mechanisms to log various security-relevant events (for example, API calls and network events) in the infrastructure, and monitor the logs for anomalous behavior. Alerts generated by monitoring mechanisms are tracked and triaged by the security team.

• **Network security**: By default, customer communications with Oracle Cloud Infrastructure services are done using the latest TLS ciphers and configuration to secure customer data in transit, and hinder any man-in-the-middle attacks. As a further defense in depth, customer commands to the services are digitally signed using public keys, to prevent any tampering. The services also deploy proven, industry-leading tools and mechanisms to mitigate distributed denial of service (DDoS) attacks and maintain high availability.

• **Control plane security**: Oracle Cloud Infrastructure back-end (control plane) hosts are securely isolated from customer instances by using network ACLs. Provisioning and management of customer instances are done by software agents that must interact with the backend hosts. Only authenticated and authorized software agents can successfully interact with Oracle Cloud Infrastructure back-end hosts. For back-end hosts, pre-production environments (for example, dev, test, and integ) are separated from production environments so that any development and test activities do not have any impact on production systems.

• **Server security and media management**: Oracle has a long history of enterprise-class secure hardware development. Our Hardware Security team is responsible for designing and testing the security of the hardware used to deliver Oracle Cloud Infrastructure services. This team works with our supply chain and tests hardware components to validate them against rigorous Oracle Cloud Infrastructure hardware security standards. This team also works closely with our product development functions to ensure that hardware can be returned to a pristine, safe state after being released by customers.

• **Secure host wipe and media destruction**: Oracle Cloud Infrastructure instances are securely wiped after hardware is released by customers. This secure wipe restores hardware to a pristine state. We have re-engineered
the platform with proprietary hardware components that allow us to wipe and reinitialize the hardware in a secure manner. When the underlying hardware has reached end-of-life, it is securely destroyed. Before leaving our data centers, drives are rendered unusable by using industry-leading media destruction devices.

Secure Software Development

Secure product development requires consistently applied methodologies that conform to clear security objectives and principles. We build security practices into every element of our product development life cycle. Oracle employs formal secure product development standards that are a roadmap and guide for developers. These standards discuss general security knowledge areas such as design principles and common vulnerabilities, and provide specific guidance on topics such as data validation, data privacy, and user management.

Oracle secure product development standards have evolved and expanded over time to address the common issues affecting code, new threats as they are discovered, and new use cases by Oracle customers. The standards incorporate insights and learned lessons; they do not live in a vacuum, nor are they an “after the fact” addendum to software development. They are integral to language-specific standards such as C/C++, Java, PL/SQL, and others, and are a cornerstone to Oracle’s secure development programs and processes.

Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis. These tests fit differently in the product development lifecycle and tend to find different categories of issues, so they are used together by Oracle product teams.

Personnel Security

Our people make our business. We strive to hire the best, and we invest in and continue to develop our employees. We value training, and we require not only baseline security training for all our employees but also specialized training to keep our teams abreast of the latest security technologies, exploits, and methodologies. In addition to standard annual corporate training programs that cover our information security and privacy programs (among many others), we engage with a broad spectrum of industry groups and send our employees to specialist conferences to collaborate with other industry experts on emerging challenges. The objectives of our security training programs are to help our employees better protect our customers and products, to enable employees to grow in their knowledge areas around security, and to further our mission to attract and retain the best talent.

We work to recruit the best talent for our team as we grow, and we hire people with strong ethics and good judgment. All our employees undergo pre-employment screening as permitted by law, including criminal background checks and prior-employment validation. We also maintain performance evaluation processes to recognize good performance and help our teams and employees identify opportunities for growth. We maintain both team and employee evaluation processes, and we use security as a component of our team evaluation processes. This approach provides our teams and leadership visibility into how our teams are performing against our security standards and enables us to identify best practices and improvement areas for critical security processes.

Physical Security

Oracle Cloud Infrastructure data centers are designed for security and availability of customer data. This approach begins with our site selection process. Candidate build sites and provider locations undergo an extensive risk evaluation process that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations, among other criteria.

Oracle Cloud Infrastructure data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers housing Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security or availability events that may arise.

We take a layered approach to physical security that starts with the site build. Oracle Cloud Infrastructure data center facilities are durably built with steel, concrete, or comparable materials and are designed to withstand impact from a
light vehicle strike. Our sites are staffed with security guards who are ready to respond to incidents 24 hours a day, 7 days a week, 365 days a year. The exterior of the sites is secured with perimeter barriers and vehicle checks are actively monitored by a guard force and cameras that cover the building perimeter.

All persons entering our data centers must first go through a layer of security at the site entrances, which are staffed with security guards. Persons without site-specific security badges entering the site must present government-issued identification and have an approved access request granting them access to the data center building. All employees and visitors must wear visible, official identification badges at all times. There are additional security layers between the entrance and server rooms that vary depending on the site build and risk profile. Data center server rooms are built with additional security layers including cameras that cover server rooms, two-factor access control, and intrusion-detection mechanisms. Physical barriers are in place to create isolated security zones around server and networking racks that span from the floor (including below the raised floor where applicable) to the ceiling (including above ceiling tiles where applicable).

Access to Oracle Cloud Infrastructure data centers is carefully controlled and follows a least-privilege access approach. All access to server rooms must be approved by authorized personnel and is granted only for the necessary period. Access usage is audited, and access provisioned within the system is periodically reviewed by data-center leadership. Server rooms are isolated into secure zones that are managed on a zone-by-zone basis, and access is provisioned only for those zones required by personnel.

Security Operations

The Oracle Cloud Infrastructure Security Operations team is responsible for monitoring and securing the unique Oracle Cloud Infrastructure hosting and virtual networking technologies. The team works and trains directly with the Oracle engineers who develop these technologies to leverage the unique security and introspection capabilities they provide.

We monitor emerging internet security threats daily and implement appropriate response and defense plans to address risks to the business. When we determine that urgent changes are recommended that are within the scope of the customers’ responsibilities, we issue security alert bulletins to those customers to ensure their protection.

In the case of a detected or reported security issue that affects Oracle Cloud Infrastructure servers or networks, Security Operations staff is available 24/7 to respond, escalate, or take required corrective action. When necessary, we will escalate and coordinate with external parties (including network and hosting service providers, hardware vendors, or law enforcement) to protect Oracle Cloud Infrastructure, our customers, and our network's security and reputation.

All actions performed in response to a security issue by the Security Operations team are done according to our documented process, and are logged in accordance with compliance requirements. Care is always taken to protect the goals of service and data integrity, privacy, and business continuity.

Customer Data Protection

Data Rights and Ownership

Oracle Cloud Infrastructure customers retain all ownership and intellectual property rights in and to their content. Customer data protection is critically important, and we strive to be transparent with our data protection processes as well as law enforcement requests that we might receive.

Data Privacy

Oracle complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Oracle is also responsible for ensuring that third parties who act as an agent on our behalf do the same.

Oracle has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in our privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit https://www.privacyshield.gov/list.
For personal information received or transferred pursuant to the Privacy Shield Framework, Oracle is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

Oracle continues to adhere to the underlying European privacy principles of the U.S.-Swiss Safe Harbor for the processing of Personal Information received from Switzerland. To learn more about the Safe Harbor program, and to view our certification, visit https://safeharbor.export.gov/swisslist.aspx.

**Law Enforcement Requests**

Except as otherwise required by law, Oracle will promptly notify customers of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority that it receives and which relates to the personal data Oracle is processing on the customer’s behalf. Upon customer request, Oracle will provide customers with reasonable information in its possession relevant to the law enforcement request and any assistance reasonably required for them to respond to the request in a timely manner.

**Compliance**

Oracle Cloud Infrastructure is built for enterprises. We operate under practices aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which we have identified a comprehensive set of security controls that apply to our business. Oracle Cloud Infrastructure is still a new product line, and we must operate for a period of time in order for these security controls and our operations to undergo external audit. As an enterprise cloud, we plan to pursue a broad suite of industry and government certifications, audits, and regulatory programs.

**Security Services and Features**

A key objective of Oracle Cloud Infrastructure is to allow you to create a logical extension of your on-premises infrastructure and data centers in Oracle Cloud Infrastructure. You can gain the benefits of a modern public cloud without having to compromise or reinvent your existing security posture. This idea was central to the design of all our infrastructure and services.

**Regions and Availability Domains**

To provide data availability and durability, Oracle Cloud Infrastructure enables you to select from infrastructure with distinct geographic and threat profiles. A region is the top-level component of the infrastructure. Each region is a separate geographic area with multiple, fault-isolated locations called availability domains. An availability domain is the subcomponent of a region and is independent and highly reliable. Each availability domain is built with fully independent infrastructure: buildings, power generators, cooling equipment, and network connectivity. With physical separation comes protection against natural and other disasters. Availability domains within the same region are connected by a secure, high-speed, low-latency network, which allows customers to build and run highly reliable applications and workloads with minimum impact to application latency and performance. All links between availability domains are encrypted. Each region has one or more availability domains, each allowing customers to deploy highly available applications.

**Identity and Access Management (IAM) Service**

The Oracle Cloud Infrastructure Identity and Access Management (IAM) service is built to meet the requirements of enterprises, and it provides authentication and authorization for all their Oracle Cloud Infrastructure resources and services. An enterprise can use a single tenancy shared by various business units, teams, and individuals while maintaining security, isolation, and governance.

When a customer joins Oracle Cloud Infrastructure, a tenancy is created. A tenancy is a virtual construct that contains all of the Oracle Cloud Infrastructure resources that belong to the customer. The administrator of the tenancy can create users and groups and assign them least-privileged access to resources that are partitioned into compartments. A compartment is a group of resources that can be managed as a single logical unit, providing a streamlined way to manage large infrastructure. For example, a customer can create a compartment (HR-Compartment) to host a specific set of cloud network, compute instances, and storage volumes necessary to host its HR applications. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating cloud resources. Customers use them to clearly separate resources for the purposes of isolation (separating the resources for...
one project or business unit from another). A common approach is to create a compartment for each major part of an organization. Unlike most Oracle Cloud Infrastructure services that are regionally scoped, the IAM service resources are global. Customers can have a single tenancy across multiple regions.

The following are key IAM primitives:

• **Resource**: A cloud object that a company’s employees create and use when interacting with Oracle Cloud Infrastructure services, for example, compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, and route tables.

• **Policy**: A set of authorization rules that define access to resources within a tenancy.

• **Compartment**: A heterogeneous collection of resources for the purposes of security isolation and access control.

• **Tenancy**: The root compartment that contains all of an organization’s resources. Within a tenancy, administrators can create one or more compartments, create more users and groups, and assign policies that grant groups the ability to use resources within a compartment.

• **User**: A human being or system that needs access to manage their resources. Users must be added to groups in order to access resources. Users have one or more credentials that must be used to authenticate to Oracle Cloud Infrastructure services. Federated users are also supported.

• **Group**: A collection of users who share a similar set of access privileges. Administrators can grant access policies that authorize a group to consume or manage resources within a tenancy. All users in a group inherit the same set of privileges.

• **Identity Provider**: A trusted relationship with a federated identity provider. Federated users who attempt to authenticate to the Oracle Cloud Infrastructure console are redirected to the configured identity provider. After successfully authenticating, federated users can manage Oracle Cloud Infrastructure resources in the console just like a native IAM user. Currently, Oracle Cloud Infrastructure supports the Oracle Identity Cloud Service and Microsoft Active Directory Federation Service (ADFS) as identity providers. Federated groups are mapped to native IAM groups to define the policies apply to a federated user.

All customer calls to access Oracle Cloud Infrastructure resources are first authenticated by the IAM service (or federated provider) and then authorized based on IAM policies. A customer can create a policy that gives a set of users permission to access the infrastructure resources (network, compute, storage, and so on) within a compartment in the tenancy. These policies are flexible and are written in a human-readable form that is easy to understand and audit. A policy contains one or more policy statements that follow this easy-to-understand syntax:

```
Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>
```

A verb defines the type of access covered. Oracle defines the following verbs that you can use in your policy statements:

• **inspect**: Provides the ability to list resources, without access to any confidential information or user-specified metadata that might be part of that resource.
• **read**: Includes inspect plus the ability to get user-specified metadata and the actual resource itself.
• **use**: Includes read plus the ability to work with existing resources (the actions vary by resource type). Includes the ability to update the resource, except for resource types where the update operation has the same effective impact as the create operation (for example, UpdatePolicy and UpdateSecurityList). In such cases, the update ability is available only with the manage verb. In general, this verb does not include the ability to create or delete that type of resource.
• **manage**: Includes all permissions for the resource.

The following example policy enables the GroupAdmins group to create, update, or delete any groups:

```
Allow group GroupAdmins to manage groups in tenancy
```

Each user has one or more of the following credentials to authenticate themselves to Oracle Cloud Infrastructure. Users can generate and rotate their own credentials. In addition, a tenancy security administrator can reset credentials for any user within their tenancy.

• **Console password**: Used to authenticate a user to the Oracle Cloud Infrastructure Console.
• **API key**: All API calls are signed using a user-specific 2048-bit RSA private key. The user creates a public key pair, and uploads the public key in the Console.
• **Auth token**: Auth tokens are Oracle-generated token strings that you can use to authenticate with third-party APIs that do not support Oracle Cloud Infrastructure's signature-based authentication. For example, use an auth token to authenticate with a Swift client. To ensure sufficient complexity, the token is created by the IAM service and cannot be provided by a customer.
• **Customer secret key**: Used by Amazon S3 clients to access the Object Storage service’s S3-compatible API. To ensure sufficient complexity, the password is created by the IAM service and cannot be provided by a customer.

### Security Zones Service

Security Zones Service will let you be confident that your Compute, Networking, Object Storage, Database and other resources comply with Oracle security principles and best practices. A security zone is associated with a compartment. When you create and update resources in a security zone compartment, Oracle Cloud Infrastructure validates these operations against security zone policies. If any security zone policy is violated, then the operation is denied.

Here are some examples of security zone policies:

• Subnets in a security zone can't be public. All subnets must be private.
• The boot volume for a compute instance in a security zone must also be in a security zone.
• Object Storage buckets in a security zone must use a customer-managed master encryption key.
• You can't move certain resources like block volumes and compute instances from a security zone to a standard compartment.

For more information, see [Security Zones](#).

### Audit Service

Audit Service Service records all API calls to resources in a customer’s tenancy as well as login activity from the graphical management Console. Using the Audit service, customers can achieve their own security and compliance goals by monitoring all user activity within their tenancy. Because all Console, SDK, and command line (CLI) calls go through our APIs, all activity from those sources is included. Audit records are available through an authenticated, filterable query API or can be retrieved as batched files from Oracle Cloud Infrastructure Object Storage. Audit log contents include what activity occurred, the user that initiated it, the date and time of the request, as well as source IP, user agent, and HTTP headers of the request.

### Compute Service

Compute is a core component of Oracle Cloud Infrastructure and provides on-demand and elastic compute capabilities with enterprise-grade security and performance. Customers can provision thousands of compute instances and scale them up or down through an easy-to-use web-based management console. Programmatic support to do the
same is available through feature-rich SDKs and command-line interfaces (CLIs). All compute instances are hosted in Oracle enterprise-grade data centers.

Compute instances are based on high-performance server hardware that uses latest-generation, multi-core server CPUs, large amounts of memory, and high-throughput NVMe local storage. Oracle Cloud Infrastructure provides bare metal (BM) and virtual machine (VM) instances. Customers can choose instances that fit their performance, cost, and software flexibility requirements.

- **Bare metal instances:** In bare metal instances, physical servers are dedicated to a single customer who has complete control over the server. There is no Oracle-managed hypervisor and Oracle personnel have no access to memory or local (NVMe) storage while the instance is running. All network virtualization is performed off-box and only the Oracle Integrated Lights Out Manager (ILOM) is accessible to the infrastructure (required in order to remotely reboot or reprovision instances). These bare metal instances offer consistent high performance and are immune to any noisy-neighbor issues. Customers have OS-level administrative privileges to the bare metal instance. After a customer terminates their bare metal instance, the server undergoes an automated disk and firmware-level wipe process to ensure isolation between customers.

- **Virtual machine (VM) instances:** Customers with flexibility requirements or those who don't need a dedicated bare metal instance can opt for VMs. Multi-tenant customer VMs in Oracle Cloud Infrastructure are managed by a security hardened hypervisor that provides strong isolation between customers.

Oracle Cloud Infrastructure instances use key-based SSH by default. Customers provide the SSH public keys to Oracle Cloud Infrastructure and securely use the SSH private keys for accessing the instances. Oracle recommends using key-based SSH to access Oracle Cloud Infrastructure instances. Password-based SSH could be susceptible to brute-forcing attacks, and are not recommended.

Oracle Linux images hardened with the latest security updates are available for you to run on Oracle Cloud Infrastructure instances. Oracle Linux images run the Unbreakable Enterprise Kernel (UEK) and support advanced security features such as Ksplice to apply security patches without booting, which allows enterprises to live-update their instances without any disruption. In addition to Oracle Linux, Oracle Cloud Infrastructure makes a growing list of other OS images available, including CentOS, Ubuntu, and Windows Server. You can also bring your own custom images. All Oracle-provided images come with secure defaults including OS-level firewalls turned on by default.

**Networking Service**

High-throughput and reliable networking is fundamental to public-cloud infrastructure that delivers compute and storage services at scale. As a result, we invested significant innovation in Oracle Cloud Infrastructure networking to support requirements of enterprise customers and their workloads. Oracle Cloud Infrastructure regions have been built with a state-of-the-art, non-blocking Clos network that is not over-subscribed and provides customers with a predictable, high-bandwidth, low latency network. The data centers in a region are networked to be highly available and have low-latency connectivity between them.

The Oracle Cloud Infrastructure Networking service offers a customizable private network (a VCN, or virtual cloud network) to customers, which enforces logical isolation of customer Oracle Cloud Infrastructure resources. As with their on-premises network in their data centers, customers can set up a VCN with hosts with private IP addresses, subnets, route tables and gateways using VCN. The VCN can be configured for internet connectivity, or connected to the customer's private data center through an IPSec VPN gateway or FastConnect. FastConnect offers a private connection between an existing network's edge router and Dynamic Routing Gateways (DRG). Traffic does not traverse the internet.

The Networking service also supports bi-directional, stateful and stateless firewalls that allow customers to initialize network security access controls. Firewalls and ACLs specified for a customer VCN are propagated throughout the network topology and control plane, ensuring a multi-tiered and defense-in-depth implementation. Each tenant (customer) can create multiple VCNs to implement logical grouping of their resources.

The following are key networking concepts associated with a VCN:

- **Subnets:** The primary subdivision of a VCN. Subnets have historically been specific to an availability domain, but can now be regional (covering all availability domains in the region). Subnets can be marked as private upon creation, which prevents instances launched in that subnet from having public IP addresses.
Security Guide and Announcements

- **Internet gateway**: A virtual router that provides public internet connectivity from a VCN. By default, a newly created VCN has no internet connectivity.
- **Dynamic routing gateway**: A virtual router that provides a path for private traffic between a VCN and a data center’s network. It is used with an IPSec VPN or Oracle Cloud Infrastructure FastConnect connection to establish private connectivity between a VCN and an on-premises or other cloud network.
- **NAT gateway**: A virtual router that gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.
- **Service gateway**: A virtual router that gives cloud resources private access to Oracle services such as Object Storage without using an internet gateway or NAT gateway.
- **Routing tables**: Virtual routing tables that give the subnets access to the VCN’s gateways (Internet Gateway and Dynamic Routing Gateway). Routes can also use private IPs as a target to implement network functionality such as NAT, firewalls, IDS, and so on.
- **Primary VNICs**: Subnets contain virtual network interface cards (VNICs) that attach to instances. The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each instance has a primary VNIC that is created during instance launch and cannot be removed. During instance launch, the Networking service also assigns a public IP address. Customers can override that behavior during instance launch and request to have no public IP address assigned.
- **Secondary VNICs**: VNICs with public and private IP addresses that can be attached to an instance. In a bring-your-own-hypervisor (BYOH) scenario, where customers can run their hypervisor on a BM instance, a secondary VNIC can be assigned to a VM, to allow VCN networking for the VM. This is very useful for running virtual security appliances in a VCN.
- **IPSec VPN connection**: A secure VPN connection between a VCN and a data center.
- **Security lists**: Virtual firewall rules that define allowed ingress and egress to an instance at the packet level. Individual rules can be defined to be stateful or stateless.

Virtual firewalls are implemented by using VCN security lists. Customers can specify a set of firewall rules and associate them with one or more subnets. Associating a security list with a subnet applies those firewall rules to all instances running inside the subnet, at the packet level. There are two types of firewall rules:

- **Ingress rules**: Ingress rules specify the source (IP CIDR and port range), destination port range, and protocol to match on, and are applied to ingress network connections.
- **Egress rules**: Egress rules specify the destination (IP CIDR and port range), source port range, and protocol to match on, and are applied to egress network connections.

Every VCN has a default security list customers may optionally use that allows only SSH and certain types of important ICMP ingress traffic, and all egress traffic. Customers can associate multiple security lists with a subnet. The subnet uses the default security list if the customer doesn’t specify another list for the subnet to use.

For further information about security in the Networking service, see:
- **Ways to Secure Your Network** on page 2830
- **Access Control** on page 2831
- **Security Lists** on page 2850

**Storage Services**

Oracle Cloud Infrastructure offers multiple storage solutions to meet the performance and durability requirements of customers:

- **Local Storage**: NVMe-backed storage on compute instances, offering extremely high IOPS.
- **Block Volumes**: Network-attached storage volumes, attachable to compute instances.
- **Object Storage**: Regional service for storing large amounts of data as objects, providing strong consistency and durability.

The Oracle Cloud Infrastructure Block Volumes service provides persistent storage that can be attached to compute instances using the iSCSI protocol. The volumes are stored in high-performance network storage and support automated backup and snapshot capabilities. Volumes and their backups are accessible only from within a customer's...
VCN and are encrypted at rest using unique keys. For additional security, iSCSI CHAP authentication can be required on a per-volume basis.

The Oracle Cloud Infrastructure Object Storage service provides highly scalable, strongly consistent, and durable storage for objects. API calls over HTTPS provide high-throughput access to data. All objects are encrypted at rest using unique keys. Objects are organized by bucket, and, by default, access to buckets and objects within them requires authentication. Users can use IAM security policies to grant users and groups access privileges to buckets.

To allow bucket access by users who do not have IAM credentials, the bucket owner (or a user with necessary privileges) can create pre-authenticated requests that allow authorized actions on buckets or objects for a specified duration. Alternately, buckets can be made public, which allows unauthenticated and anonymous access. Given the security risk of inadvertent information disclosure, Oracle highly recommends carefully considering the business case for making buckets public. Object Storage enables you to verify that an object was not unintentionally corrupted by allowing an MD5 checksum to be sent with the object (or with each part, in the case of multipart uploads) and returned upon successful upload. This checksum can be used to validate the integrity of the object.

In addition to its native API, the Object Storage service supports Amazon S3 compatible APIs. Using the Amazon S3 Compatibility API, customers can continue to use the existing Amazon S3 tools (for example, SDK clients), and partners can modify their applications to work with Object Storage, with minimal changes to their applications. Their native API can co-exist with the Amazon S3 Compatibility API, which supports CRUD operations. Before customers can use the Amazon S3 Compatibility API, they must create an S3 Compatibility API key. After they've generated the necessary key, they can use the Amazon S3 Compatibility API to access Object Storage in Oracle Cloud Infrastructure.

**Database Service**

Oracle Cloud Infrastructure makes it easy to run, scale, and secure your Oracle databases (DBs) in the cloud. The Oracle Cloud Infrastructure Database service offers three types of DB systems:

- **Bare metal**: Comprising 1-node DB and 2-node Real Application Cluster (RAC) systems, providing exceptional performance at cost-effective pricing.
- **Exadata**: Proven industry-leading Exadata DB systems in quarter, half, and full rack configurations.
- **Virtual machine**: Allows customers to create full-featured Oracle databases on VM shapes with various cores.

DB systems are accessible only from a customer’s VCN, and customers can configure VCN security lists to control network access to their databases. The Database service is integrated with Oracle Cloud Infrastructure IAM for controlling which users can launch and manage DB systems. By default, data is encrypted at rest using Oracle TDE with master keys stored in an Oracle Wallet on each DB system. RMAN backups of DB systems are encrypted and stored in customer-owned buckets in the Object Storage service. Customers need to create a bucket for DB backups and configure the Oracle Database Cloud Backup module with an auth token (to use with the Swift API) and IAM permissions to access the bucket. Alternately, DB backups can be made to local NVMe storage on the DB system.

Each user automatically has the ability to create, update, and delete their own auth tokens in the Console or the API. An administrator does not need to create a policy to give a user those abilities. Administrators (or anyone with permission to the tenancy) also have the ability to manage auth tokens for other users. Any user of a Swift client that integrates with Object Storage needs permission to work with the service.

**Load Balancing Service**

Oracle Cloud Infrastructure Load Balancing provides automated traffic distribution to compute instances in a customer’s VCN. Load balancers (LBs) can be created as public (accepting traffic from the internet and directing it to private instances) or private (directing traffic between private instances). LBs can be configured for SSL termination using customer-provided certificates; end-to-end SSL, whereby the LB terminates the SSL connection and creates a new SSL connection to the backend; or SSL tunneling, in which the SSL connection is passed through to the backend (TCP load balances only). The Load Balancing service supports TLS 1.2 by default, and prioritizes the following forward-secrecy ciphers in the TLS cipher-suite:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
Managed Domain Name Servers (DNS) Service

The Oracle Cloud Infrastructure DNS service provides dynamic, static, and recursive DNS solutions for enterprise customers. The service connects visitors to customer websites and applications with fast and secure services. The DNS service operates on a global anycast network with 18 points of presence (PoPs) on five continents and offers fully redundant DNS constellations and multiple Tier 1 transit providers per PoP. The solution provides a DNS-based Distributed Denial of Services (DDoS) protection and in-house security expertise that leverages a vast sensor network that collects and analyzes over 240 billion data points per day. The DNS service also fully supports the secondary DNS features to complement the customer’s existing DNS service, providing resiliency at the DNS layer.

Vault Service

The Vault service lets you create and manage the encryption keys and secret credentials that you use to protect your data and connect to secured resources. As customer-managed resources, you have complete control over who has access to vaults, keys, and secrets. You also control what authorized users and services can do with Vault resources. Levels of access might range from something as granular as whether an individual key can be used by a particular service to more broadly impactful lifecycle management activities, like whether a user can delete a key from a vault to prevent its use altogether.

Keys are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. The Vault service uses the Advanced Encryption Standard (AES) as its encryption algorithm and its keys are AES symmetric keys. Secrets and secret versions are base64-encoded and encrypted with master encryption keys, but do not reside within the HSM.

If you use the Security Zones service to improve the tenancy’s security posture, security zones require you to encrypt resources using customer-managed keys where possible. The following services support the use of customer-managed keys for resource encryption:

- Block Volume
- Container Engine for Kubernetes
- File Storage
- Object Storage
- Streaming

For more information, see Overview of Vault on page 3952.

Security Advisor

Security Advisor supports the creation of resources that are encrypted with a customer-managed master encryption key, which is one of the security requirements enforced by security zone policies. You can use Security Advisor to create the following resources:

- Object Storage buckets
- File Storage file systems
- Compute virtual machine instances (and associated boot volumes)
- Block Volume block storage volumes

For more information, see Overview of Security Advisor on page 3738.

Oracle Cloud Testing Policies

This section describes the Oracle Cloud Security Testing and Functional Testing policies, tests involving data scraping tools, and how you can submit a request to schedule tests of our services.
Oracle Cloud Security Penetration and Vulnerability Testing

The Oracle Cloud Security Testing policy describes when and how you may conduct certain types of security testing of Oracle Cloud Infrastructure services, including vulnerability and penetration tests, as well as tests involving data scraping tools. Any such testing of Oracle Cloud services may be conducted only by customers who have an Oracle Account with the necessary privileges to file service maintenance requests, and who are signed-in to the environment that will be the subject of such testing.

Oracle regularly performs penetration and vulnerability testing and security assessments against the Oracle Cloud infrastructure, platforms, and applications. These tests are intended to validate and improve the overall security of Oracle Cloud services.

However, Oracle does not assess or test any components (including, non-Oracle applications, non-Oracle databases or other non-Oracle software, code or data, as may be applicable) that you manage through or introduce into – including introduction through your development in or creation in - the Oracle Cloud services (the “Customer Components”). This policy does not address or provide any right to conduct testing of any third-party materials included in the Customer Components.

Except as otherwise permitted or restricted in your Oracle Cloud services agreements, your service administrator who has system level access to your Oracle Cloud services may run penetration and vulnerability tests for the Customer Components included in certain of your Oracle Cloud services in accordance with the following rules and restrictions.

Permitted Penetration and Vulnerability Testing

The following explains where penetration and vulnerability testing of Customer Components is permitted:

- **IaaS**: Using your own monitoring and testing tools, you may conduct penetration and vulnerability tests of your acquired single-tenant Oracle Infrastructure as a Service (IaaS) offerings. You must notify Oracle prior to conducting any such penetration and vulnerability tests in accordance with the process set forth below. Pursuant to such penetration and vulnerability tests, you may assess the security of the Customer Components; however, you may not assess any other aspects or components of these Oracle Cloud services including the facilities, hardware, software, and networks owned or managed by Oracle or its agents and licensors.

- **PaaS**: Using your own monitoring and testing tools, you may conduct penetration and vulnerability tests of your acquired single-tenant Oracle Platform as a Service (PaaS) offerings. You must notify Oracle prior to conducting any such penetration and vulnerability tests in accordance with the process set forth below. Pursuant to such penetration and vulnerability tests, you may assess the security of the Customer Components; however, you may not assess any other aspects or components of these Oracle Cloud services including the facilities, hardware, networks, applications, and software owned or managed by Oracle or its agents and licensors. To be clear, you may not assess any Oracle applications that are installed on top of the PaaS service.

- **SaaS**: Penetration and vulnerability testing is not permitted for Oracle Software as a Service (SaaS) offerings.

Oracle Cloud Security Testing Rules of Engagement

The following rules of engagement apply to cloud penetration and vulnerability testing:

- Your testing must not target any other subscription or any other Oracle Cloud customer resources, or any shared infrastructure components.

- You must not conduct any tests that will exceed the bandwidth quota or any other subscribed resource for your subscription.

- You are strictly prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such, or any “load testing” against any Oracle Cloud asset including yours.

- Any port scanning must be performed in a non-aggressive mode.

- You are responsible for independently validating that the tools or services employed during penetration and vulnerability testing do not perform DoS attacks, or simulations of such, prior to assessment of your instances. This responsibility includes ensuring any contracted third parties perform assessments in a manner that does not violate this policy.

- Social Engineering of Oracle employees and physical penetration and vulnerability testing of Oracle facilities is prohibited.
You must not attempt to access another customer’s environment or data, or to break out of any container (for example, virtual machine).

Your testing will continue to be subject to terms and conditions of the agreement(s) under which you purchased Oracle Cloud services, and nothing in this policy shall be deemed to grant you additional rights or privileges with respect to such Cloud Services.

If you believe you have discovered a potential security issue related to Oracle Cloud, you must report it to Oracle within 24 hours by conveying the relevant information to My Oracle Support. You must create a service request within 24 hours and must not disclose this information publicly or to any third party. Note that some of the vulnerabilities and issues you may discover may be resolved by you by applying the most recent patches in your instances.

In the event you inadvertently access another customer’s data, you must immediately terminate all testing and report it to Oracle within one hour by conveying the relevant information to My Oracle Support.

You are responsible for any damages to Oracle Cloud or other Oracle Cloud customers that are caused by your testing activities by failing to abide by these rules of engagement.

Notification Process
The process for notifying Oracle of your election to conduct a penetration or vulnerability test as required by this policy can be found in Submitting a Cloud Security Testing Notification on page 3672.

Oracle Cloud Functional Testing

Important:
You must abide by the terms of both this policy and the Oracle Cloud Security Testing policy when performing functional testing.

This policy outlines how and when you may conduct functional testing of Oracle Cloud services. The purpose of functional testing is to validate features of Oracle Cloud services to ensure they meet particular functional requirements or specifications. This is often referred to as black-box testing, regression testing, or unit testing whereby functionality of the application is assessed without the need to scrutinize internal structures or source code.

The following rules apply to functional testing of Oracle Cloud services:

You must not conduct any tests in the production environment. Before deployment, you must test all changes in a test environment.

You can perform functional testing using manual or automated tools.

You can conduct functional tests to validate the main functions of the Oracle Cloud service to meet business requirements including usability, accessibility, and error handling.

You must not use functional testing procedures or tools to test other aspects of the Oracle Cloud service, such as performance, reliability, and scalability.

You can conduct unit tests, user-acceptance tests, regression tests, and black-box tests to test the functionality of the Oracle Cloud services.

Data Scraping Tools
Any use of data scraping tools or technologies with Oracle Cloud services to collect data available through any Oracle user interface or via web service calls requires the express written permission of Oracle. Oracle reserves the right to require that your proposed data scraping tools are validated and tested by Oracle prior to use in production, and are subsequently re-validated and tested annually.

Automated Tools
Oracle doesn't make any recommendation on which third-party automated testing tools you can use.

Load Testing Tools
You can't perform automated load testing of Oracle Cloud services.
**Submitting a Cloud Security Testing Notification**

As a service administrator, you can run tests for some Oracle Cloud services. Before running the tests, you must first review the Oracle Cloud Testing Policies on page 3669 section. Follow the steps below to notify Oracle of a penetration and vulnerability test.

**Note:**

You must have an Oracle Account with the necessary privileges to file service maintenance requests, and you must be signed in to the environment that will be the subject of the penetration and vulnerability testing.

1. Log in to My Services.
2. From the service tile in the dashboard, click the **Action** menu, and then select **Maintenance and Service Requests**.
3. On the Service Request Details page, select **Penetration & Vulnerability Testing** from the **Request Type** list.
4. Review the information and accept the terms and conditions, and then click **Next**.

   The available time slots are identified with the text, “Penetration and Vulnerability Testing”.

   You can switch your view to either daily, weekly, monthly, or a list by using the respective buttons on top of the calendar. The view you select is stored as your preference and you’ll be shown the same when you log in the next time.

5. Select an available slot by clicking **Penetration and Vulnerability Testing** on a specific date.
   
   a. Provide technical contact details. If using a third party for testing, then provide the name and email address of the third party.
   
   b. Specify the testing details, such as duration of testing, purpose, IP addresses, services, and other information. Required fields are marked with an asterisk (*).
   
   c. Click **Submit Request**.

A service maintenance request is created and is automatically approved. In some cases, we may require your approval to confirm the time slots of your maintenance. Such requests are indicated by the phrase **To Review**. The status of each filed service maintenance request is color-coded and displayed in the calendar. To view, edit, or cancel your service maintenance request, see Viewing and Editing Service Maintenance Requests. To request a secondary IDCS instance, contact My Oracle Support.

For more information, see Frequently Asked Questions About Cloud Security Testing.

**Frequently Asked Questions About Cloud Security Testing**

This section provides answers to frequently asked questions (FAQ) related to cloud security testing.

To fully understand how you can conduct cloud penetration and vulnerability testing of the **Customer Components**, you must first review the Oracle Cloud Testing Policies on page 3669 section.

Topics:

- **Do I need Oracle’s permission for all penetration and vulnerability tests?**
- **How can I notify Oracle for penetration and vulnerability tests?**
- **Which instances can I test?**
- **What other actions on my part are required after I receive an authorization to perform my tests?**
- **What do I do when I believe that I have discovered a potential security issue related to Oracle Cloud?**
- **What limitations do I need to be aware of regarding my tests?**
- **Can I conduct any tests that may exceed the bandwidth quota for my subscription?**
- **Can I use my hosted instances to conduct assessments against other services not hosted by Oracle?**

**Do I need Oracle’s permission for all penetration and vulnerability tests?**

No. Per the Oracle Penetration and Vulnerability Testing Policy, you do not need Oracle’s permission to conduct penetration and vulnerability tests of the customer components included in certain Oracle Cloud services. However, you will need to notify Oracle prior to commencing such penetration and vulnerability testing. You may not conduct any penetration and vulnerability testing for Oracle Software as a Service (SaaS) offerings.
How can I notify Oracle for penetration and vulnerability tests?

To notify Oracle, you must log into My Services using your administrator credentials associated with the instances you wish to test. You will need to complete and submit a form with information about the instances you wish to test, the planned start and end dates of your test, as well as the testing tools you want to use. This notification process is explained in more detail in the Oracle Cloud Testing Policies on page 3669 section.

Which instances can I test?

The Oracle Penetration and Vulnerability Testing Policy only permits testing of instances, services, and applications that are customer components. All other aspects and components of the Oracle Cloud Services (including Oracle-managed facilities, hardware components, networks, software, and database instances) must not be tested. You may not conduct any penetration and vulnerability testing of Oracle Software as a Service (SaaS) offerings. In addition, you may not attempt to socially engineer Oracle employees or perform physical penetration and vulnerability testing of Oracle facilities.

What other actions on my part are required after I receive an authorization to perform my tests?

No other actions are required before performing your tests. You may conduct your testing for the duration you requested.

What do I do when I believe that I have discovered a potential security issue related to Oracle Cloud?

If you believe you have discovered a potential security issue related to Oracle Cloud, you must report it to Oracle within 24 hours, by conveying the relevant information to My Oracle Support. You must create a service request (SR) within 24 hours and you must not disclose this information publicly or to any third party. Note that some of the vulnerabilities and issues you discovered may be resolved by you, by applying the most recent patches in your instances.

What limitations do I need to be aware of regarding my tests?

All penetration and vulnerability testing against Oracle Software as a Service (SaaS) instances is prohibited. In addition, the Oracle Penetration and Vulnerability Testing Policy sets forth certain rules applicable to the performance of penetration and vulnerability testing on Oracle Cloud Services. See the policy for limitations.

Can I conduct any tests that may exceed the bandwidth quota for my subscription?

No. You are not allowed to conduct any tests that will exceed the bandwidth quota or any other subscribed resource for your subscription.

Can I use my hosted instances to conduct assessments against other services not hosted by Oracle?

No, all testing must be directed at single-tenant Oracle Infrastructure as a Service (Oracle IaaS) or Oracle Platform as a Service (Oracle PaaS) instances hosted by Oracle. These are not to be used as a platform to test other internet-based services.

Security Best Practices

This guide provides actionable guidance and recommendations to Oracle Cloud Infrastructure customers for securely configuring Oracle Cloud Infrastructure services and resources. Understanding Oracle Cloud Infrastructure services and their security features is an essential prerequisite before reading. As a prerequisite, Oracle recommends that you become familiar with security of services. For more information, see Oracle Cloud Infrastructure Security Guide on page 3656.

Security of an Oracle Cloud Infrastructure tenancy is based on a combination of factors, all of which must be thought through and securely configured. From a practical perspective, take a hierarchical view of Oracle Cloud Infrastructure tenancy security configuration, where we start with addressing the foundational security issues. The following steps provide a roadmap of high-level guidelines to follow when configuring security of a tenancy, where we provide a link to a section enumerating detailed security guidance related to each step.

- **User authentication and authorization:** The initial step in securely configuring a tenancy is to create mechanisms for authenticating users and authorizing users to access tenancy resources in a least-privilege manner.
This step comprises creating Oracle Cloud Infrastructure Identity and Access Management (IAM) users, creating IAM groups, formulating authentication mechanisms (for example, Console access using password, API access using API keys, and auth token for object store) for the IAM users created, grouping customer tenancy resources into logical groups using compartments, and formulating IAM security policies authorizing access of IAM groups to tenancy or compartment resources. For enterprises, federating their on-premises users and groups to their tenancy is an important consideration. IAM allows you to create users, groups, security polices, and federation mechanisms. Security recommendations for configuring IAM are provided in the IAM section.

- **Network security architecture:** After formulating IAM user authentication and authorization, a next step is creating a network security architecture for securely running the customer applications and storing their data in a tenancy. All the customer's compute and storage resources are enclosed in a virtual cloud network (VCN) created for the customer. VCN is a software-defined network, resembling the on-premises physical network used by customers to run their workloads. Formulating a VCN security architecture includes tasks such as:
  - Creating VCN subnets for network segmentation
  - Formulating VCN and load balancer firewalls using VCN security lists
  - Using load balancing for high-availability and TLS
  - Determining type of VCN external connectivity whether internet, on-premises network, peered VCN, or combination of these
  - Using virtual network security appliances (for example, next-generation firewalls, IDs)
  - Creating DNS zones and mappings. An important security consideration in load balancers is using customer Transport Layer Security (TLS) certificates to configure TLS connections to customer's VCN. Security recommendations for VCN are provided in the Networking section.

- **Compute instances security configuration:** Within a customer VCN, the customer applications run on compute instances including Bare Metal (BM) instances, Virtual Machine (VM) instances and GPUs. Compute instances are the basic compute building blocks. Bare metal instances have no Oracle-managed software running on them, with the result that the instances and data stored (in memory and local drives) are completely controlled by the customer. VM instances are architected with least privilege mechanisms, and with corporate industry-leading hypervisor security best-practices. Depending on their security and performance requirements, customers have a choice of using BM and VM instances, to run their application workloads in their tenancy. It is imperative to securely configure compute instances, to maintain security of customer applications running on them. Recommendations related to instance security configuration with respect to instance firewalls, instance credential management, entropy, security patching, and security logging and monitoring are provided in the Compute section.

- **Data storage security configuration:** Depending on the type of data and access required, customers can store data in local drives (attached to compute instances), remote block volumes, object store buckets, databases, or file storage in their tenancy. To handle these data storage requirements, Oracle Cloud Infrastructure offers multiple data storage services such as Block Volume, Object Storage, Database, and File Storage. In order to meet their data security requirements, customers need to formulate a tenancy data storage architecture for storing their data in their tenancy, and securely configure the storage services used. Compliance and regulatory requirements are an important factor in determining an appropriate data storage security architecture. Recommendations related to storage services security configuration are available in Block Volume, Object Storage, Database, and File Storage sections. In addition to these services, customers need to consider security of data stored ephemerally in compute instance memory (DRAM) and local NVMe storage.

API Audit logs record calls to APIs (for example, through the Console, SDKs, CLIs, and custom clients using the APIs) as log events. The API Audit logs are always on by default and can’t be turned off. These logs are available to customers for 90 days, with retention period configurable up to 365 days. Information in the API Audit logs show what time API activity occurred, the source of the activity, the target of the activity, what the action was, and what the response was. Oracle recommends that customers periodically review the OCI API Audit logs to ensure they are in accordance with actions they took on their tenancy resources.

For service-specific best practices, see the following topics:

- Securing Block Volume on page 3675
- Securing Compute on page 3677
- Securing Container Engine for Kubernetes on page 3680
- Securing Data Catalog on page 3684
Security Block Volume

Security Recommendations

- There are two types of volumes: block volumes and boot volumes. Block volumes allow instance storage capacity to be expanded dynamically. A boot volume contains the image used to boot the compute instance. The IAM service groups the family of related volume resource types into a combined resource type called volume-family.
- Assign least privilege access for IAM users and groups to resource types in volume-family. The resource types in volume-family are volumes, volume-attachments, and volume-backups. The volume-family resources are detachable block volume devices that allow dynamic expansion of instance storage capacity or contain the image for booting the instance. The volume-attachments resources are attachments between volumes and instances. The volume-backups resources are point-in-time copies of volumes that can be used to create block volumes or recover block volumes.

Data Durability

To minimize loss of data due to inadvertent deletes by an authorized user or malicious deletes, Oracle recommends giving VOLUME_DELETE, VOLUME_ATTACHMENT_DELETE, and VOLUME_BACKUP_DELETE permissions to a minimum possible set of IAM users and groups. DELETE permissions should be given only to tenancy and compartment administrators.

To minimize loss of data due to deletes or corruption, Oracle recommends that you make periodic backups of volumes. Oracle Cloud Infrastructure allows automated scheduled backups. For more information about scheduled backups, see Policy-Based Backups on page 547.

Data-at-rest Encryption

By default, volumes and their backups are encrypted at rest using AES-256. You can also encrypt your data volumes using tools like dm-crypt, veracrypt, and BitLocker. Instructions on dm-crypt encryption are presented in the next section.

Security Policy Examples

Prevent Delete of Volumes

The following example policy allows group VolumeUsers to perform all actions on volumes and backups, except deleting them.

```plaintext
Allow group VolumeUsers to manage volumes in tenancy
   where request.permission!="VOLUME_DELETE"
Allow group VolumeUsers to manage volume-backups in tenancy
   where request.permission!="VOLUME_BACKUP_DELETE"
```

If VolumeUsers can't detach volumes from instances, you can add the following policy to the previous example.

```plaintext
Allow group VolumeUsers to manage volume-attachments in tenancy
```
Security-related Tasks

Encrypting Non-root Volumes with dm-crypt

dm-crypt is a kernel-level encryption mechanism (part of Linux device mapper framework) to provide encrypted volumes. It encrypts data passed from the filesystem (for example, ext4 and NTFS), and stores it on a storage device in Linux Unified Key Setup (LUKS) format. The encrypted volumes can be stored on a complete disk, disk partition, logical volume, or a file-backed storage created using loopback devices. Cryptsetup is the user-level utility used to manage dm-crypt, and used to encrypt partitions and files. dm-crypt uses the Linux crypto APIs for encryption routines.

1. Attach block storage volume to an instance (for example, /dev/sdb)
2. Format /dev/sdb for LUKS encryption. Enter LUKS passphrase when prompted. The passphrase is used to encrypt the LUKS master key used for encrypting the volume.

   cryptsetup -y luksFormat /dev/sdb

3. Verify that the LUKS formatting is successful.

   cryptsetup isLuks /dev/sdb && echo Success

4. Get encryption information about the device.

   cryptsetup luksDump /dev/sdb

5. Get LUKS UUID of the device. The UUID value is used to configure the /etc/crypttab.

   cryptsetup luksUUID /dev/sdb

6. Create a LUKS container with device name, dev_name. This also creates a device node, /dev/mapper/<dev_name>.

   cryptsetup luksOpen /dev/sdb <dev_name>

7. Get information about the mapped device.

   dmsetup info <dev_name>

8. Format the device node as ext4 filesystem.

   sudo mkfs -t ext4 /dev/sdb

9. Mount the device node.

   mount /dev/mapper/<dev_name> /home/encrypt_fs

10. Add an entry to /etc/crypttab.

    <dev_name> UUID=<LUKS UUID of /dev/sdb> none

All the files copied to /home/encrypt_fs are encrypted by LUKS.

11. Add a keyfile to an available keyslot of the encrypted volume. This keyfile can be used to access the encrypted volume.

    dd if=/dev/urandom of=$HOME/keyfile bs=32 count=1
    chmod 600 $HOME/keyfile
    cryptsetup luksAddKey /dev/sdb ~/keyfile
12. Verify the encryption status of files.

```
cryptsetup status /home/encrypt_fs
```

13. Unmount after you're finished.

```
umount /home/encrypt_fs
cryptsetup luksClose <dev_name>
```

To access the encrypted volume:

```
cryptsetup luksOpen /dev/sdb <dev_name> --key-file=/home/opc/keyfile
mount /dev/mapper/<dev_name> /home/encrypt_fs
```

If you lose the keyfile, or if the keyfile or passphrase gets corrupted, you can't decrypt the encrypted volume. This results in permanent loss of data. Oracle recommends that you store durable copies of the keyfile on an on-premises host.

**Remote Mounting of dm-crypt Encrypted Data Volumes**

The following steps assume that the keyfile is on an on-premises host (SRC_IP) and that `<OCI_SSH_KEY>` is the SSH private key of the instance.

1. Copy keyfile from the on-premises host to an instance.

```
scp -i <OCI_SSH_KEY> keyfile opc@SRC_IP:/home/opc
```

2. Open the encrypted volume.

```
ssh i <OCI_SSH_KEY> opc@SRC_IP "cryptsetup luksOpen /dev/sdb <dev_name> --key-file=/home/opc/keyfile"
```

3. Mount the volume.

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "mount /dev/mapper/<dev_name> /home/encrypt_fs"
```

4. Perform operations on data in the mounted volume.

5. Unmount the encrypted volume.

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "umount /home/encrypt_fs"
```

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "cryptsetup luksClose <dev_name>"
```

6. Delete the keyfile from the instance.

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "\rm -f /home/opc/keyfile"
```

**Securing Compute**

**Security Recommendations**

Oracle Cloud Infrastructure Compute provides both bare metal and virtual machine (VM) instances, architected and managed in accordance with security best practices.

**Managing Instances and Credentials**

- To prevent inadvertent or malicious termination of critical instances (for example, production instances), Oracle recommends that you give INSTANCE_DELETE permissions to a minimal set of groups. Give DELETE permissions only to tenancy and compartment administrators.
You can use the Oracle Cloud Infrastructure instance principals feature to authorize instances to access Oracle Cloud Infrastructure services (Compute, Block Volume, Networking, Load Balancing, Object Storage) on behalf of an IAM user. To use this feature, create dynamic groups and grant them access to service APIs. Dynamic groups allow you to group Oracle Cloud Infrastructure computer instances as "principal" actors (similar to user groups). You can then create policies to permit instances to make API calls against Oracle Cloud Infrastructure services.

When you create a dynamic group, rather than adding members explicitly to the group, you instead define a set of matching rules to define the group members. A short-lived private key to sign API calls is delivered through the instance metadata service (http://169.254.169.254/opc/v1/identity/cert.pem), and the key is rotated multiple times a day. For more information about accessing services from instances, see Calling Services from an Instance on page 2410.

**Instance Metadata Access Control**

- Instance metadata (http://169.254.169.254) provides predefined instance information, such as OCID and display name, and custom fields. The instance metadata can also provide short-lived credentials, such as dynamic group credentials. Oracle recommends that you limit instance metadata access to privileged users on the instance. The following example shows how to use iptables to restrict instance metadata access to the root user.

```
iptables -A OUTPUT -m owner ! --uid-owner root -d 169.254.169.254 -j DROP
```

- Instances use link local addresses to access the instance metadata service (169.254.169.254:80), DNS (169.254.169.254:53), NTP (169.254.169.254:123), kernel updates (169.254.0.3), and iSCSI connections to boot volumes (169.254.0.2:3260, 169.254.2.0/24:3260). You can use host-based firewalls, such as iptables, to ensure that only the root user is authorized to access these IPs. Make sure these operating system firewall rules are not altered.

**Instance Network Access Controls**

- Harden secure shell (SSH) on all instances. The following table shows some SSH security recommendations. SSH configuration options can be set in the `sshd_config` file (located at `/etc/ssh/sshd_config` in Linux).

<table>
<thead>
<tr>
<th>Security Recommendation</th>
<th>Configuration sshd_config</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use public-key logins only</td>
<td>PubkeyAuthentication yes</td>
<td>Periodically review SSH public keys in the <code>~/.ssh/authorized_keys</code> file.</td>
</tr>
<tr>
<td>Disable password logins</td>
<td>PasswordAuthentication no</td>
<td>Mitigates password brute-force attacks.</td>
</tr>
<tr>
<td>Disable root logins</td>
<td>PermitRootLogin no</td>
<td>Prevents root privileges for remote logins.</td>
</tr>
<tr>
<td>Change SSH port to a non-standard port</td>
<td>Port &lt;port number&gt;</td>
<td>Optional. Verify that this change does not break applications using port 22 for SSH.</td>
</tr>
</tbody>
</table>

- Use secure SSH private keys to access instances and to prevent inadvertent disclosures. For more information about creating an SSH key pair and configuring an instance with the keys, see Managing Key Pairs on Linux Instances on page 693.

- To limit instance access to authorized IP addresses, use VCN network security groups or security lists. Fail2ban is an application that blocklists IP addresses involved in brute-force sign-in attempts (that is, too many failed attempts to sign in to an instance). By default, Fail2ban inspects SSH accesses, and you can configure it to inspect other protocols. For more information about Fail2ban, see Fail2ban Main Page.

- In addition to VCN network security groups and security lists, use host-based firewalls, such as iptables and firewalld, to restrict network access to instances by controlling ports, protocols, and packet types. Use these firewalls to prevent potential network security attack reconnaissance, such as port scanning and intrusion attempts.
Custom firewall rules can be configured, saved, and initialized on every instance boot. The following example shows commands for iptables.

```
# save iptables rules after configuration
sudo iptables-save > /etc/iptables/iptables.rules
# restore iptables rules on next reboot
sudo /sbin/iptables-restore < /etc/iptables.rules
# restart iptables after restore
sudo service iptables restart
```

### Instance Entropy

Both bare metal and VM instances provide high-quality and high-throughput entropy source. Instances have random number generators whose output is fed into the entropy pools used by the operating system to generate random numbers. In Linux instances, `/dev/random` is non-blocking and should be used for security applications requiring random numbers. You can use the following commands to check the throughput and quality of the random numbers generated by `/dev/random` before using the output in applications.

```
# check sources of entropy
sudo rngd -v
# enable rngd, if not already
sudo systemctl start rngd
# verify rngd status
sudo systemctl status rngd
# verify /dev/random throughput and quality using rngtest
cat /dev/random | rngtest -c 1000
```

### Host Security Hardening and Patching

- Establish a baseline for security hardening of Linux and Windows images running on instances. For more information about security hardening of Oracle Linux images, see Tips for Hardening an Oracle Linux Server. The Center for Internet Security Benchmarks provides a comprehensive set of operating system security hardening benchmarks for various distributions of Linux and Windows Server.
- Keep instance software up to date with security patches. Oracle recommends that you periodically apply the latest available software updates to your instances. Oracle Autonomous Linux images are automatically updated with the latest patches. For Oracle Linux images, you can run the `sudo yum update` command (``sudo dnf update`` on Oracle Linux 8). On Oracle Linux, you can get information about available and installed security patches using the `yum-security` plugin. The following example provides commands for `yum-security`. For Oracle Linux instances launched after February 15, 2017, Ksplice support is available for applying patches without rebooting the instance. For more information about using Ksplice on Oracle Cloud Infrastructure instances, see Installing and Running Oracle Ksplice on page 664.

```
# Install yum-security plugin
yum install yum-plugin-security
# Get list of security patches without installing them
yum updateinfo list security all
# Get list of installed security patches
yum updateinfo list security all
```

### Instance Security Logging and Monitoring

- Various security-related events are captured in log files. Oracle recommends that you periodically review these log files to detect any security issues. In Oracle Linux, the log files are located in `/var/log`. Some security-relevant log files are listed in the following table.

<table>
<thead>
<tr>
<th>Log File or Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/var/log/secure</code></td>
<td>Auth log showing failed and successful sign ins.</td>
</tr>
</tbody>
</table>
Log File or Directory | Description
--- | ---
/var/log/audit | Auditd logs capturing system calls issued, sudo attempts, user sign-ins, and so on. ausearch and aureport are two tools used to query auditd logs.
/var/log/yum.log | Lists packages installed or updated on instances with yum.
/var/log/cloud-init.log | During instance boot, cloud-init can run user-provided scripts as a privileged user. For example, cloud-init can introduce SSH keys. Oracle recommends that you review the cloud-init logs for any unrecognized commands.

Security Policy Examples

In all the following examples, the policies are scoped to a tenancy. However, by specifying a compartment name, they can be scoped down to specific compartment in a tenancy.

Restrict Users Ability to Delete Instances

The following example allows the InstanceUsers group to launch instances, but not to delete them.

- Allow group InstanceUsers to manage instance-family in tenancy where request.permission!='INSTANCE_DELETE'
- Allow group InstanceUsers to use volume-family in tenancy
- Allow group InstanceUsers to use virtual-network-family in tenancy

Restrict Ability to Use Instance Console

For security compliance reasons, some customers do not want to expose the instance console to users in their tenancy. The following policy example restricts ability to create or read from consoles.

- Allow group InstanceUsers to manage instance-console-connection in tenancy where all {request.permission!= INSTANCE_CONSOLE_CONNECTION_READ, request.permission!= INSTANCE_CONSOLE_CONNECTION_CREATE}

Securing Container Engine for Kubernetes

This topic provides security recommendations for using Oracle Cloud Infrastructure's Container Engine for Kubernetes (also known as OKE).

Multi-Tenant Clusters

At this time, it is not recommended to run mutually distrusted workloads in the same cluster. For example, you should not run the following workloads in the same cluster:

- Development workloads and production workloads
- Control plane and data plane
- Workloads that run arbitrary customer code

Additionally, you should consider having separate clusters if you have multiple tenants, teams, or users accessing the same cluster with differing levels of trust. As mentioned in subsequent sections, Kubernetes and OKE offer methods to isolate workloads. However, these methods are not currently sufficient for hard multi-tenancy.

Encrypt Secrets at Rest in Etcd

Please review Encrypting Kubernetes Secrets at Rest in Etcd on page 900 for information on configuring secret encryption.
Role-Based Access Control (RBAC)

Kubernetes ships an integrated Role-Based Access Control (RBAC) component that matches an incoming user or group to a set of permissions which are bundled into roles. These permissions combine verbs (get, create, delete) with resources (pods, services, nodes) and can be scoped to a namespace or cluster. A set of preconfigured roles are provided which offer reasonable default separation of responsibility, depending on what actions a client might want to perform.

It is important to understand how updates on one object may cause actions in other places. For example, a user may not be able to create pods directly, but allowing them to create a deployment, which creates pods on their behalf, will let them create those pods indirectly. Likewise, deleting a node from the API will result in the pods scheduled to that node being terminated and recreated on other nodes. The preconfigured roles represent a balance between flexibility and the common use cases, but more limited roles should be carefully reviewed to prevent accidental privilege escalation. You can make roles specific to your use case if the preconfigured roles don't meet your needs.

You should always follow the principle of least privilege to ensure users and Kubernetes Service Accounts have the minimal set of privileges required. By default, any user with USE CLUSTER access in Oracle Cloud Infrastructure IAM or any Kubernetes Service Account will have no access to the Kubernetes API, except to the discovery roles. See About Access Control and Container Engine for Kubernetes to learn how IAM integrates with OKE.

Note that you cannot currently use IAM Groups in RBAC policies. You must use the OCID of the Principal when creating RBAC bindings (for example, user OCID, instance OCID, and service name).

Cluster Security

You can control the operations that pods are allowed to perform on a cluster you've created with Container Engine for Kubernetes by setting up pod security policies for the cluster. Pod security policies are a way to ensure that pods meet security-related conditions before they can be accepted by a cluster. For example, you can use pod security polices to:

- limit the storage choices available to pods
- restrict the host networking and ports that pods can access
- prevent pods from running as the root user
- prevent pods from running in privileged mode

Having defined a pod security policy for a cluster, you have to authorize the requesting user or pod to use the policy by creating roles and bindings. You can then specify whether a cluster enforces the pod security policies defined for it by enabling the cluster's PodSecurityPolicy admission controller.

For more information, see Using Pod Security Policies with Container Engine for Kubernetes on page 905.

Node Pool Security

Node Pool Compartments

Node pools in a cluster can span compartments. However, while using multiple compartments provides a convenient way to group and manage worker nodes, it does not provide any isolation between the worker nodes in the cluster. Any workload can be scheduled across any node pool regardless of the compartment. A valid use case for using more than one compartment for a node pool would be to easily create dynamic groups and IAM policies for worker nodes. An invalid use case for multiple compartments would be putting each node pool running a customer workload in a separate compartment under the assumption that the compartments are providing some type of security boundary or isolation.

Node Pool Subnets

We recommend only using private subnets for node pools. A service gateway should be configured to provide access to Oracle Cloud Infrastructure services. A service gateway cannot be used if the subnets are public with an internet gateway. If your private subnets require access to the internet, use a NAT gateway.
Controlling Which Nodes Pods May Access

By default, a pod may be scheduled on any node in the cluster. Kubernetes offers a rich set of policies for controlling placement of pods onto nodes and the taint based pod placement and eviction that are available to end users. For many clusters, the use of these policies to separate workloads can be a convention that authors adopt or enforce via tooling. These placement controls are not adequate in a multi-tenant environment when users with deployment capabilities are untrusted. If you have untrusted users deploying code then you should consider a cluster per untrusted group.

Limit Access Given to Instance Principals

By default, all pods on a node are able to access the instance principal certificates using the instance metadata endpoint. In order to avoid privilege escalation via instance principals, you should isolate workloads across node pools with different dynamic groups so that pods in a given node pool have the minimal set of privileges required to function.

For example, assume you have the following two workloads, which both require different access:

- LogArchiver - requires access to manage buckets and objects in Object Storage
- HostMonitor - requires access to the Compute API to manage Instances

The simplest approach would be to schedule them in the same node pool and provide the instance principal with all the required access. However, this increases the impact in the event one of the workloads becomes compromised. A better approach would be to schedule the workloads on separate node pools with the limited set of access the instance principals require for the applicable workload.

Block Container Access to Instance Metadata

The preferred way to block access is using a network policy plugin with a default policy of "deny all". Then you would explicitly grant access to pods and networks using NetworkPolicy resources in Kubernetes via label selectors. If you don't have a network policy plugin installed, you can use a IPTables rule to restrict access from all pods on the host. We recommend that you do not use this approach to block a subset of pods on a host.

Important: NetworkPolicies and the following IPTable rule only apply to containers in the pod overlay network. Containers and services running in the host network are not impacted by either option:

```
iptables --insert FORWARD 1 --in-interface veth+ --destination 169.254.0.0/16 --jump DROP
```

Network Security

Pods running in your OKE Cluster often need to communicate with other pods in the cluster or with services outside the cluster. Container Engine for Kubernetes offers multiple options to secure communication to and from the workloads in your cluster. For the best network security posture, you should evaluate using a combination of network policies (to secure pod-level network communication) and security lists (to secure host-level network communication).

Network Policies

Network policies in Kubernetes allow administrators to define how groups of pods are able to communicate with other pods in the cluster. Additionally, network policies allow you to define how groups of pods are able to communicate with services outside the cluster (for example, Oracle Cloud Infrastructure services).

To restrict access using network policies, you need to install a network plugin. Network plugins configure and enforce the network policies defined in Kubernetes. There are numerous network plugin options. You can follow our instructions here to install and configure Calico in your cluster. Network policy plugins work by restricting access on the host. For information on installing Calico into OKE, see Example: Installing Calico and Setting Up Network Policies on page 960.
Node Pool Security Lists

Network administrators can define security list rules on node pool subnets to restrict access to and from worker nodes. Defining security list rules allows administrators to enforce network restrictions that cannot be overridden on the hosts in your cluster.

Because all pod-to-pod communication occurs in a VXLAN overlay network on the worker nodes, you are cannot use security list rules to restrict pod-to-pod communication. However, you can use security lists to restrict access to and from your worker nodes.

Important: There is a minimum set of security list rules that must exist on node pool subnets to ensure that the cluster can function. See Example Network Resource Configurations on page 840 for information on the minimum set of security list rules before making any changes to your security list rules.

Workload Security Best Practices

Use Image Digests Instead of Tags

We recommend that you only pull images using the image digests, and not pull images using tags (because image tags are mutable). Image digests are the sha256 digest of your image, which allows docker to verify the image it downloaded is what you expected.

Example image digest id:

sha256:77af4d6b9913e693e8d0b4b294fa62ade6054e6b2f1ff617ac955dd63fb0182

Pull the image as shown in the following example:

docker pull acme@sha256:77af4d6b9913e693e8d0b4b294fa62ade6054e6b2f1ff617ac955dd63fb0182

You can use the following command to show all the digests for your local images:

docker images --digests

Limit Resource Utilization

Resource quota limits the number or capacity of resources granted to a namespace. This is most often used to limit the amount of CPU, memory, or persistent disk a namespace can allocate, but can also control how many pods, services, or volumes exist in each namespace.

Limit ranges restrict the maximum or minimum size of some of the resources above, to prevent users from requesting unreasonably high or low values for commonly reserved resources like memory, or to provide default limits when none are specified.

Access to resource quotas can be restricted via RBAC policies in Kubernetes. This can help an administrator ensure that users of a cluster are not able to use resources that they should not have access to. See Limiting resource usage in the on a cluster in the Kubernetes documentation for more information.

Disabling the Tiller Add-on

OKE offers an optional Tiller add-on. This provides an easy way to install and use Helm+Tiller, allowing you to quickly provision and run Kubernetes. It is not recommended to use this add-on for production clusters because of the security risks associated with Tiller. Clusters provisioned with Tiller do not have authentication or authorization for API calls made to Tiller, which means they cannot provide attribution for requests. Therefore, any operator or service that can reach Tiller can invoke its APIs with Tiller access.

To solve the security problems associated with Tiller, Helm V3 was developed. The Helm V3 release completely removed Tiller from Helm. We recommend that you consider using Helm V3 if you’d like to utilize the functionality offered by Helm+Tiller.
Disabling the Kubernetes Dashboard Add-on

OKE offers an optional Kubernetes Dashboard add-on, providing an easy way to install the Kubernetes Dashboard. The Kubernetes Dashboard is installed by OKE with the minimal set of privileges required to run. You will not be able to use the dashboard without providing additional credentials. See Accessing a Cluster Using the Kubernetes Dashboard on page 891 for more information.

The dashboard is particularly useful for new Kubernetes users. We do not recommend installing this add-on on production clusters due to the lack of extensible authentication support. If you do install the Kubernetes Dashboard, we recommend that you restrict access within your cluster, instead of exposing it externally via either a load balancer or an ingress controller. The Kubernetes Dashboard is a common attack vector used to gain access to a Kubernetes Cluster.

Note:
To disable the Kubernetes Dashboard add-on on an existing cluster, contact Oracle Support.

Securing Data Catalog

Oracle Cloud Infrastructure Data Catalog provides a collaborative data discovery and governance solution in accordance with industry-leading security best practices.

Security Recommendations

• Assign least privilege access for IAM users and groups to resource types in data-catalog-family.
• To minimize loss of data due to inadvertent deletes by an authorized user or malicious deletes, Oracle recommends giving CATALOG_DELETE permission to a minimum possible set of IAM users and groups. Give CATALOG_DELETE permissions only to tenancy and compartment admins.
• To protect your data sources from any security vulnerability, provide credentials to read-only accounts only. Data Catalog only needs read access to harvest data assets.

Security Policy Examples

Prevent Delete of Data Catalogs

Create this policy to allow group DataCatalogUsers to perform all actions on data catalogs, except deleting them.

Allow group DataCatalogUsers to manage data-catalog-family in tenancy where request.permission! = 'CATALOG_DELETE'

For more information on creating policies, see Data Catalog Policies.

Securing Data Integration

Oracle Cloud Infrastructure Data Integration provides a collaborative data integration solution in accordance with industry-leading security best practices.

Security Recommendations

• Assign least privilege access for IAM users and groups to resource types in dis-family.
• To minimize loss of data due to inadvertent deletes by an authorized user or malicious deletes, Oracle recommends giving DIS_WORKSPACE_DELETE permission to a minimum possible set of IAM users and groups. Give DIS_WORKSPACE_DELETE permissions only to tenancy and compartment admins.
• To protect your data sources from any security vulnerability, provide credentials to read-only accounts only. Data Integration only needs read access to ingest data from data assets.
Security Policy Examples

Prevent Delete of Workspaces
Create this policy to allow group DISUsers to perform all actions on workspaces, except deleting them.

| Allow group DISUsers to manage dis-family in tenancy where request.permission!='DIS_WORKSPACE_DELETE' |

For more information on creating policies, see Data Integration Policies.

Securing Data Transfer

Oracle offers offline data transfer solutions that let you migrate large amounts of data to buckets in a tenancy in Oracle Cloud Infrastructure. Data transfer solutions include:

- Disk-Based Data Import
  For more information about securely transferring data using this service, see Secure Disk Data Transfer to Oracle Cloud Infrastructure on page 972
- Appliance-Based Data Import
  For more information about securely transferring data using this service, see Secure Appliance Data Transfer to Oracle Cloud Infrastructure on page 1020

Securing Database

Security Recommendations

This section lists security recommendations for managing Oracle Cloud Infrastructure Database instances. Recommendations for securely configuring Oracle databases are available in the Oracle Database Security Guide.

Database Access Control

- Users authenticate to the database using their password. Oracle recommends that these passwords be strong. For guidelines on choosing Oracle database passwords, see Guidelines for Securing Passwords. In addition, Oracle database provides a PL/SQL script to verify database password complexity. This script is located at $ORACLE_HOME/rdbms/admin/UTLPWDMG.SQL. For instructions on running UTLPWDMG.SQL script to verify password complexity, see Enforcing Password Complexity Verification.
- In addition to the database password, you can use VCN network security groups or security lists to enforce network access control to database instances. Oracle recommends that you configure VCN network security groups or security lists to allow least privilege access to customer databases in Oracle Cloud Infrastructure Database.
- DB systems created within a public subnet can send outbound traffic directly to the Internet. DB systems created within a private subnet do not have internet connectivity, and internet traffic (both egress and ingress) cannot reach the instance directly. If you try to define a route to a DB system within a private subnet using an internet gateway, the route is ignored.

To perform OS patching and backup for a DB system on private subnet, you can use a service gateway or a NAT gateway to connect to your patching or backup endpoints.

In an virtual cloud network (VCN), you can use security rules along with a private subnet to restrict access to a DB system. In multi-tier deployments, a private subnet and VCN security rules can be used to restrict access to the DB system from the application tiers.

Data Durability

- Oracle recommends that you give database delete permissions (DATABASE_DELETE, DB_SYSTEM_DELETE) to a minimum possible set of IAM users and groups. This minimizes loss of data due to inadvertent deletes by
an authorized user or due to malicious deletes. Only give DELETE permissions to tenancy and compartment administrators.

- You can use RMAN to do periodic backups of Database databases, where encrypted backup copies are stored in local storage (block volumes, for example) or Oracle Cloud Infrastructure Object Storage. RMAN encrypts each backup of a database with a unique encryption key. In transparent mode, the encryption key is stored in the Oracle Wallet. RMAN backups to Object Storage require internet gateway (IGW), and VCN network security groups or security lists need to be configured to allow secure access to Object Storage. For information about setting up the VCN for backing up bare metal databases, see Backing Up a Database to Oracle Cloud Infrastructure Object Storage on page 1435. For information about backing up and Exadata databases, see Managing Exadata Database Backups by Using bkup_api on page 1323.

**Database Encryption and Key Management**

- All databases created in Oracle Cloud Infrastructure are encrypted using transparent data encryption (TDE). Note that if you migrate an unencrypted database from on-premise to Oracle Cloud Infrastructure using RMAN, the migrated database will not be encrypted. Oracle requires encrypting such databases after migrating them to the cloud.

To learn how to encrypt your database with minimum downtime during migration, see the Oracle Maximum Availability Architecture white paper Converting to Transparent Data Encryption with Oracle Data Guard using Fast Offline Conversion.

Note that virtual machine DB systems use Oracle Cloud Infrastructure block storage instead of local storage. Block storage is encrypted by default.

- User-created tablespaces are encrypted by default in Oracle Cloud Infrastructure Database. In these databases, `ENCRYPT_NEW_TABLESPACES` parameter is set to `CLOUD_ONLY` where tablespaces created in a Database Cloud Service (DBCS) database are transparently encrypted with the AES128 algorithm unless a different algorithm is specified.

- The Database administrator creates a local Oracle Wallet on a newly created database instance, and initializes the Transparent Data Encryption (TDE) master key. Then the Oracle Wallet is configured to be "auto-open". However, a customer can choose to set a password for the Oracle Wallet, and Oracle recommends that you set a strong password (eight characters or more, with at least one capital letter, one small letter, one number, and one special symbol).

- Oracle recommends that you periodically rotate the TDE master key. The recommended rotation period is 90 days or less. You can rotate the TDE master key by using native database commands ("administer key management" in 12c, for example) or dbaascli. All previous versions of TDE master key are maintained in the Oracle Wallet.

- Oracle Key Vault (OKV) is a key management appliance used for managing Oracle TDE master keys. OKV can store, rotate, and audit accesses to TDE master keys. For instructions about installing and configuring OKV in Oracle Cloud Infrastructure, see Managing Oracle Database Encryption Keys in Oracle Cloud Infrastructure with Oracle Key Vault.

**Database Patching**

Applying Oracle database security patches (Oracle Critical Patch Updates) is imperative to mitigate known security issues, and Oracle recommends that you keep patches up-to-date. Patchsets and Patch Set Updates (PSUs) are released on a quarterly basis. These patch releases contain security fixes and additional high-impact/low-risk critical bug fixes.

For information about the latest known security issues and available fixes, see Critical Patch Updates, Security Alerts and Bulletins. If your application does not support the latest patches and needs to use a DB system with older patches, you can provision a DB system with an older version of the Oracle Database edition you are using. In addition to reviewing the critical patch updates and security alerts for your Oracle Database, Oracle recommends that you analyze and patch the operating system provisioned with the DB system.

For information about applying patches to Oracle Cloud Infrastructure Database instances, see Patching a DB System on page 1407 and Patching an Exadata Cloud Service Instance Manually on page 1289.
**Database Security Configuration Checking**

- The Oracle Database Security Assessment Tool (DBSAT) provides automated security configuration checks of Oracle databases in Oracle Cloud Infrastructure. DBSAT performs security checks for user privilege analysis, database authorization controls, auditing policies, database listener configuration, OS file permissions, and sensitive data stored. Oracle database images in Oracle Cloud Infrastructure Database are scanned with DBSAT before provisioning. After provisioning, Oracle recommends that you periodically scan databases with DBSAT, and remediate any issues found. DBSAT is available free of charge to Oracle customers.

**Database Security Auditing**

Oracle Audit Vault and Database Firewall (AVDF) monitors database audit logs and creates alerts. For instructions about installing and configuring AVDF in Oracle Cloud Infrastructure, see Deploying Oracle Audit Vault and Database Firewall in Oracle Cloud Infrastructure.

**Database Backups**

Oracle recommends using Managed backups (backups created using the Oracle Cloud Infrastructure Console or the API) whenever possible. When you use managed backups, Oracle manages the object store user and credentials, and rotates these credentials every 3 days. Oracle Cloud Infrastructure encrypts all managed backups in the object store. Oracle uses the Database Transparent Encryption feature by default for encrypting the backups.

If you are not using managed backups, Oracle recommends that you change the object store passwords at regular intervals.

**Security Policy Examples**

**Prevent Delete of Database Instances**

The following example policy allows the group DBUsers to perform all management actions except delete databases and any artifacts.

```
Allow group DBUsers to manage db-systems in tenancy
   where request.permission!='DB_SYSTEM_DELETE'
Allow group DBUsers to manage databases in tenancy
   where request.permission!='DATABASE_DELETE'
Allow group DBUsers to manage db-homes in tenancy
   where request.permission!='DB_HOME_DELETE'
```

**Securing Email Delivery**

The Email Delivery service offers an SMTP endpoint, secured by a password generated in the Console. The SMTP password is required for sending emails using Email Delivery. Oracle recommends that you create a separate IAM user for SMTP. This user must have manage permissions for approved-senders and suppressions resource types. Oracle recommends that you securely store the SMTP credential, and periodically rotate it. For more information about generating an SMTP credential for Email Delivery, see Generate SMTP Credentials for a User on page 1750.

For Email Delivery best practices, including managing your sender reputation and help for avoiding being blocklisted, see Deliverability Best Practices on page 1780.

**Securing File Storage**

The File Storage Service exposes an NFSv3 endpoint as a mount target in each customer’s VCN subnet. The mount target is identified by a DNS name and is mapped to an IP address. Oracle recommends that you use VCN security lists (of the mount target subnet) to configure network access to the mount target from only authorized IP addresses.

You can mount a file system using the Console or from a Linux command line using NFS utilities. You can authorize users to mount file systems using IAM security policies, but this applies to the console only.
For data durability, Oracle recommends that you take periodic snapshots of the file system. To minimize accidental deletion of data, constrain the set of users having privileges to delete mount targets, file-systems, and snapshots.

All file-system data is encrypted at rest.

Access to mounted NFS file systems from a remote host is determined by POSIX user and group permissions. Oracle recommends that you use well-known NFS security best practices such as the all_squash option to map all users to nfsnobody, and NFS ACLs to enforce access control to the mounted file system.

**Security Policy Examples**

**Prevent Mount Target and File System Deletion**

The following example prevents group FileUsers from deleting mount targets and file-systems.

```plaintext
Allow group FileUsers to manage file-systems in tenancy where request.permission!="FILE_SYSTEM_DELETE"
Allow group FileUsers to manage mount-targets in tenancy where request.permission!="MOUNT_TARGET_DELETE"
Allow group FileUsers to manage export-sets in tenancy where request.permission!="EXPORT_SET_DELETE"
```

**Securing IAM**

**Security Recommendations**

Oracle Cloud Infrastructure Identity and Access Management (IAM) provides authentication of users, and authorization to access resources. Security-relevant IAM concepts include:

**IAM concepts and descriptions**

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compartment</td>
<td>A compartment is a fundamental mechanism to aggregate resources into logical groups. They also provide isolation.</td>
</tr>
<tr>
<td>Tenancy</td>
<td>Oracle Cloud Infrastructure automatically creates a tenancy for an account created by an organization. It is the root compartment that contains all the organization's resources.</td>
</tr>
<tr>
<td>Users and groups</td>
<td>A group is an aggregation of users who need similar access to a group of resources.</td>
</tr>
<tr>
<td>Resource</td>
<td>A resource is an object created in Oracle Cloud Infrastructure services.</td>
</tr>
<tr>
<td>Security policy</td>
<td>A security policy specifies the type of access IAM groups have to resources in a specified aggregation level. An aggregation level can be the tenancy, a compartment, or a service.</td>
</tr>
<tr>
<td>Dynamic groups</td>
<td>A dynamic group allows aggregating Compute instances as principal actors (similar to user groups), in order to authorize instances to make calls to Oracle Cloud Infrastructure APIs.</td>
</tr>
<tr>
<td>Tags</td>
<td>Tags allow you to organize resources across multiple compartments for reporting purposes or for taking bulk actions.</td>
</tr>
</tbody>
</table>
Security Guide and Announcements

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation</td>
<td>Mechanism to federate IAM with other identity providers (IdP) used by an organization to authenticate their users.</td>
</tr>
</tbody>
</table>

Oracle recommends that you periodically monitor Audit logs to review changes to IAM users, groups, and security policies.

**IAM Tenancy and Compartments**

- Compartments are unique to IAM, and offer a mechanism that allows an enterprise customer to meet its central needs by having a single account or tenancy. This single account or tenancy provides full central control and visibility while also allowing the account or tenancy to be subdivided to meet the needs of constituent teams, projects, and initiatives.
- For security and governance reasons, users should only have access to resources they need. For example, enterprise users working on a project or belonging to a business unit should have access only to resources belonging to the project or business unit. Compartments provide an effective mechanism to group tenancy resources based on their access privileges and authorize groups of users to access the compartments on as needed basis. In the example above, a compartment can be created to include all resources belonging to a business unit, and authorize only members of the business unit to access the compartment. Similarly, a groups’ access to a compartment can be revoked when they do not need it anymore.
- Keep the following in mind when you create a compartment and assign resources:
  - Every resource should belong to a compartment.
  - A resource can be reassigned to a different compartment after creation. See Managing Compartments on page 2431.
  - A compartment can be deleted after creation. See Managing Compartments on page 2431.
  - Resource tags provide a way to logically aggregate resources distributed across multiple compartments. For example, tenancy resources can be tagged as `test` or `production` depending on their use. For more information about resource tags (free-form and defined tags), see Resource Tags on page 211.
  - Every tenancy comes with a default administrators group. This group can perform any action on all resources in a tenancy (that is, they have root access to the tenancy). Oracle recommends that you keep the group of tenancy administrators as small as possible. Some security recommendations on managing tenancy administrators:
    - Have security policies granting membership of tenancy administrator group strictly on a as-needed basis.
    - Tenancy administrators should use high-complexity passwords, along with MFA, and periodically rotate their passwords.
    - After account set up and configuration, Oracle recommends that you don't use the tenancy administrator account for day-to-day operations. Instead, create less privileged users and groups.
    - Though administrator accounts are not used for daily operations, they are still needed to address emergency scenarios impacting customer tenancy and operations. Specify secure and auditable "break-glass" procedures for using administrator accounts in such emergencies.
    - Disable tenancy administration access immediately when an employee leaves the organization.
    - Because the tenancy administrator group membership is restricted, Oracle recommends that you create security policies which prevent administrator account lock-out (for example, if the tenancy administrator leaves the company and no current employees have administrator privileges).

**IAM Users and Groups**

- Create an IAM user for everyone in the customer organization who needs access to resources. Do not share IAM user accounts across multiple users, especially those with administrative accounts. Using distinct IAM users enables enforcing least privilege access for each user, and captures their actions in audit logs.
- The recommended unit of administration is IAM groups, which makes it easier to manage and keep track of security permissions (as opposed to individual users). Create IAM groups with permissions to do commonly needed tasks (for example, network administration, volume administration), and assign users to these groups on an as-needed basis. IAM permissions can be used to give a group access to resources across multiple compartments in a tenancy.
• Periodically review membership of IAM users in IAM groups, and remove IAM users from groups they do not need access to anymore. Using group membership to manage user access scales well with increasing number of users.
• Deactivate IAM users who do not need access to tenancy resources. Deleting an IAM user removes the user permanently. You can temporarily deactivate an IAM user by doing the following:
  • Rotate the user password and throw it away.
  • Remove all tenancy permissions of the user by removing membership from all groups.

IAM Credentials
IAM user credentials (Console password, API signing key, auth tokens, and customer secret keys) grant access to resources. It is important to secure these credentials to prevent unauthorized access to Oracle Cloud Infrastructure resources. General guidelines for handling credentials include:
• Create a strong console password for each IAM user, with sufficient complexity. Oracle recommends the following for a complex password:
  • Password has a minimum length of 12 characters
  • Password contains at least one uppercase letter
  • Password contains at least one lowercase letter
  • Password contains at least one symbol
  • Password contains at least one number
• Rotate IAM passwords and API keys regularly, every 90 days or less. In addition to a security engineering best practice, this is also a compliance requirement. For example, PCI-DSS Section 3.6.4 states, "Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined crypto period(s)."
• Do not hard code sensitive IAM credentials directly in software or documents accessible to a wide audience. Examples include code uploaded to GitHub, presentations, or documents available on the internet. There have been known, highly publicized cases of hackers breaching customer cloud accounts, using credentials inadvertently disclosed on public sites. When software applications need to access Oracle Cloud Infrastructure resources, Oracle recommends that you use instance principals. If it is not feasible to use instance principals, other recommendations include using user environment variables to store credentials, and using locally stored credential files with API keys to be used by the Oracle Cloud Infrastructure SDK or CLI.
• Do not share IAM credentials between multiple users.
• By federating the Console login through Oracle Identity Cloud Service, customers can use multifactor authentication (MFA) for IAM users, especially administrators.

When rotating API keys, verify that the rotated keys work as expected before disabling older keys. For information about generating and uploading IAM API keys, see Required Keys and OCIDs on page 4179. The high-level steps in rotating an API key are:
1. Generate and upload a new API key.
2. Update the SDK and CLI configuration files with the new API key.
3. Verify that the SDK and CLI calls are working correctly with the new key.
4. Disable the old API key. Use ListApiKeys to list all active API keys.

IAM Security Policies
IAM policies are used to govern access of IAM groups to resources in compartments and in the tenancy. Oracle recommends that you assign least privilege access to IAM groups for accessing resources. The common format for IAM policies is shown in the following example.

```
Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>
Allow group <group_name> to <verb> <resource-type> in tenancy
```

IAM policies allow four predefined verbs: inspect, read, use and manage. Inspect allows least privilege and manage allows the maximum. The four verbs are shown in increasing order of privilege in the following table.
### IAM policy verbs

<table>
<thead>
<tr>
<th>Verb</th>
<th>Access Type</th>
<th>Example User</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>Should only show metadata. This usually results in ability to list resources only</td>
<td>third-party auditor</td>
</tr>
<tr>
<td>read</td>
<td>inspect plus ability to read resource and user metadata. This is the permission most users need to get work done.</td>
<td>internal auditors</td>
</tr>
<tr>
<td>use</td>
<td>read plus ability to work with resources (the actions vary by resource type). Excludes ability to create or delete resource</td>
<td>regular users (software developers, system engineers, dev managers, etc) setting up and configuring tenancy resources, and applications running on them</td>
</tr>
<tr>
<td>manage</td>
<td>All the permissions for all the resources</td>
<td>administrators, executives (for break-glass scenarios)</td>
</tr>
</tbody>
</table>

The resource types of Oracle Cloud Infrastructure resources are shown in the following table.

### IAM resource families, descriptions, and resource types

<table>
<thead>
<tr>
<th>Resource Type Family</th>
<th>Description</th>
<th>Resource Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-resources</td>
<td>All resource types</td>
<td>compartments, users, groups, dynamic-groups, policies, identity-providers, tenancy tag-namespaces, tag-definitions</td>
</tr>
<tr>
<td>No name by design</td>
<td>Resource types in IAM service</td>
<td>console-histories, instance-console-connection, instance-images, instances, volume-attachments</td>
</tr>
<tr>
<td>instance-family</td>
<td>Resource types in compute service</td>
<td>volumes, volume-attachments, volume-backups</td>
</tr>
<tr>
<td>volume-family</td>
<td>Resource types in block storage</td>
<td></td>
</tr>
<tr>
<td>object-family</td>
<td>Resource types in object storage</td>
<td>buckets, objects</td>
</tr>
<tr>
<td>Resource Type Family</td>
<td>Description</td>
<td>Resource Types</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>database-family</td>
<td>Resource types in DbaaS service</td>
<td>db-systems, db-nodes, db-homes, databases, backups</td>
</tr>
<tr>
<td>load-balancers</td>
<td>Resources in Load Balancer service</td>
<td>load-balancers</td>
</tr>
<tr>
<td>file-family</td>
<td>Resources in file storage service</td>
<td>file-systems, mount-targets, export-sets</td>
</tr>
<tr>
<td>dns</td>
<td>Resources in DNS service</td>
<td>dns-zones, dns-records, dns-traffic</td>
</tr>
<tr>
<td>email-family</td>
<td>Resources in email delivery service</td>
<td>approved-senders, suppressions</td>
</tr>
</tbody>
</table>

For more information about IAM verbs and resource type permission mappings, see [Details for the Core Services](#) on page 2181.

IAM security policies can be made fine-grained through conditions. Access specified in the policy is allowed only if the condition statements evaluate to true. Conditions are specified using predefined variables. The variables use the key words request or target, depending on whether the variable is relevant to the request or the resource being acted on, respectively. For information about supported predefined variables, see [Policy Reference](#) on page 2167.

IAM dynamic groups are used to authorize Compute instances to access Oracle Cloud Infrastructure APIs. The instance principals feature can be used by applications, running on the instances, to programmatically access Oracle Cloud Infrastructure services. Customers create dynamic groups, which include instances as members, and authorize access to their tenancy resources using IAM security policies. All access by instances is captured in the audit logs available to customers.

**IAM Federation**

- Oracle recommends that you use federation to manage logins into the Console. Identity federation supports SAML 2.0 compliant identity providers, and can be used to federate on-premises users and groups to IAM users and groups. The enterprise administrator needs to set up a federation trust between the on-premises identity provider (IdP) and IAM, in addition to creating mapping between on-premises groups and IAM groups. Then, on-premises users can single sign-on (SSO) into the Console, and access resources based on authorization of IAM groups they belong to. For more information about federating to the Console, see [Federating with Identity Providers](#) on page 2362. Federation is especially important for enterprises using custom policies for user authentication (for example, multifactor authentication). For more information about managing users and groups under federation, see [Federating with Identity Providers](#) on page 2362.

- When using federation, Oracle recommends that you create a federation administrators group that maps to the federated IdP administrator group. The federation administrators group will have administrative privileges to manage customer tenancy, while being governed by the same security policies as the federated IdP administrator group. In this scenario, it is a good idea to have access to the local tenancy administrator user (that is, member of the default tenancy administrator IAM group), to handle any break-glass type scenarios (for example, inability to access resources through federation). However, you must prevent any unauthorized use of this highly privileged...
local tenancy administrator user. Oracle recommends the following approach to securely managing the tenancy administrator user:

1. Create a local user belonging to the default tenancy administrator group.
2. Create a highly complex Console password or passphrase (18 characters or more, with at least one lowercase letter, one uppercase letter, one number, and one special character) for the local tenancy administrator user.
3. Securely escrow the local tenancy administrator user password in an on-premises location (for example, place the password in a sealed envelope in an on-premises physical safe).
4. Create security policies for accessing the escrowed password only under specific "break-glass" scenarios.
5. Have IAM security policy to prevent the federated administrators IAM group from adding or modifying membership of the default tenancy administrator group to prevent security by-passes.
6. Monitor audit logs for accesses by default tenancy administrator and changes to the administrator group, to alert on any unauthorized actions. For additional security, the local tenancy administrator user password can be rotated after every login, or periodically, based on a password policy.

For an example that shows the way various IAM components fit together, see Example Scenario on page 2126. Periodically monitor Audit logs to review changes to IAM users, groups, policies, compartments, and tags.

**Security Policy Examples**

Common IAM security policy examples are available at Common Policies on page 2142. In all the examples that follow, the policies are scoped to a tenancy. However, by specifying a compartment name, you can scope down the policies to specific compartments in a tenancy.

**Create Service-level Admins for Least Privilege**

To implement security principle of least privilege, you can create service-level admins in the tenancy to further scope down administrative access. This means that service-level administrators can only manage resources of a specific service. For instance, network administrators need administrative (manage) access only to VCN resources, and not to other resources. The following example shows how to create administrator groups for block storage (VolumeAdmins), VCN (NetworkAdmins), databases (DBAdmins), and object storage (StorageAdmins).

| Allow group TenancyAdmins to manage all-resources in tenancy |
| Allow group VolumeAdmins to manage volume-family in tenancy |
| Allow group NetworkAdmins to manage virtual-network-family in tenancy |
| Allow group StorageAdmins to manage object-family in tenancy |
| Allow group DBAdmins to manage database-family in tenancy |

You can further constrain the security policies to a specific compartment. For example, the HR department in an enterprise can create group HRAdmins to manage resources within its compartment, HR-compartment. The HRNetworkAdmins group has administrative access to VCN resources only within the HR-compartment compartment.

| Allow group HRAdmins to manage all-resources in compartment HR-compartment |
| Allow group HRNetworkAdmins to manage virtual-network-family in compartment HR-compartment |

Compliance auditors are tasked with examining cloud resources and verifying for policy violations. The following policy allows group InternalAuditors to inspect (list) all resources in a tenancy.

| Allow group InternalAuditors to inspect all-resources in tenancy |

If you want to limit auditors to only inspect users and groups in a tenancy, you can create a group UserAuditors with the following policy:

| Allow group UserAuditors to inspect users in tenancy |
| Allow group UserAuditors to inspect groups in tenancy |
If you want to create an auditor group that can only inspect VCN firewalls in the tenancy, use the following policy:

```
Allow group FirewallAuditors to inspect security-lists in tenancy
```

In all the policy examples, you can constrain the policies to a compartment by specifying `Compartment <name>` (where `<name>` is the compartment name) in the policy.

**Restrict Ability to Change Tenancy Administrators Group Membership**

Members in the group Administrators can manage all resources in a tenancy. Membership of the Administrators group is controlled by users in the group. Usually, it's convenient to have a group to create and add users in the tenancy, but restrict them from making changes to the Administrators group membership. The following example creates a group UserAdmins to do this.

```
Allow group UserAdmins to inspect users in tenancy
Allow group UserAdmins to inspect groups in tenancy
Allow group UserAdmins to use users in tenancy
  where target.group.name!='Administrators'
Allow group UserAdmins to use groups in tenancy
  where target.group.name!='Administrators'
```

Use verb with conditions (third and fourth policy statements) allows UserAdmins to add users and groups using APIs (UpdateUser, UpdateGroup) to all groups in the tenancy except the Administrators group. However, because `target.group.name!='Administrators'` is not related to the list and get APIs (ListUsers, GetUser, ListGroups, and GetGroup), these APIs will fail. So you must explicitly add the inspect verb (first and second policy statements) to allow UserAdmins to get user and group membership information.

**Prevent Delete or Update of Security Policies**

The following example creates a group PolicyAdmins to be able to create and list security policies created by tenancy administrators, but not delete or update them.

```
Allow group PolicyAdmins to use policies in tenancy
Allow group PolicyAdmins to manage policies in tenancy
  where request.permission='POLICY_CREATE'
```

This security policy statement explicitly only allows POLICY_CREATE permission, and not to POLICY_DELETE and POLICY_UPDATE.

**Prevent Admins from Accessing or Altering User Credentials**

Some compliance requirements need separation of duties, especially where user credential management functionality is separated from tenancy management. In this case, you can create two administration groups, TenancyAdmins and CredentialAdmins where TenancyAdmins can perform all tenancy management functions except user credential management, and CredentialAdmins can manage user credentials. TenancyAdmins can access all APIs except those that list, update, or delete user credentials. CredentialAdmins can only manage the user credentials.

```
Allow group TenancyAdmins to manage all resources in tenancy
  where all {request.operation!='ListApiKeys',
               request.operation!='ListAuthTokens',
               request.operation!='ListCustomerSecretKeys',
               request.operation!='UploadApiKey',
               request.operation!='DeleteApiKey',
               request.operation!='UpdateAuthToken',
               request.operation!='CreateAuthToken',
               request.operation!='DeleteAuthToken',
               request.operation!='CreateSecretKey',
               request.operation!='UpdateCustomerSecretKey',
```
Allow group CredentialAdmins to manage users in tenancy where any request.operation='ListApiKeys', request.operation='ListAuthTokens', request.operation='ListCustomerSecretKeys', request.operation='UploadApiKey', request.operation='DeleteApiKey', request.operation='UpdateAuthToken', request.operation='CreateAuthToken', request.operation='DeleteAuthToken', request.operation='CreateSecretKey', request.operation='UpdateCustomerSecretKey', request.operation='DeleteCustomerSecretKey'}

Useful CLI Commands

In all the following examples, environment variables $T$ and $C$ are set to tenancy OCID and compartment OCID, respectively.

**List Compartments in a Tenancy**

```
# list all compartments (OCID, display name, description) in tenancy $T
oci iam compartment list -c $T
# grep above command for important fields
oci iam compartment list -c $T | grep -E "name\ndescription\nid""
```

**List IAM Users**

```
# lists all users (OCID, display name, description) in tenancy $T
oci iam user list -c $T
# grep above command for important fields
oci iam user list -c $T | grep -E "name\ndescription\nid"
```

**List IAM groups**

```
# lists all groups (OCID, display name, description) in tenancy $T.
oci iam group list -c $T
# grep above command for important fields
oci iam group list -c $T | grep -E "name\ndescription\nid"
```

**List Users in a Group**

The following command is helpful for listing users in groups, especially users with administrative privileges. This command requires the OCID of the group whose users are listed.

```
# list users in group with OCID <GROUP_OCID>
oci iam group list-users -c $T --group-id <GROUP_OCID>
```

**List Security Policies**

```
# lists all policies (OCID, name, statements) in tenancy $T. Remove pipe to
grep to get entire information
oci iam policy list -c $T
# grep above command for important fields
oci iam policy list -c $T | grep -E "name\nAllow\nid"
```
Securing Networking: VCN, Load Balancers, and DNS

Security Recommendations

The Networking service has a collection of features for enforcing network access control and securing VCN traffic. These features are listed in the following table.

<table>
<thead>
<tr>
<th>VCN Feature</th>
<th>Security Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public and private subnets</td>
<td>Your VCN can be partitioned into subnets. Subnets have historically been specific to an availability domain, but can now be regional (covering all availability domains in the region). Instances inside private subnets cannot have public IP addresses. Instances inside public subnets can optionally have public IP addresses at your discretion.</td>
</tr>
<tr>
<td>Security rules</td>
<td>Security rules provide stateful and stateless firewall capability to control network access to your instances. To implement security rules in your VCN, you can use network security groups (NSGs) or security lists. For more information, see Comparison of Security Lists and Network Security Groups on page 2833.</td>
</tr>
<tr>
<td>Gateways</td>
<td>Gateways let resources in a VCN communicate with destinations outside the VCN. The gateways include:</td>
</tr>
<tr>
<td></td>
<td>• Internet gateway: for internet connectivity (for resources with public IP addresses in public subnets)</td>
</tr>
<tr>
<td></td>
<td>• NAT gateway: for internet connectivity without exposing the resources to incoming internet connections (for resources in private subnets)</td>
</tr>
<tr>
<td></td>
<td>• Dynamic routing gateway (DRG): for connectivity to networks outside the VCN's region (for example, your on-premises network by way of an IPSec VPN or FastConnect, or a peered VCN in another region)</td>
</tr>
<tr>
<td></td>
<td>• Service gateway: for private connectivity to Oracle services such as Object Storage</td>
</tr>
<tr>
<td></td>
<td>• Local peering gateway (LPG): for connectivity to a peered VCN in the same region</td>
</tr>
<tr>
<td>Route table rules</td>
<td>Route tables control how traffic is routed from your VCN's subnets to destinations outside the VCN. Routing targets can be VCN gateways or a private IP address in the VCN.</td>
</tr>
<tr>
<td>IAM polices for virtual-network-family</td>
<td>IAM policies specify access and actions permitted by IAM groups to resources in a VCN. For example, IAM polices can give administrative privileges to network administrators who manage the VCNs, and scoped-down permissions to normal users.</td>
</tr>
</tbody>
</table>

Oracle recommends that you periodically monitor Oracle Cloud Infrastructure Audit logs to review changes to VCN network security groups, security lists, route table rules, and VCN gateways.
Network Segmentation: VCN Subnets

• Formulate a tiered subnet strategy for the VCN, to control network access. A common design pattern is to have the following subnet tiers:

1. DMZ subnet for load balancers
2. Public subnet for externally accessible hosts such as NAT instances, intrusion detection (IDS) instances, and web application servers
3. Private subnet for internal hosts such as databases

No special routing is required for the instances in the different subnets to communicate. However, you can control the types of traffic between the different tiers by using the VCN's network security groups or security lists.

• Instances in the private subnet only have private IP addresses and can be reached only by other instances in the VCN. Oracle recommends that you place security-sensitive hosts (DB systems, for example) in a private subnet, and use security rules to control the type of connectivity to hosts in a public subnet. In addition to VCN security rules, configure host-based firewalls such as iptables, firewalld for network access control, as a defense-in-depth mechanism.

• You can add a service gateway to your VCN to enable DB systems in the private subnet to directly back up to Object Storage without the traffic traversing the internet. You must set up the routing and security rules to enable that traffic. For more information for bare metal or virtual machine DB systems, see Network Setup for DB Systems on page 1359. For more information for Exadata DB systems, see Network Setup for Exadata Cloud Service Instances on page 1232.

Network Access Control: VCN Security Rules

• Use your VCN’s security rules to restrict network access to instances. A security rule is stateful by default, but can also be configured to be stateless. A common practice is to use stateless rules for high-performance applications. In a case where network traffic matches both stateful and stateless security lists, the stateless rule takes precedence. For more information about configuring VCN security rules, see Security Rules on page 2833.

• To prevent unauthorized access or attacks on Compute instances, Oracle recommends that you use a VCN security rule to allow SSH or RDP access only from authorized CIDR blocks rather than leave them open to the internet (0.0.0.0/0). For additional security, you can temporarily enable SSH (port 22) or RDP (port 3389) access on an as-needed basis using the VCN API UpdateNetworkSecurityGroupSecurityRules (if you're using network security groups) or UpdateSecurityList (if you're using security lists). For more information about enabling RDP access, see To enable RDP access in Creating an Instance on page 695. For performing instance health checks, Oracle recommends that you configure VCN security rules to allow ICMP pings. For more information, see Rules to Enable Ping on page 2841.

• Oracle recommends bastion hosts as a way to control external access (for example, SSH) to VCN hosts. Usually bastion hosts in a VCN public subnet control access to VCN private subnet hosts. For more information about setting up an SSH bastion host in a VCN, see the white paper Bastion Hosts.

• VCN network security groups (NSGs) and security lists enable security-critical network access control to Compute instances, and it is important to prevent any unintended or unauthorized changes to NSGs and security lists. To prevent unauthorized changes, Oracle recommends that you use IAM policies to allow only network administrators to make NSG and security list changes.

Secure Connectivity: VCN Gateways and FastConnect Peering

• VCN gateways provide external connectivity (internet, on-premises, or peered VCN) to VCN hosts. See the table earlier in this topic for a list of the type of gateways. Oracle recommends that you use an IAM policy to allow only network administrators to create or modify VCN gateways.
• Carefully consider allowing internet access to any instances. For example, you don't want to accidentally allow internet access to sensitive database instances. In order for an instance in a VCN to be publicly accessible from the internet, you must configure the following VCN options:

  • The instance must be in a VCN public subnet.
  • The VCN containing the instance must have an internet gateway enabled and configured to be the routing target for outbound traffic.
  • The instance must have a public IP address assigned to it.
  • The VCN security list for the instance's subnet must be configured to allow inbound traffic from 0.0.0.0/0. Or if you're using network security groups (NSG), the instance must be in an NSG that allows that traffic.

• VPN IPSec provides connectivity between a customer's on-premises network and VCN. You can create two IPSec tunnels for high availability. For more information about creating VPN tunnels to connect VCN DRG to customer CPEs, see VPN Connect on page 2932.

• FastConnect peering allows you to connect your on-premises network to your VCN with a private circuit so that the traffic does not traverse the public internet. You can set up private peering (to connect to private IP addresses), or public peering (to connect to Oracle Cloud Infrastructure public endpoints, such as for Object Storage). For more information about FastConnect peering options, see FastConnect on page 3173.

Virtual Security Appliances in a VCN

• The Networking service lets you implement network security functions such as intrusion detection, application-level firewalls, and NAT (although you can instead use a NAT gateway with your VCN). You can do this by routing all the subnet traffic to a network security host, using route table rules that use a local VCN private IP address as a target. For more information, see Using a Private IP as a Route Target on page 2924. For high availability, you can assign the gateway security host a secondary private IP address, which you can move to a VNIC on a standby host in case of primary host failure. Full network packet capture or network flow logs can be captured on the NAT instances using tcpdump, and the logs can be uploaded periodically to an Object Storage bucket.

• Virtual security appliances can be run as virtual machines (VMs) on a bring-your-own-hypervisor (BYOH) model on a bare metal instance. Virtual security appliance VMs running on the BYOH bare metal instance each have their own secondary VNIC, giving direct connectivity to other instances and services in the VNIC's VCN. For information about enabling BYOH on a bare metal instance using an open-source KVM hypervisor, see Installing and Configuring KVM on Bare Metal Instances with Multi-VNIC.

• Virtual security appliances can also be installed on Compute virtual machines (VMs) where VMDK or QCOW2 images of security appliances can be imported using the bring your own image (BYOI) feature. However, due to infrastructure dependencies, the BYOI feature might not work for some appliances, in which case the BYOH model would be another option to use. For more information about importing appliance images into Oracle Cloud Infrastructure, see Bring Your Own Image (BYOI) on page 675.

Load Balancers

• Oracle Cloud Infrastructure load balancers enable end-to-end TLS connections between a client's applications and a customer's VCN. The TLS connection can be terminated at an HTTP load balancer, or on a back-end server by using a TCP load balancer. The load balancers use TLS1.2 by default. For information about configuring an HTTPS listener, see Managing Listeners on page 2522. You can also upload your own TLS certificates. For more information see Managing SSL Certificates on page 2551.

• You can configure network access to load balancers by using VCN network security groups or security lists. This method provides similar functionality to traditional load balancer firewalls. For public load balancers, Oracle recommends that you use a regional public subnet (for example, DMZ subnet) for instantiating the load balancers in a highly available configuration across two different availability domains. You can configure the load balancer firewall rules by setting up the load balancer's network security groups or the subnet's security lists. For more information about creating load balancer security lists, see Update Load Balancer Security Lists and Allow Internet Traffic to the Listener on page 114. Similarly, you must configure the VCN network security groups or security lists for the backend servers to limit traffic only from the public load balancers. For more information
about configuring backend server security lists, see Update Rules to Limit Traffic to Backend Servers on page 116.

**DNS Zones and Records**

DNS zones and records are critical for accessibility of web properties. Incorrect updates or unauthorized deletions could result in outage of services, accessed through the DNS names. Oracle recommends that you limit IAM users who can modify DNS zones and records.

**Security Policy Examples**

**Allow Users to Only View Security Lists**

Your network administrators are the personnel who should have the ability to create and manage network security groups and security lists.

However, you may have network users who need to know what security rules are in a particular network security group (NSG) or security list.

The first line in the following example policy allows the NetworkUsers group to view security lists and their contents. This policy does not let the group create, attach, delete, or modify security lists.

The second line lets the NetworkUsers group view the security rules in NSGs, and also view what VNICs and parent resources are in NSGs. The second line does not let the NetworkUsers group change the security rules in NSGs.

```
Allow group NetworkUsers to inspect security-lists in tenancy
Allow group NetworkUsers to use network-security-groups in tenancy
```

**Prevent Users from Creating External Connection to the Internet**

In some cases, you might need to prevent users from creating external internet connectivity to their VCN. In the following example policy, the NetworkUsers group is prevented from creating an internet gateway.

```
Allow group NetworkUsers to manage internet-gateways in tenancy
where request.permission!='INTERNET_GATEWAY_CREATE'
```

**Prevent Users from Updating DNS Records and Zones**

In the following example policy, the NetworkUsers group is prevented from deleting and updating DNS zones and records.

```
Allow group NetworkUsers to manage dns-records in tenancy
where all {request.permission!='DNS_RECORD_DELETE',
            request.permission!='DNS_RECORD_UPDATE'}
Allow group NetworkUsers to manage dns-zones in tenancy
where all {request.permission!='DNS_ZONE_DELETE',
            request.permission!='DNS_ZONE_UPDATE'}
```

**Useful CLI Commands**

In all the following examples, the environment variables $T, $C and $VCN are set to tenancy OCID, compartment OCID, and VCN OCID, respectively.

**List Open Security Lists in a VCN**

```
# list open (0.0.0.0/0) security lists in VCN $VCN in compartment $C
oci network security-list list -c $C --vcn-id $VCN | grep "source" | grep "\"0.0.0.0/0\""
```
List Gateways in a VCN

```
# list all internet gateways in VCN $VCN in compartment $C
oci network internet-gateway list -c $C --vcn-id $VCN
# list all DRGs in compartment $C
oci network drg list -c $C
# list all local peering gateways in vcn $VCN in compartment $C
oci network local-peering-gateway list -c $C --vcn-id $VCN
```

List Route Table Rules in a VCN

```
# list route table rules in VCN $VCN in compartment $C
oci network route-table list -c $C --vcn-id $VCN
```

Securing Object Storage

Security Recommendations

Assign least privileged access for IAM users and groups to resource types in object-family (buckets and objects). For example, the inspect verb gives the least privilege. Inspect lets you check to see if a bucket exists (HeadBucket) and list the buckets in a compartment (ListBucket). The manage verb gives all permissions on the resource. You can create IAM security policies to give appropriate bucket and object access to various IAM groups. For more information about IAM verbs and permissions for Object Storage buckets and objects, see Details for Object Storage, Archive Storage, and Data Transfer on page 2324. For users without IAM credentials, we recommend that you use pre-authenticated requests (PARs) to give time-bound access to objects or buckets.

Public Buckets Security Controls

- A public bucket allows unauthenticated and anonymous reads to all objects in the bucket. Carefully evaluate the intended use case for public buckets before you enable public buckets. We recommend that you use pre-authenticated requests (PARs) to give bucket or object access (read or write) to users without IAM credentials. By default, buckets are created with no public access (access type is set to NoPublicAccess).
- You can make existing buckets public by updating the bucket access type to ObjectRead or ObjectReadWithoutList. To minimize the possibility of existing buckets being made public inadvertently or maliciously, BUCKET_UPDATE permission should be restricted to a minimal set of IAM groups.

Pre-Authenticated Request (PAR)

- Pre-authenticated requests (PARs) provide a mechanism to provide access to objects stored in buckets, to users who do not have IAM user credentials. In a PAR, an IAM user who has appropriate privileges for accessing objects, can create URLs which grant time-bound read or write access to these objects. For more information about creating PARs, see Using Pre-Authenticated Requests on page 3482.
- The creator of a PAR must have PAR_MANAGE IAM permission. You can create the following PARs:
  - Bucket PAR to allow writes to a bucket
  - Object PAR for reading an object
  - Object PAR for writing an object
  - Object PAR to read or write an object
- A PAR cannot be used to list objects in a bucket.
- PAR accesses to a bucket are logged in Audit logs. PAR accesses to an object are logged in Service logs.
- We recommend that you note down the PAR URL created. By design, it is not possible to retrieve a forgotten PAR URL. If you forget a PAR URL, you must create a new PAR.
**Data Durability**

- Minimize data loss because of inadvertent deletes by an authorized user or malicious deletes. We recommend the following:
  - Use object versioning to automatically create an object version each time a new object is uploaded, an existing object is overwritten, or when an object is deleted.
  - Give BUCKET_DELETE and OBJECT_DELETE permissions to a minimum set of IAM users and groups. Grant delete permissions only to tenancy and compartment administrators.
  - Write once read many (WORM) compliance requires that objects cannot be deleted or modified. Use retention rules to achieve WORM compliance. Retention rules are configured at the bucket level and are applied to all individual objects in the bucket. You cannot update, overwrite, or delete objects or object metadata until the retention rule is deleted (indefinite rule) or for the duration specified (time-bound rules).

**Data Encryption**

- All data in Object Storage is encrypted at rest by using AES-256. Encryption is on by default and cannot be turned off. Each object is encrypted with its encryption key, and the object encryption keys are encrypted with a master encryption key. In addition, customers can use client-side encryption to encrypt objects with their encryption keys before storing them in Object Storage buckets. An available option for customers is to use the Amazon S3 Compatibility API, along with client-side object encryption support available in AWS SDK for Java. See Amazon S3 Compatibility API on page 3493 for more details about on this SDK.
  - Data in transit between customer clients (for example, SDKs and CLIs) and Object Storage public endpoints is encrypted with TLS 1.2 by default. FastConnect public peering allows on-premises access to Object Storage to go over a private network, rather than the public internet.

**Data Integrity**

- To verify object data integrity, an MD5 checksum is provided for all objects uploaded to Object Storage. We recommend that you verify that the offline MD5 checksum of an object matches the checksum value returned by the Console or API after upload. Oracle Cloud Infrastructure provides the object checksum value in base64 encoding. To covert the base64 encoded checksum value to hexadecimal, use the following command:

  ```
  python -c 'print "BASE64-ENCODED-MD5-VALUE".decode("base64").encode("hex")'
  ```

  Linux provides an md5sum command line utility to compute MD5 checksum value of an object in hexadecimal format.
  - Object Storage service supports multipart uploads for more efficient and resilient uploads, especially for large objects. In a multipart upload, a large object is broken up into smaller parts by specifying a part size in MiB. Each part is uploaded separately. Object Storage then combines all the parts to create the original object. If any of the parts fail to upload, only those parts need to be retried for upload, and not the entire object. In a multipart upload, the MD5 checksum values are computed for each part, and an MD5 checksum computed over all the individual checksum values to get the output MD5 value. To verify the MD5 value returned for a multipart upload, follow the same process for offline MD5 checksum calculation. A sample script for the offline calculation of an MD5 checksum value for a multipart upload to Object Storage is available here: https://gist.github.com/itemir/f5bc9f9fed6483cd79c89ebf4ca1cfd30.

**Security Policy Examples**

In the following examples, the policies are scoped to a tenancy. However, specifying a compartment name reduces the scope to a specific compartment in a tenancy.

**Restrict Group Access to Specific Buckets**

You can restrict access by a group to a specific bucket by using the specific bucket name (target.bucket.name), regular expression matching (/^name/, /name*/, /name*/), or defined tags (target.tag.definition.name).
The following is an example of restricting access by groups `BucketUsers` to a specific bucket.

```
Allow group BucketUsers to use buckets in tenancy
where target.bucket.name='BucketFoo'
```

You can modify this policy to restrict access by group `BucketUsers` to all buckets whose names are prefixed with `ProjectA_`.

```
Allow group BucketUsers to use buckets in tenancy
where target.bucket.name=/ProjectA_*/
```

You can also match for post-fix (`/*_ProjectA/`) or substring (`/*ProjectA*/`).

**Restrict Group Access to Read or Write to Objects in a Specific Bucket**

The following example allows listing and reading objects by group `BucketUsers` from a specific bucket named `BucketFoo`.

```
Allow group BucketUsers to read buckets in tenancy
Allow group BucketUsers to manage objects in tenancy
where all {target.bucket.name='BucketFoo',
          any {request.permission='OBJECT_INSPECT',
               request.permission='OBJECT_READ'}}
```

The following policy modifies the previous policy to allow listing and writing objects to `BucketFoo`.

```
Allow group BucketUsers to read buckets in tenancy
Allow group BucketUsers to manage objects in tenancy
where all {target.bucket.name='BucketFoo',
          any {request.permission='OBJECT_INSPECT',
               request.permission='OBJECT_CREATE'}}
```

You can restrict this policy to read or write access to a set of buckets by using regular expressions or tags rather than a specific bucket.

**Restrict Resource Access to a Particular User**

You can restrict access to Object Storage resources to a specific user by adding a condition to the policy that specifies the user's OCID in a variable.

The following policy restricts access to the resources in `ObjectStorage` compartment to the user OCID specified:

```
Allow any-user to read object-family in compartment ObjectStorage where
request.user.id = 'ocid1.user.oc1..<user_OCID>'
```

**Restrict Access to Requests That Originate From an Allowed IP Address**

You can restrict access only to requests that originate from an allowed IP address. First, you create a `network source` to specify the allowed IP addresses, then you add a condition to your policy to restrict access to the IP addresses in the network source.

The following policy restricts access to only IP addresses in a network source `corpnet` that defines the allowed IP addresses:

```
Allow group CorporateUsers to manage object-family in tenancy where
request.networkSource.name='corpnet'
```

For information on creating network sources and using them in a policy, see Managing Network Sources on page 2427.
**Prevent Delete of Buckets or Objects**

In the following example, the group *BucketUsers* can perform all actions on buckets and objects except delete.

```
Allow group BucketUsers to manage objects in tenancy
  where request.permission!='OBJECT_Delete'
Allow group BucketUsers to manage buckets in tenancy
  where request.permission!='BUCKET_Delete'
```

The following example further restricts object deletion from the specific bucket (*BucketFoo*).

```
Allow group BucketUsers to manage objects in tenancy
  where any {target.bucket.name!='BucketFoo',
              all {target.bucket.name='BucketFoo',
                   request.permission!='OBJECT_Delete'}}
```

**Enable WORM Compliance for Objects**

Use retention rules to achieve WORM compliance. Retention rules are configured at the bucket level and are applied to all individual objects in the bucket. You cannot update, overwrite, or delete objects or object metadata until the retention rule is deleted (indefinite rule) or for the duration specified (time-bound rules).

The following policies let *BucketUsers* manage the buckets and objects in the tenancy and allow *BucketUsers* to create, manage, and delete retention rules. These policies also let *BucketUsers* lock retentions rules for a specified time.

```
Allow group BucketUsers to manage buckets in tenancy
Allow group BucketUsers to manage objects in tenancy
```

The following more restrictive policies let *BucketUsers* perform all actions on buckets and objects except locking retention rules.

```
Allow group BucketUsers to manage buckets in tenancy
  where request.permission!='RETENTION_RULE_LOCK'
Allow group BucketUsers to manage objects in tenancy
```

**Prevent Public Buckets Configuration**

*BUCKET_CREATE* and *BUCKET_UPDATE* permissions are required to create buckets or make existing private buckets public. Removing these permissions prevents users from creating buckets or making existing buckets public.

```
Allow group BucketUsers to manage buckets in tenancy
  where any {request.permission='BUCKET_INSPECT',
              request.permission='BUCKET_READ',
              request.permission='PAR_MANAGE'}
```

**Useful CLI Commands**

Here are some useful commands to determine if you have public buckets or PARS in your tenancy.

**List of Public Buckets**

The following command returns the public-access-type assigned to a bucket.

```
# "public-access-type" of 'NoPublicAccess' indicates a private bucket, and
# anything else ('ObjectRead') indicates a public bucket
oci os bucket get -ns <your_namespace> --bucket-name <bucket_name> | grep
"public-access-type"
```
List of Bucket Pre-Authenticated Requests (PARs)

The following command returns a list of object PARs in a bucket.

```bash
# list all PARs for objects in bucket $BUCKET_NAME
oci os preauth-request list -ns <your_namespace> -bn <bucket_name>
```

Securing Resource Manager

Resource Manager allows you to automate installing and provisioning Oracle Cloud Infrastructure resources by committing the provisioning instructions to configuration files. These configuration files capture the step-by-step provisioning instructions using a declarative language that follows the "infrastructure-as-code" model. The provisioning instructions are executed as "jobs"; the Oracle Cloud Infrastructure resources that are provisioned when you run the jobs are organized into "stacks."

Executing jobs and provisioning stacks is gated using role-based access control (RBAC), which is enabled by Oracle Cloud Infrastructure Identity and Access Management (IAM). This gives administrators granular control over user access to Oracle Cloud Infrastructure resources and the actions that users can take on these resources.

The Resource Manager security scheme rests on three pillars:

- **Security groups.** Administrator-defined groups that have permission to perform specific operations on stacks and jobs. Individual users are assigned to security groups and can then perform operations that are allowed by that group. For more information about security policies, see [Getting Started with Policies](#) on page 2135. See also [How Policies Work](#) on page 2136 and [Policy Syntax](#) on page 2164. For recommended Resource Manager policies, see [Policies for Managing Resources Used with Resource Manager](#) on page 2476.

- **Permission sets.** Sets of permissions that are specific to jobs and stacks.

- **Operations.** The operations (or actions) that are allowed and the permissions that are required to perform each one.

For permission sets and operations used with Resource Manager, see [Details for Resource Manager](#) on page 2336.

Potential Security Risks and Mitigations

**Terraform State Files**

Terraform state (.tfstate) can contain sensitive data, including resource IDs and in some cases sensitive user data like passwords. HashiCorp provides recommendations for handling Terraform state in the article [Sensitive Data in State](#).

To control access to the Terraform state file, you can create a security policy that limits access to reading jobs, such as the following:

```
Allow group <group_name> to read orm-jobs in compartment
```

**Note:**

Because the permission `read orm-jobs` also affects other operations such as getting logs and Terraform configurations, you should segregate state files in a compartment on which a restrictive policy will not limit the ability to perform other operations.

**Terraform Configurations**

The Resource Manager workflow typically includes writing or generating a Terraform configuration that is then used to manage your stack. Because the Terraform configuration can be accessed using the Resource Manager API `GetJobTfConfig`, we recommend that you do not include sensitive information in your configuration files.

Addressing Basic Configuration Issues

This topic lists procedures to address common configuration issues that affect the security of your cloud resources.
Block Volume
Block volume detached from instance

**Issue:** Ensure that only Oracle Cloud Infrastructure administrators can detach block volumes from instances.

**Basics:** When you detach a block volume it decouples the volume from its associated instance, affecting the data available to the instance. This could impact data availability from business-critical data to the successful completion of scheduled volume backups. To minimize loss of data due to inadvertent volume detachments by an authorized user or malicious volume detachments you should restrict the `VOLUME_ATTACHMENT_DELETE` permission to administrators.

**To prevent detachment of block volumes:**
The following policy allows the group `VolumeUsers` to manage volumes and volume attachments except for detaching volumes:

```
Allow group VolumeUsers to manage volumes in tenancy
Allow group VolumeUsers to manage volume-attachments in tenancy
where request.permission!='VOLUME_ATTACHMENT_DELETE'
```

This change prevents `VolumeUsers` from detaching volumes from instances.

**More information:**
- [Securing Block Volume](#) on page 3675
- [Getting Started with Policies](#) on page 2135
- [How Policies Work](#) on page 2136
- [For volume-family Resource Types](#) on page 2219

Compute
Instance created based on unapproved custom image

**Issue:** An instance was created from a custom image that is unsupported in your environment.

**Basics:** When users create instances they can select from Oracle-provided images, boot volumes from terminated instances, or custom images. Custom images represent a wide variety of images which can include images that aren't approved for your environment. If you use tags in your Oracle Cloud Infrastructure tenancy to identify approved images, verify whether the image the instance is based on is an approved image and terminate the instance if necessary.

**To verify the tags for the image the instance was created from:**
The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance you're interested in.
3. Click the **Image** link to view the source image.
4. Click the **Tags** tab to view the tags applied to this image.

If the custom image does not have an approved tag, and the instance needs to be terminated, see [Terminating an Instance](#) on page 783.

**More information:**
- [Securing Compute](#) on page 3677
- [Resource Tags](#) on page 211
- [Creating an Instance](#) on page 695
- [Image Import/Export](#) on page 670
- [Bring Your Own Image (BYOI)](#) on page 675
I AM

Member of the Administrators group used API keys

Issue: A user who is a member of the Administrators group accessed resources using an API key.

Basics:

• API keys are credentials used to grant programmatic access to Oracle Cloud Infrastructure.
• For security and governance reasons, users should only have access to resources they need to interact with.
• For individuals who are members of the Administrators group who also need access to resources through the API, create another user in IAM to which you attach the API keys. Grant the user with the API keys permissions to only the resources they need to interact with programatically.

To create a user, group, and policy with limited permissions:

The following set of procedures shows you how to set up an example user with limited permissions. In this example, the user needs to be able to launch instances in a specific compartment.

The following procedure is for the Oracle Cloud Infrastructure Console.

Create a User

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Users.
2. Click Create User.
3. In the New User dialog:
   • Name: Enter a unique name or email address for the new user. The value will be the user's login to the Console and must be unique across all other users in your tenancy.
   • Description: Enter a description (required).
4. Click Create User.

Create a Group

Next, create the group ("InstanceLaunchers") that you will create the policy for.

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Groups.
2. Click Create Group.
3. In the Create Group dialog:
   • Name: Enter a unique name for your group, for example, "InstanceLaunchers".
     Note that the name cannot contain spaces.
   • Description: Enter a description (required).
4. Click Create Group.

Create a Policy

In this example, the policy grants members of the group InstanceLaunchers permissions to launch instances in a specific compartment (CompartmentA).

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Policies.
2. Click Create Policy.
3. Enter a unique Name for your policy, for example, "InstanceLaunchersPolicy".
   Note that the name cannot contain spaces.
4. Enter a Description (required), for example, "Grants users permission to launch instances in CompartmentA".
5. Enter the following Statement:

   Allow group InstanceLaunchers to manage instance-family in compartment CompartmentA

This statement grants members of the InstanceLaunchers group permissions to launch and manage instances in the compartment called CompartmentA.
6. Click **Create Policy**.

**Add the User to the Group**

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**.
2. In the **Users** list, find the user and click the name.
3. On the user detail page, click **Groups** (on the left side of the page). The list of groups that the user belongs to is displayed.
4. Click **Add User to Group**.
5. From the **Groups** list, select **InstanceLaunchers**.
6. Click **Add**.

**Upload an API signing key for the user**

The following procedure works for a regular user or an administrator. Administrators can upload an API key for either another user or themselves.

---

**Important:**

The API key must be an **RSA key in PEM format (minimum 2048 bits)**. The PEM format looks something like this:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoTFqF...
...
-----END PUBLIC KEY-----
```

For more information about generating a public PEM key, see **Required Keys and OCIDs** on page 4179.

---

1. View the user's details:
   - If you're uploading an API key for your **self**:
     
     Open the **Profile** menu (🔍) and click **User Settings**.
   - If you're an administrator uploading an API key for another **user**: In the Console, click **Identity**, and then click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. Click **Add Public Key**.
3. Paste the key's value into the window and click **Add**.


**More information:**

- **Securing IAM** on page 3688
- **How Policies Work** on page 2136 and **Common Policies** on page 2142
- **Managing User Credentials** on page 2456
- **Managing Groups** on page 2419
- **Managing Users** on page 2414

**Policy grants broad permissions**

**Issue:** A policy grants full management permissions for at least one service in a compartment or in the tenancy.

**Basics:**

- Access to resources is controlled through policies. A **policy** is a document that specifies who can access which Oracle Cloud Infrastructure resources that your company has, and how. A policy simply allows a **group** to work in certain ways with specific types of **resources** in a particular **compartment**.
- For security and governance reasons, users should only have access to resources they need.
Consider carefully the access level a user needs. Policy language provides a default set of verbs (manage, use, read, inspect) that allow you to easily scope users' permissions to a set of common tasks. For example, if a user needs to be able to update resources, but does not need to create or delete them, grant them the use permission, rather than the manage permission.

The policy language is designed to let you write simple statements involving only verbs and resource-types, without having to state the permissions in the statement. For more fine-grained access control, you can use conditions combined with permissions or API operations to reduce the scope of access granted by a particular verb.

Wherever possible, scope access to the specific compartments a user needs access to, rather than scoping it to the full tenancy.

**Tips for writing least-privilege policies:**

**Scope the policy to a compartment instead of the tenancy**

Each policy consists of one or more policy statements that follow a basic syntax. Where possible, scope policies to compartments, rather than to the tenancy. For example, update a policy like this:

```
Allow group <group_name> to <verb><resource-type> in tenancy
```

to include just the compartments needed:

```
Allow group <group_name> to <verb><resource-type> in compartment <compartment_name>
```

If the user needs access to multiple compartments, create a policy statement for each compartment. It is then easy to remove access to individual compartments, if necessary.

**Scope permissions to those required to perform a job function**

Oracle defines the possible verbs you can use in your policies. Here's a summary of the verbs, from least amount of access to the most:

<table>
<thead>
<tr>
<th>Verb</th>
<th>Types of Access Covered</th>
<th>Target User</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspect</td>
<td>Ability to list resources, without access to any confidential information or user-specified metadata that may be part of that resource.</td>
<td>Third-party auditors</td>
</tr>
<tr>
<td>read</td>
<td>Includes inspect plus the ability to get user-specified metadata and the actual resource itself.</td>
<td>Internal auditors</td>
</tr>
<tr>
<td>use</td>
<td>Includes read plus the ability to work with existing resources (the actions vary by resource type). In general, this verb does not include the ability to create or delete that type of resource.</td>
<td>Day-to-day end users of resources</td>
</tr>
<tr>
<td>manage</td>
<td>Includes all permissions for the resource.</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

Users who don't need to create or delete resources generally don't need manage permissions. If you have a policy like

```
Allow group <group_name> to manage <resource-type> in compartment <compartment_name>
```

but the user will never create or delete the resource-type, consider rewriting the policy to

```
Allow group <group_name> to use <resource-type> in compartment <compartment_name>
```

The Policy Reference on page 2167 includes details of the specific resource-types for each service, and which verb + resource-type combination gives access to which API operations.
**Service-specific links**

- Details for the Audit Service on page 2177
- Details for Container Engine for Kubernetes on page 2177
- Details for the Core Services on page 2181 (this includes Networking, Compute, and Block Volume)
- Details for the Database Service on page 2240
- Details for the DNS Service on page 2262
- Details for the Email Service on page 2270
- Details for the File Storage Service
- Details for IAM on page 2280
- Details for Load Balancing on page 2292
- Details for Object Storage, Archive Storage, and Data Transfer on page 2324
- Details for Registry on page 2335
- Details for the Search Service

**For fine-grained access control, scope access using conditions and API operations**

In a policy statement, you can use conditions combined with permissions or API operations to reduce the scope of access granted by a particular verb.

For example, let's say you want group XYZ to be able to list, get, create, or update groups (change their description), but not delete them. To list, get, create, and update groups, you need a policy with manage groups as the verb and resource-type. According to the table in Details for Verbs + Resource-Type Combinations on page 2281, the permissions covered are:

- GROUP_INSPECT
- GROUP_UPDATE
- GROUP_CREATE
- GROUP_DELETE

To restrict access to only the desired permissions, you could add a condition that explicitly states the permissions you want to allow:

```
Allow group XYZ to manage groups in tenancy

where any 
{ request.permission='GROUP_INSPECT',
  request.permission='GROUP_CREATE',
  request.permission='GROUP_UPDATE'
}
```

An alternative would be a policy that allows all permissions except GROUP_DELETE:

```
Allow group XYZ to manage groups in tenancy where request.permission != 'GROUP_DELETE'
```

Another alternative would be to write a condition based on the specific API operations. Notice that according to the table in Permissions Required for Each API Operation on page 2288, both ListGroups and GetGroup require only the GROUP_INSPECT permission. Here's the policy:

```
Allow group XYZ to manage groups in tenancy

where any 
{ request.operation='ListGroups',
  request.operation='GetGroup',
  request.operation='CreateGroup',
  request.operation='UpdateGroup'
}
```

It can be beneficial to use permissions instead of API operations in conditions. In the future, if a new API operation is added that requires one of the permissions listed in the permissions-based policy above, that policy will already control XYZ group's access to that new API operation.
But notice that you can further scope a user's access to a permission by also specifying a condition based on API operation. For example, you could give a user access to GROUP_INSPECT, but then only to ListGroups.

Allow group XYZ to manage groups in tenancy

where all {request.permission='GROUP_INSPECT', request.operation='ListGroups'}

More information:
- Securing IAM on page 3688
- How Policies Work on page 2136 and Common Policies on page 2142
- Advanced Policy Features on page 2160
- Managing Policies on page 2450

API signing keys over 90 days old

**Issue:** A user's API signing keys are older than 90 days. Oracle recommends that you rotate API keys at least every 90 days.

**Basics:**
- API keys are credentials used to grant programmatic access to Oracle Cloud Infrastructure.
- It is a security engineering best practice and compliance requirement to rotate API keys regularly, every 90 days or less.
- Ensure that you test the new keys before you deactivate the old keys.

**To generate and upload new API keys:**

The following procedure is for the Oracle Cloud Infrastructure Console.

**Generate new API keys**

You can use the following OpenSSL commands to generate the key pair in the required PEM format. If you're using Windows, you'll need to install Git Bash for Windows and run the commands with that tool.

1. If you haven't already, create a .oci directory to store the credentials:

   ```bash
   mkdir ~/.oci
   ```

2. Generate the private key with one of the following commands.

   - Recommended: To generate the key, encrypted with a passphrase you provide when prompted:
     ```bash
     openssl genrsa -out ~/.oci/oci_api_key.pem -aes128 2048
     ```
     
     **Note:** For Windows, you may need to insert `-passout stdin` to be prompted for a passphrase. The prompt will just be the blinking cursor, with no text.
     ```bash
     openssl genrsa -out ~/.oci/oci_api_key.pem -aes128 -passout stdin 2048
     ```

   - To generate the key with no passphrase:
     ```bash
     openssl genrsa -out ~/.oci/oci_api_key.pem 2048
     ```

3. Ensure that only you can read the private key file:

   ```bash
   chmod go-rwx ~/.oci/oci_api_key.pem
   ```
4. Generate the public key:

```bash
openssl rsa -pubout -in ~/.oci/oci_api_key.pem -out ~/.oci/oci_api_key_public.pem
```

**Note:** For Windows, if you generated the private key with a passphrase, you may need to insert `-passin stdin` to be prompted for the passphrase. The prompt will just be the blinking cursor, with no text.

```bash
openssl rsa -pubout -in ~/.oci/oci_api_key.pem -out ~/.oci/oci_api_key_public.pem -passin stdin
```

5. Copy the contents of the public key to the clipboard using pbcopy, xclip or a similar tool (you'll need to paste the value into the Console later). For example:

```bash
cat ~/.oci/oci_api_key_public.pem | pbcopy
```

Your API requests will be signed with your private key, and Oracle will use the public key to verify the authenticity of the request. You must upload the public key to IAM (instructions below).

**Get the key's fingerprint**

You can get the key's fingerprint with the following OpenSSL command.

**For Linux and Mac OS X:**

```bash
openssl rsa -pubout -outform DER -in ~/.oci/oci_api_key.pem | openssl md5 -c
```

**For Windows:**

**Note:**

If you're using Windows, you'll need to install Git Bash for Windows and run the command with that tool.

```bash
openssl rsa -pubout -outform DER -in \.\/oci\api_key.pem | openssl md5 -c
```

When you upload the public key in the Console, the fingerprint is also automatically displayed there. It looks something like this: `12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef`

**Upload the API signing key for the user**

You can upload the PEM public key in the Console, located at [https://cloud.oracle.com](https://cloud.oracle.com). If you don't have a login and password for the Console, contact an administrator.

1. Open the Console, and sign in.
2. View the details for the user who will be calling the API with the key pair:
   - If you're signed in as this user, click your username in the top-right corner of the Console, and then click **User Settings**.
   - If you're an administrator doing this for another user: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.
3. Click **Add Public Key**.
4. Paste the contents of the PEM public key in the dialog box and click **Add**.

The key's fingerprint is displayed (for example, `12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef`). Notice that after you've uploaded your first public key, you can also use the **UploadApiKey** API operation to upload additional keys.
You can have up to three API key pairs per user. In an API request, you specify the key's fingerprint to indicate which key you're using to sign the request.

**Test the new key**

Test the key in a sample API call against Oracle Cloud Infrastructure.

**Delete the old key**

The following procedure works for a regular user or an administrator. Administrators can delete an API key for either another user or themselves.

1. View the user's details:
   - If you're deleting an API key for *yourself*:
     
     Open the **Profile** menu (🔗) and click **User Settings**.  
   - If you're an administrator deleting an API key for *another user*:
     
     Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. For the API key you want to delete, click **Delete**.

3. Confirm when prompted.

The API key is no longer valid for sending API requests.

**More information:**

- Securing IAM on page 3688
- API Signing Key on page 179

**Tenancy administrator privilege grant to an IAM group**

**Issue:** A group other than the Administrators group has been granted administrator privileges.

**Basics:**

- Granting the tenancy administrator privilege *(manage all-resources in tenancy)* to a group enables the members to have full access to all resources in the tenancy.
- This high-privilege entitlement must be controlled and restricted to only the users who need it to perform their job function.
- Verify with the Oracle Cloud Infrastructure administrator that this entitlement grant was sanctioned and that the membership of the group remains valid after the grant of the administrator privilege.
- Rather than create an alternative group with administrator privileges, consider instead adding users needing administrator privileges to the default Administrators group.

**To resolve this issue:**

Add users who need administrator privileges to the Administrators group:

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Groups**.
2. In the **Groups** list, click **Administrators**.
3. Click **Add User to Group**.
4. In the **Add User to Group** dialog, select the user from the **User** list.
5. Click **Add User**.

Remove the policy or policy statement that grants the (non-Administrators) group administration privileges.

1. Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Policies**. A list of the policies in the compartment you're viewing is displayed.
   
   If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).
2. Click the policy you want to update.
   
   The policy's details and statements are displayed.
3. Find the statement that grants administrator privileges to the group. This policy will look like:

```plaintext
Allow group <group_name> to manage all-resources in tenancy
```

Click the the Actions icon (three dots) and then click **Delete**.

4. If the policy has no other statements, you can delete the policy by clicking **Delete** next to the policy name.

**More information:**
- [Securing IAM](#) on page 3688
- [Managing Policies](#) on page 2450

**Networking: VCN, Load Balancers, and DNS**

**No ingress rules in security lists**

**Issue:** A VCN's security lists have no ingress rules. This means that the instances in the VCN can't receive incoming traffic.

**Basics:**
- Security lists provide stateful and stateless firewall capability to control network access to your instances.
- A security list is configured at the subnet level and enforced at the instance level.
- You can associate multiple security lists with a subnet. A packet is allowed if it matches any rule in any of the security lists used by the subnet.
- If there are no ingress (inbound) rules in any of the subnet's security lists, no traffic is allowed to the instances in that subnet.
- For defense in depth, ingress security list rules should state a specific known source and not an open source (0.0.0.0/0).
- You can configure an exception in Oracle CASB Cloud Service to reduce alerts from exempted security lists.

**To add an ingress rule to an existing security list:**

The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Confirm you're viewing the compartment that contains the cloud network you're interested in.
3. Click the cloud network you're interested in.
4. Click **Security Lists**.
5. Click the security list you're interested in.
6. Click **Edit All Rules**.
7. Add at least one ingress rule:
   a. In the **Allow Rules for Ingress** section, click **+ Rule**.
   b. Choose whether it's a stateful or stateless rule (see [Stateful Versus Stateless Rules](#) on page 2839). By default, rules are stateful unless you specify otherwise.
   c. Enter the source CIDR. Typical CIDRs you might specify in a rule are the CIDR block for your on-premises network or a particular subnet. If you're setting up a security list rule to allow traffic with a service gateway, instead see [Task 3: (Optional) Update security rules](#) on page 3261.
   d. Select the protocol (for example, TCP, UDP, ICMP, "All protocols", and so on).
   e. Enter further details depending on the protocol:
      - If you chose TCP or UDP, enter a source port range and destination port range. You can enter "All" to cover all ports. If you want to allow a specific port, enter the port number (for example, 22 for SSH or 3389 for RDP) or a port range (for example, 20-22).
      - If you chose ICMP, you can enter "All" to cover all types and codes. If you want to allow a specific ICMP type, enter the type and an optional code separated by a comma (for example, 3,4). If the type has multiple codes you want to allow, create a separate rule for each code.
8. When you're done, click **Save Security List Rules**.
This change enables ingress access from the source CIDR block listed in the rule. Add additional rules if you want to allow ingress from other known sources.

More information:
- Securing Networking: VCN, Load Balancers, and DNS on page 3696
- Security Lists on page 2850
- UpdateSecurityList

Security list allows traffic from any IP address (open source)

Issue: A security list has at least one rule with an open source (0.0.0.0/0). This means that traffic could come from any source and is not controlled.

Basics:
- Security lists provide stateful and stateless firewall capability to control network access to your instances.
- A security list is configured at the subnet level and enforced at the instance level.
- You can associate multiple security lists with a subnet. A packet is allowed if it matches any rule in any of the security lists used by the subnet.
- If there are no ingress (inbound) rules in any of the subnet's security lists, no traffic is allowed to the instances in that subnet.
- For defense in depth, ingress security list rules should state a specific known source and not an open source (0.0.0.0/0).
- You can configure an exception in Oracle CASB Cloud Service to reduce alerts from exempted security lists.

To change the source of a security list rule:

The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Confirm you're viewing the compartment that contains the cloud network you're interested in.
3. Click the cloud network you're interested in.
5. Click the security list you're interested in.
6. Click Edit All Rules.
7. Locate the rule that lists 0.0.0.0/0 as the source CIDR.
8. For that rule, change 0.0.0.0/0 to the CIDR block of a known source.

This change restricts ingress so packets are allowed only from a specific CIDR block. Add additional rules if you want to allow ingress from other known sources.

More information:
- Securing Networking: VCN, Load Balancers, and DNS on page 3696
- Security Lists on page 2850
- UpdateSecurityList

Security list allows traffic to sensitive ports

Issue: A security list has at least one rule that enables access to a sensitive port.

Basics:
- Security lists provide stateful and stateless firewall capability to control network access to your instances.
- A security list is configured at the subnet level and enforced at the instance level.
- You can associate multiple security lists with a subnet. A packet is allowed if it matches any rule in any of the security lists used by the subnet.
- If there are no ingress (inbound) rules in any of the subnet's security lists, no traffic is allowed to the instances in that subnet.
• For defense in depth, ingress security list rules should state a specific known source and not an open source (0.0.0.0/0).
• You can configure an exception in Oracle CASB Cloud Service to reduce alerts from exempted security lists.

Recommendation: Update the subnet's security list to enable access to instances through SSH (TCP port 22) or RDP (TCP port 3389) on a temporary, as-needed basis, and only from authorized CIDR blocks (not 0.0.0.0/0). To perform instance health checks, update the security list to allow ICMP pings.

**To change an existing security list:**

The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Confirm you're viewing the compartment that contains the cloud network you're interested in.
3. Click the cloud network you're interested in.
4. Click **Security Lists**.
5. Click the security list you're interested in.
6. Click **Edit All Rules**.
7. Make one or more of these changes:
   • Delete an existing rule by clicking the X next to the rule.
   • Change an existing rule in the list. For example: change the source from 0.0.0.0/0 to the CIDR block of a known source.
   • Add a new rule by clicking + Rule and entering values for the new rule.
8. Click **Save Security List Rules**.

**More information:**

- [Securing Networking: VCN, Load Balancers, and DNS](#) on page 3696
- [To enable RDP access](#)
- Security Lists on page 2850
- UpdateSecurityList

**Internet gateway attached to VCN**

**Issue:** A VCN has an internet gateway. The gateway must be authorized to be attached to the VCN and must not unintentionally expose resources to the internet.

**Basics:**

• Gateways provide external connectivity to hosts in a VCN. For example: an internet gateway enables direct internet connectivity for instances that are in a public subnet and have a public IP address. A dynamic routing gateway (DRG) enables connectivity with the on-premises network over an IPSec VPN or FastConnect.
• To enable traffic through the internet gateway from a particular subnet in the VCN, there must be a rule in the subnet's route table that lists the internet gateway as a route target. To delete the internet gateway from the VCN, you must first delete any route rules that specify the internet gateway as the target.
• You can configure an exception in Oracle CASB Cloud Service to reduce alerts from exempted VCNs.

**To remove an internet gateway from a VCN:**

Prerequisite: Ensure that there are no route rules that specify the internet gateway as a target.

The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Confirm you're viewing the compartment that contains the cloud network you're interested in.
3. Click the cloud network you're interested in.
4. Click **Internet Gateways**.
5. Click the Actions icon (three dots) for the internet gateway, and then click **Terminate**.
6. Confirm when prompted.

This change disables direct internet connectivity for the VCN.
Instance has a public IP

**Issue:** An instance has a public IP address. This means the instance could be publicly addressable if other required components are present and configured correctly in the VCN.

**Basics:**

- Carefully consider allowing internet access to any instances. For example, don't accidentally allow internet access to sensitive DB systems.
- For an instance to be publicly addressable:
  - The instance must have a public IP address and reside in a public subnet in the VCN (instances in private subnets cannot have public IP addresses).
  - The subnet's security list must be configured to allow traffic for all IPs (0.0.0.0/0) and all ports.
  - The VCN must have an internet gateway and be configured to route outbound traffic from the subnet to the internet gateway.
  - An instance can have more than one public IP address. A given public IP is assigned to a private IP on a particular VNIC on the instance. An instance can have more than one VNIC, and each VNIC can have more than one private IP.

**To remove a public IP address from an instance:**

The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Confirm you're viewing the compartment that contains the instance you're interested in.
3. Click the instance to view its details.
4. Click **Attached VNICS**.
   - The primary VNIC and any secondary VNICS attached to the instance are displayed.
5. Click the VNIC you're interested in.
   - The VNIC's primary private IP and any secondary private IPs are displayed.
6. For the private IP you're interested in, click the Actions icon (three dots), and then click **Edit**.
7. In the **Public IP Address** section, for **Public IP Type**, select the radio button for **No Public IP**.
8. Click **Update**.

The public IP is unassigned from the instance.

**More information:**

- Securing Networking: VCN, Load Balancers, and DNS on page 3696
- Internet Gateway on page 3243
- DeleteInternetGateway
- Public IP Addresses on page 2875

Load balancer has no inbound rules or listeners

**Issue:** A load balancer's subnet security lists have no ingress rules, or a load balancer has no listener. In this case, the load balancer can't receive incoming traffic.

**Basics:**

- Load balancers provide automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). Each load balancer exists in a subnet governed by security list rules. A load balancer receives incoming data traffic from one or more listeners.
- Security lists provide stateful and stateless firewall capability to control network access to your load balancer and backend servers.
- If there are no ingress (inbound) rules in any of the subnet's security lists, no traffic is allowed to the instances in that subnet.
- For defense in depth, configure ingress security list rules to state a specific known source and not an open source (0.0.0.0/0).
- A listener is a logical entity that checks for incoming traffic on the load balancer's IP address.
- To handle TCP, HTTP, and HTTPS traffic, you must configure at least one listener per traffic type.
- You can apply path route rules to a listener to route traffic to the correct backend set without using multiple listeners or load balancers. A path route is a string that the listener matches against an incoming URI to determine the appropriate destination backend set.
- Ensure that your Oracle Cloud Infrastructure load balancers use inbound rules or listeners to allow access only from known resources.
- Exceptions can be configured in CASB to reduce alerts from exempted load balancers.

To enable a listener to accept traffic:

The following procedure is for the Oracle Cloud Infrastructure Console.

To enable a listener to accept traffic, you must update your VCN's security list rules:

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   The list of VCNs in the current compartment appears.
2. Click the name of the VCN containing your load balancer, and then click Security Groups or Security Lists.
   A list of the security groups or lists in the cloud network appears.
3. Click the name of the NSG or security list that applies to your load balancer.
4. Add or edit the existing rules to allow access from the appropriate resources.
   An NSG's security rules appear on the Network Security Group Details page. From there you can add, edit, or remove rules.
   The Security List Details page provides access to separate tables in which you can add or edit Ingress Rules or Egress Rules.

   For details on rule configuration, see Security Rules on page 2833.

To create a listener:

Usually, you create a listener as part of the load balancer creation workflow. To create a listener for an existing load balancer:

1. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
2. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click Listeners under the Resources menu, then click Create Listener.
   The Create Listener dialog box appears.
4. Enter the following:

- **Name:** Required. Specify a friendly name for the listener. The name must be unique, and cannot be changed. Avoid entering confidential information.
- **Hostname:** Optional. Select up to 16 virtual hostnames for this listener.

  | Important: |
  |
  | To apply a virtual hostname to a listener, the name must be part of the load balancer's configuration. If the load balancer has no associated hostnames, you can create one on the Hostnames page. |

- **Protocol:** Required. Specify the protocol to use, either HTTP or TCP.
- **Port:** Required. Specify the port on which to listen for incoming traffic.
- **Use SSL:** Optional. Check this box to associate an SSL certificate bundle with the listener. The following settings are required to enable SSL handling. See Managing SSL Certificates on page 2551 for more information.

  - **Certificate Name:** The friendly name of the SSL certificate bundle to use.
  - **Verify Peer Certificate:** Optional. Select this option to enable peer certificate verification.
  - **Verify Depth:** Optional. Specify the maximum depth for certificate chain verification.
- **Backend Set:** Required. Specify the default backend set to which the listener routes traffic.
- **Idle Timeout in Seconds:** Optional. Specify the maximum idle time in seconds. This setting applies to the time allowed between two successive receive or two successive send network input/output operations during the HTTP request-response phase.

  | Tip: |
  |
  | The maximum value is 7200 seconds. For more information, see Connection Management on page 2489. |

- **Path Route Set:** Optional. Specify the name of the set of path-based routing rules that applies to this listener's traffic.

  | Important: |
  |
  | To apply a path route set to a listener, the set must be part of the load balancer's configuration. |
  | To remove a path route set from an existing listener, choose None as the Path Route Set option. The path route set remains available for use by other listeners on this load balancer. |

- **Show Advanced Options:** Click to display the following options:

  - **TLS Version:** Specify the Transport Layer Security (TLS) version(s):
    - 1.0
    - 1.1
    - 1.2 (recommended)

    You can select any combination of versions. Choose the ones you want from the list. If you do not specify the TLS versions, the default TLS is version 1.2 only.

    - **Select Cipher Suite** - Select a set of cipher suites from the list. (default).
      
      All choices present in the list have at least one cipher associated with each TLS version you selected.

    - Click Show Cipher Suite Details to display the individual ciphers the selected cipher suite contains.
    - **Server Order Preference:** Select Enable to give preference to the server ciphers over the client.

5. Click Create.

When you create a listener, you must also update your VCN's security list rules to allow traffic to that listener.

More information:
Load balancer has no backend sets

**Issue:** A load balancer has no backend set. In this case, the load balancer has no place to distribute incoming data and no means to monitor backend server health.

**Basics:**
- A backend set is a logical entity defined by a load balancing policy, a health check policy, and a list of backend servers.
- The backend set determines the load balancer's traffic distribution policy, such as:
  - IP Hash
  - Least Connections
  - Weighted Round Robin
- You specify the test parameters to confirm the health of backend servers when you create a backend set.
- If you have an existing load balancer with no backend set, you can specify the backend servers that receive traffic from the load balancer after you create a backend set.
- You can configure an exception in Oracle CASB Cloud Service to reduce alerts from exempted load balancers.

**To create a backend set:**

The following procedure is for the Oracle Cloud Infrastructure Console.

Usually, you create a backend set as part of the load balancer creation workflow. To create a backend set for an existing load balancer:

1. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.
2. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.
3. Click **Backend Sets** under the **Resources** menu, then click **Create Backend Set**.

   The **Create Backend Set** dialog box appears.
4. Enter the following:

- **Name:** Required. Specify a friendly name for the backend set. It must be unique within the load balancer, and it cannot be changed.
  
  Valid backend set names include only alphanumeric characters, dashes, and underscores. Backend set names cannot contain spaces. Avoid entering confidential information.

- **Traffic Distribution Policy:** Required. Choose the load balancer policy for the backend set. The available options are:
  
  - IP Hash
  - Least Connections
  - Weighted Round Robin

  For more information on these policies, see How Load Balancing Policies Work on page 2488.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot add a backend server marked as Backup to a backend set that uses the IP Hash policy.</td>
</tr>
</tbody>
</table>

- **Use SSL:** Optional. Check this box to associate an SSL certificate bundle with the backend set.
  
  If there are no certificate bundles attached to the load balancer, this option is disabled.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you check Use SSL, the SSL Policies fields appear at the bottom of the page.</td>
</tr>
</tbody>
</table>

  - **Certificate Name:** Required. Select the certificate bundle to use. You can choose any certificate bundle that is attached to the current load balancer. See Managing SSL Certificates on page 2551 for more information.

  - **Verify Peer Certificate:** Optional. Select this option to enable peer certificate verification.

  - **Verify Depth:** Optional. Specify the maximum depth for certificate chain verification.

  - **Session Persistence:** Optional. Specify how the load balancer manages session persistence.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>See Session Persistence on page 2491 for important information on configuring these settings.</td>
</tr>
</tbody>
</table>

  - **Disable Session Persistence:** Choose this option to disable cookie-based session persistence.

  - **Enable Application Cookie Persistence:** Choose this option to enable persistent sessions from a single logical client when the response from a backend application server includes a Set-cookie header with the cookie name you specify.

  - **Cookie Name:** The cookie name used to enable session persistence. Specify * to match any cookie name. Avoid entering confidential information.

  - **Disable Fallback:** Check this box to disable fallback when the original server is unavailable.

  - **Enable Load Balancer Cookie Persistence:** Choose this option to enable persistent sessions based on a cookie inserted by the load balancer.

  - **Cookie Name:** Specify the name of the cookie used to enable session persistence. If blank, the default cookie name is X-Oracle-BMC-LBS-Route.

    Ensure that any cookie names used at the backend application servers are different from the cookie name used at the load balancer. Avoid entering confidential information.

  - **Disable Fallback:** Check this box to disable fallback when the original server is unavailable.

  - **Domain Name:** Optional. Specify the domain in which the cookie is valid.

    This attribute has no default value. If you do not specify a value, the load balancer does not insert the domain attribute into the Set-cookie header.
• **Path:** Optional. Specify the path in which the cookie is valid. The default value is /.

• **Expiration Period in Seconds:** Optional. Specify the amount of time the cookie remains valid. If blank, the cookie expires at the end of the client session.

• **Attributes**
  - **Secure:** Specify whether the Set-cookie header should contain the Secure attribute. If selected, the client sends the cookie only using a secure protocol.
    
    If you enable this setting, you cannot associate the corresponding backend set with an HTTP listener.

  - **HTTP Only:** Specify whether the Set-cookie header should contain the HttpOnly attribute. If selected, the cookie is limited to HTTP requests. The client omits the cookie when providing access to cookies through non-HTTP APIs such as JavaScript channels.

• **Health Check:** Required. Specify the test parameters to confirm the health of backend servers.

  - **Protocol:** Required. Specify the protocol to use, either HTTP or TCP.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure your health check protocol to match your application or service.</td>
</tr>
</tbody>
</table>

  - **Port:** Optional. Specify the backend server port against which to run the health check.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can enter the value '0' to have the health check use the backend server's traffic port.</td>
</tr>
</tbody>
</table>

  - **URL Path (URI):** (HTTP only) Required. Specify a URL endpoint against which to run the health check.

  - **Interval in ms:** Optional. Specify how frequently to run the health check, in milliseconds. The default is 10000 (10 seconds).

  - **Timeout in ms:** Optional. Specify the maximum time in milliseconds to wait for a reply to a health check. A health check is successful only if a reply returns within this timeout period. The default is 3000 (3 seconds).

  - **Number of retries:** Optional. Specify the number of retries to attempt before a backend server is considered "unhealthy". This number also applies when recovering a server to the "healthy" state. The default is '3'.

  - **Status Code:** (HTTP only) Optional. Specify the status code a healthy backend server must return.

  - **Response Body Regex:** (HTTP only) Optional. Provide a regular expression for parsing the response body from the backend server.

• **SSL Policy:** Optional. Specify the type of cipher suite to use:

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must check Use SSL for the SSL Policy features to be displayed.</td>
</tr>
</tbody>
</table>

  - **TLS Version:** Optional. Specify the Transport Layer Security (TLS) version(s):

    - 1.0
    - 1.1
    - 1.2 (recommended)

    You can select any combination of versions. Choose the ones you want from the list. If you do not specify the TLS versions, the default TLS is version 1.2 only.

  - **Select Cipher Suite** - Select a set of cipher suites from the list. (default).

    All choices present in the list have at least one cipher associated with each TLS version you selected.

    - Click Show Cipher Suite Details to display the individual ciphers the selected cipher suite contains.

5. **Click Create.**
After your backend set is provisioned, you must specify backend servers for the set. See Managing Backend Servers on page 2515 for more information.

More information:

- Securing Networking: VCN, Load Balancers, and DNS on page 3696
- Managing Backend Sets on page 2510
- Editing Health Check Policies on page 2558
- Managing Load Balancers on page 2494

Load balancer SSL certificate expires in X days

Issue: A load balancer's SSL certificate expires soon. When the certificate expires, data traffic can be interrupted and security compromised.

Basics:

- To ensure continuous security and usability, SSL certificates must be rotated on a timely basis.
- You can configure an exception in Oracle CASB Cloud Service to reduce alerts from exempted load balancers.

To rotate a load balancer's certificate bundle:

The following procedure is for the Oracle Cloud Infrastructure Console.

To ensure consistent service, you must update (rotate) expiring certificates:

1. Update your client or backend server to work with a new certificate bundle.

Note:
The steps to update your client or backend server are unique to your system.
2. Upload the new SSL certificate bundle to the load balancer

   a. Open the navigation menu. Under the **Core Infrastructure** group, go to **Networking** and click **Load Balancers**.

   b. Click the name of the **Compartment** that contains the load balancer you want to modify, and then click the load balancer's name.

   c. Click the load balancer you want to configure.

   d. In the **Resources** menu, click **Certificates**, and then click **Add Certificate**.

   e. In the **Add Certificate** dialog box, enter the following:

      - **Certificate Name**: Required. Specify a friendly name for the certificate bundle. It must be unique within the load balancer, and it cannot be changed in the Console. (It can be changed using the API.) Avoid entering confidential information.

      - **Choose SSL Certificate File**: Required. Drag and drop the certificate file, in PEM format, into the **SSL Certificate** field. Alternatively, you can choose the **Paste SSL Certificate** option to paste a certificate directly into this field.

      - **Specify CA Certificate**: Optional. (Recommended for backend SSL termination configurations.) Select (check) this box if you want to provide a CA certificate.

         - **Choose CA Certificate File**: Drag and drop the CA certificate file, in PEM format, into the **CA Certificate** field. Alternatively, you can choose the **Paste CA Certificate** option to paste a certificate directly into this field.

      - **Specify Private Key**: Optional. (Required for SSL termination.) Select (check) this box if you want to provide a private key for the certificate.

         - **Choose Private Key File**: Drag and drop the private key, in PEM format, into the **Private Key** field. Alternatively, you can choose the **Paste Private Key** option to paste a private key directly into this field.

      - **Enter Private Key Passphrase**: Optional. Specify the private key passphrase.

   f. Click **Add Certificate**.
3. Edit listeners or backend sets (as needed) so they use the new certificate bundle

   Editing a listener:
   a. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
   b. Choose the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
   c. In the Resources menu, click Listeners.
   d. For the listener you want to edit, click the Actions icon (three dots), and then click Edit Listener.
   e. In the Certificate Name drop-down list, choose the new certificate bundle.
   f. Click Submit.

   Editing a backend set:
   Caution:
   Updating the backend set temporarily interrupts traffic and can drop active connections.

   a. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
   b. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
   c. In the Resources menu, click Backend Sets, and then click the name of the backend set you want to edit.
   d. Click Edit Backend Set.
   e. In the Edit Backend Set dialog box, select (check) Use SSL.
   f. In the Certificate Name drop-down list, choose the new certificate bundle.
   g. Click Save Changes.

4. (Optional) Remove the expiring SSL certificate bundle

   Important:
   You cannot delete an SSL certificate bundle that is associated with a listener or backend set. Remove the bundle from any additional listeners or backend sets before deleting.

   a. Open the navigation menu. Under the Core Infrastructure group, go to Networking and click Load Balancers.
   b. Click the name of the Compartment that contains the load balancer you want to modify, and then click the load balancer's name.
   c. Click the load balancer you want to configure.
   d. In the Resources menu, click Certificates.
   e. For the certificate you want to delete, click the Actions icon (three dots), and then click Delete.
   f. Confirm when prompted.

More information:

- Securing Networking: VCN, Load Balancers, and DNS on page 3696
- Managing SSL Certificates on page 2551
- Managing Listeners on page 2522
- Managing Backend Sets on page 2510
- Managing Load Balancers on page 2494
Object Storage

Public buckets detected

**Issue:** Public buckets were detected in your tenancy. Confirm that the creation of each public bucket is intentional and authorized. If the bucket is not sanctioned for public access, follow the procedure for changing the visibility of a bucket and make the bucket private.

**Basics:**

- Carefully assess the business requirement for public access to a bucket. When you enable anonymous access to a bucket, users can obtain object metadata, download bucket objects, and optionally list bucket contents.
- Changing the type of access is bi-directional. You can change a bucket's access from public to private or from private to public.
- Changing the type of access doesn't affect existing pre-authenticated requests. Existing pre-authenticated requests still work.

**To change the visibility of a bucket (private or public):**

The following procedure is for the Oracle Cloud Infrastructure Console.

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.

   A list of the buckets in the compartment you're viewing is displayed. If you don’t see the one you're looking for, verify that you’re viewing the correct compartment (select from the list on the left side of the page).

2. Click the bucket name to see the bucket details.

   **Visibility:** shows the current bucket setting, which is **Private** by default.

3. Click **Edit Visibility**.

4. In the **Edit Visibility** dialog box, edit the visibility settings:

   - **Visibility**
     - **Public**
     - **Private**
   - If you select **Public** to enable public access, decide whether you want to let users list the bucket contents. To set the visibility of bucket object lists, click **Allow users to list objects from this bucket**.

5. Click **Save Changes**.

**More information:**

- [Securing Object Storage](#) on page 3700
- [Managing Buckets](#) on page 3398
- [Using Pre-Authenticated Requests](#) on page 3482

**Oracle Cloud Security Response to Intel L1TF Vulnerabilities**

Intel disclosed a new set of speculative execution side-channel processor vulnerabilities affecting their processors. For more information, see [Vulnerability Note VU#584653](#). These L1 Terminal Fault (L1TF) vulnerabilities affect a number of Intel processors, and they have received the following CVE identifiers:

- CVE-2018-3615, which impacts Intel Software Guard Extensions (SGX) and has a CVSS Base Score of 7.9.
- CVE-2018-3620, which impacts operating systems and System Management Mode (SMM) running on Intel processors and has a CVSS Base Score of 7.1.
- CVE-2018-3646, which impacts virtualization software and Virtual Machine Monitors (VMM) running on Intel processors and has a CVSS Base Score of 7.1.

Oracle Cloud Infrastructure

Oracle has deployed technical mitigations across Oracle Cloud Infrastructure systems designed to prevent a malicious attacker’s virtual machine (VM) instance from accessing data from other VM instances.

However, vulnerability CVE-2018-3620 could enable a rogue user mode process to read privileged kernel memory within the same virtual machine. As a result, if you manage your own operating systems (OS), you are advised to keep up with OS security patches to address this vulnerability.

The following sections contain the details of mitigations and actions.

Oracle Cloud Infrastructure Compute

For details and required actions related to the Compute service's VM and bare metal instances, see Oracle Cloud Infrastructure Customer Advisory for L1TF Impact on the Compute Service on page 3726.

Oracle Cloud Infrastructure Database

If you use Autonomous Data Warehouse and Autonomous Transaction Processing, you have no further action to take.

For details and required actions related to Oracle Cloud Infrastructure offerings for VM DB systems, bare metal DB systems, and Exadata DB systems, see Oracle Cloud Infrastructure Customer Advisory for L1TF Impact on the Database Service on page 3730.

Platform Service and Kubernetes Services on Oracle Cloud Infrastructure

Oracle has deployed technical mitigations designed to prevent malicious attacker’s VM instance from accessing data from other VM instances on the same hypervisor.

However, vulnerability CVE-2018-3620 could enable a rogue user-mode process to read privileged kernel memory within the same virtual machine. As a result, Platform Service hosts managed by Oracle are being patched by Oracle. If you manage your own operating systems you're advised to keep up with the OS security patches to address this vulnerability.

Other Oracle Cloud Infrastructure Services

Mitigations designed to protect all other Oracle Cloud Infrastructure services have been deployed. Oracle will notify and coordinate directly with customers for any additional required maintenance activities.

Oracle Cloud Infrastructure Classic and Oracle Platform Service on Oracle Cloud Infrastructure Classic

For more information see Oracle Cloud Infrastructure Classic.

Oracle is deploying technical mitigations designed for Infrastructure and Platform Services on Oracle Cloud Infrastructure Classic. Some customers may experience reboots or downtime associated while deploying these mitigations.

Vulnerability CVE-2018-3620 could enable a rogue user-mode process to read privileged kernel memory within the same virtual machine. As a result, Platform Service hosts managed by Oracle are being patched by Oracle. If you manage your own operating systems you're advised to keep up with the OS security patches to address this vulnerability.

Oracle Cloud Infrastructure Customer Advisory for L1TF Impact on the Compute Service

Intel disclosed a new set of speculative execution side-channel processor vulnerabilities affecting their processors. For more information, see Vulnerability Note VU#584653. These L1 Terminal Fault (L1TF) vulnerabilities affect a number of Intel processors, and they have received the following CVE identifiers:

- CVE-2018-3615, which impacts Intel Software Guard Extensions (SGX) and has a CVSS Base Score of 7.9.
• CVE-2018-3620, which impacts operating systems and System Management Mode (SMM) running on Intel processors and has a CVSS Base Score of 7.1.
• CVE-2018-3646, which impacts virtualization software and Virtual Machine Monitors (VMM) running on Intel processors and has a CVSS Base Score of 7.1.

See the Oracle Cloud Security Response to Intel L1TF Vulnerabilities on page 3725 for more information.

Oracle has deployed technical mitigations across Oracle Cloud Infrastructure systems designed to prevent a malicious attacker’s virtual machine (VM) instance from accessing data from other VM instances.

You should be aware that the vulnerability CVE-2018-3620 could enable a rogue user-mode process to read privileged kernel memory within the same operating system (OS). As a result, you are advised to keep up with OS security patches to address this vulnerability. See Protecting your Compute Instance Against the L1TF Vulnerability on page 3727 for instructions to patch the OS on the instances you manage.

Additional Guidance for Oracle Cloud Infrastructure Bare Metal Instances

Bare metal instances in Oracle Cloud Infrastructure offer you full control of a physical server. Oracle Cloud Infrastructure’s network virtualization is designed and configured to protect these instances from unauthorized access of other instances on the Oracle Cloud Infrastructure network, including other customer instances, both VM instances and other bare metal instances.

If you're running your own virtualization stack or hypervisors on bare metal instances, the L1TF vulnerability allows a virtual machine to access privileged information from the underlying hypervisor or other VMs on the same bare metal instance. You should review the Intel recommendations about vulnerabilities CVE-2018-3615, CVE-2018-3620, and CVE-2018-3646, and make changes to your configurations as you deem appropriate.

Protecting your Compute Instance Against the L1TF Vulnerability

Intel disclosed a new set of speculative execution side-channel processor vulnerabilities affecting their processors, for more information, see Vulnerability Note VU#584653. These L1 Terminal Fault (L1TF) vulnerabilities affect a number of Intel processors, and they have received the following CVE identifiers:

• CVE-2018-3615 which impacts Intel Software Guard Extensions (SGX) and has a CVSS Base Score of 7.9.
• CVE-2018-3620 which impacts operating systems and System Management Mode (SMM) running on Intel processors and has a CVSS Base Score of 7.1.
• CVE-2018-3646 which impacts virtualization software and Virtual Machine Monitors (VMM) running on Intel processors and has a CVSS Base Score of 7.1.

See the Oracle Cloud Security Response to Intel L1TF Vulnerabilities on page 3725 for more information.

Recommended Action

Oracle recommends that you patch the operating systems for your existing bare metal and virtual machine (VM) instances, and verify that this includes the patch for the CVE-2018-3620 vulnerability. For VM instances, the Oracle Cloud Infrastructure team has implemented the necessary workarounds designed to mitigate the CVE-2018-3646 vulnerability. For bare metal instances using virtualization technology, you should also follow these instructions to ensure that they are mitigated against the CVE-2018-3646 vulnerability.

If you're running your own virtualization stack or hypervisors on bare metal instances, you should apply the patch for the CVE-2018-3646 vulnerability.

The following Oracle-provided image releases have been updated with the recommended patches, so instances created from these images or new image releases include the recommended patches for the L1TF vulnerability.

Oracle-provided images updated with recommended patches for the L1TF vulnerability:
Note:

Protections against the L1TF vulnerabilities are enabled by default in Oracle Linux 8, CentOS 8, and Windows Server 2019.

- Oracle-Linux-7.5-2018.08.14-0
- Oracle-Linux-7.5-Gen2-GPU-2018.08.14-0
- Oracle-Linux-6.10-2018.08.14-0
- CentOS-7-2018.08.15-0
- CentOS-6.10-2018.08.15-0 (end of support)
- Canonical-Ubuntu-18.04-2018.08.15-0
- Canonical-Ubuntu-16.04-2018.08.15-0
- Canonical-Ubuntu-16.04-Gen2-GPU-2018.08.15-0
- Canonical-Ubuntu-14.04-2018.08.15-0 (end of support)
- Windows-Server-2016-Standard-Edition-VM-Gen2-2018.08.16-0
- Windows-Server-2016-Datacenter-Edition-BM-Gen2-2018.08.16-0
- Windows-Server-2016-Datacenter-Edition-BM-Gen2-DenseIO-2018.08.16-0
- Windows-Server-2012-R2-Datacenter-Edition-BM-2018.08.15-0
- Windows-Server-2012-R2-Datacenter-Edition-BM-Gen2-DenseIO-2018.08.15-0
- Windows-Server-2012-R2-Datacenter-Edition-BM-Gen2-2018.08.15-0
- Windows-Server-2008-R2-Enterprise-Edition-VM-2018.08.15-0 (end of support)
- Windows-Server-2008-R2-Enterprise-Edition-VM-Gen2-2018.08.15-0 (end of support)

For your running instances created from imported custom images, refer to the operating system (OS) vendor's guidance to patch the OS for the L1TF vulnerability.

**Patching Oracle Linux Instances**

For Oracle Linux, the patches for the CVE-2018-3620 and CVE-2018-3646 vulnerabilities are addressed by the same set of patches.

Bare metal instances must have the latest microcode updates from Intel. This step is not required for VM instances.

To install the latest microcode updates, run the following command:

```
# sudo yum update microcode_ctl
```

The microcode RPM should be greater than or equal to microcode_ctl-2.1-29.2.0.4.e17_5.x86_64.rpm. This is the version of the microcode package that shipped for the Spectre v3a and Spectre v4 updates. No additional update is required. In addition to the microcode update, you should also patch your bare metal instances using the following set of instructions.

**To patch the OS for bare metal and VM instances with downtime**

The yum-plugin-security package allows you to use yum to obtain a list of all of the errata that are available for your system, including security updates. You can also use Oracle Enterprise Manager 12c Cloud Control or management tools such as Katello, Pulp, Red Hat Satellite, Spacewalk, and SUSE Manager to extract and display information about errata.

1. To install the **yum-plugin-security** package, run the following command:

```
# sudo yum install yum-plugin-security
```
2. Use the `--cve` option to display the errata that correspond to a specified CVE, and to install those required packages, by running the following commands:

```
# sudo yum updateinfo list --cve CVE-2018-3620
# sudo yum update --cve CVE-2018-3620
```

A system reboot will be required once the package is applied. By default, the boot manager will automatically enable the most recent kernel version. For more information on using `yum update`, visit Installing and Using the Yum Security Plugin.

3. After the system reboots, ensure that the following file is populated.

```
cat /sys/devices/system/cpu/vulnerabilities/l1tf
```

Patching Windows Instances

Protecting New Windows VM and Bare Metal Instances

When you create a new VM or bare metal instance based on the latest Oracle-provided Windows images, the image includes the Microsoft-recommended patches to protect against the L1TF vulnerability. Windows bare metal instances also include the latest microcode updates from Intel.

There is no further action required from you to protect your new Windows-based VM or bare metal instances from the L1TF vulnerability. You should ensure that you keep the your instances updated with the latest patches as recommended by your OS vendor.

Protecting Existing Windows VM and Bare Metal Instances

To update the microcode for existing bare metal instances

Bare metal instances launched before the Oracle-provided Windows images were updated must have the latest microcode updates from Intel. You need to recycle your Windows bare metal instances in order to receive the latest Intel microcode update. This step is not required for VM instances.

1. Create a new custom image of your Windows bare metal instance, see Creating Windows Custom Images on page 668 for more information.
2. Terminate your existing Windows bare metal instance.
3. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images. Find the custom image you want to use.
4. Click the Actions icon (three dots), and then click Create Instance.
5. Provide additional launch options as described in Creating an Instance on page 695.

Once you have completed these steps, perform the steps in the next procedure to update the instance with the latest OS updates from Microsoft.

To patch the OS for bare metal and VM instances with downtime

Windows images include the Windows Update utility, which you can run to get the latest Windows updates from Microsoft. You have to configure the security list on the subnet on which the instance is running to allow instances to access Windows update servers. See Windows OS Updates for Windows Images on page 636 and Security Lists on page 2850 for more information.

1. Verify that you have installed the latest Windows OS security update from Microsoft.
   a. If automatic updates are turned on, the updates should be automatically delivered to the instance.
   b. To manually check for the latest update, select Start.
   c. In Settings select Updates & security and then select Windows Update.
   d. In Windows Update, click Check for updates.
   e. When you turn on automatic updates, this update will be downloaded and installed automatically. For more information about how to turn on automatic updates, see Windows Update: FAQ.
For additional details see Windows Server guidance to protect against L1 terminal fault.

**Patching Ubuntu or CentOS Instances**

When you create a new VM or bare metal instance based on the latest Oracle-provided Ubuntu or CentOS images, the image includes the recommended patches to protect against the L1TF vulnerability, see for more information L1 Terminal Fault (L1TF) and L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646.

For existing VM or bare metal instances you should follow the guidance provided by the OS vendor for patching systems.

**Oracle Cloud Infrastructure Customer Advisory for L1TF Impact on the Database Service**

Intel disclosed a new set of speculative execution side-channel processor vulnerabilities affecting their processors. For more information, see Vulnerability Note VU#584653. These L1 Terminal Fault (L1TF) vulnerabilities affect a number of Intel processors, and they have received the following CVE identifiers:

- CVE-2018-3615, which impacts Intel Software Guard Extensions (SGX) and has a CVSS Base Score of 7.9.
- CVE-2018-3620, which impacts operating systems and System Management Mode (SMM) running on Intel processors and has a CVSS Base Score of 7.1.
- CVE-2018-3646, which impacts virtualization software and Virtual Machine Monitors (VMM) running on Intel processors and has a CVSS Base Score of 7.1.

See the Oracle Cloud Security Response to Intel L1TF Vulnerabilities on page 3725 for more information.

Oracle has deployed technical mitigations across Oracle Cloud Infrastructure systems designed to prevent a malicious attacker’s virtual machine (VM) instance from accessing data from other VM instances.

**Autonomous Data Warehouse and Autonomous Transaction Processing**

Autonomous Data Warehouse provides fully managed databases optimized for running data warehouse workloads. Autonomous Transaction Processing provides fully managed databases optimized for running online transaction processing and mixed database workloads. Autonomous Data Warehouse and Autonomous Transaction Processing are not affected by the L1TF vulnerabilities, CVE-2018-3615, CVE-2018-3620, and CVE-2018-3646. No further action is required by customers.

**Guidance for the Database Service on Bare Metal Instances**

The Database service on Oracle Cloud Infrastructure bare metal instances offer customers full control over their Oracle Database running on a physical server. Oracle Cloud Infrastructure's network virtualization is designed and configured to protect these instances from unauthorized access from other instances on the Oracle Cloud Infrastructure network, including other customer instances, both VM instances and other bare metal instances.

**Actions for Customers with VM DB Systems, Bare Metal DB Systems, or Exadata DB Systems**

Vulnerability CVE-2018-3620 could enable a rogue user-mode process to read privileged kernel memory within the same operating system. As a result, you need to patch these systems once these patches are available. These patches will be available shortly and Oracle will update this page when the operating system (OS) patches are published. Oracle will update the Database base images with the latest patches for new instance launches.

Once the patches are available, use the following instructions to patch a running instance:

- For DB systems on bare metal instances, apply the OS patches following the instructions in Updating a DB System on page 1397.
- For DB systems on a VM instance, configured using the Oracle Cloud Infrastructure Database service, apply the OS patches following the instructions in Updating a DB System on page 1397.
- For the DB systems on a VM instance configured using the Oracle Platform Service Manager, apply the OS patches following the instructions in Applying Linux OS Security Patches by Using the dbaascli Utility.
For Exadata DB systems, apply the OS patches following the instructions in Updating an Exadata Cloud Service Instance on page 1274.

Oracle Cloud Security Response to Intel Microarchitectural Data Sampling (MDS) Vulnerabilities

Intel disclosed four new speculative execution side-channel processor vulnerabilities affecting Intel processors. These vulnerabilities have received the following CVE identifiers:

- CVE-2019-11091: Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
- CVE-2018-12126: Microarchitectural Store Buffer Data Sampling (MSBDS)
- CVE-2018-12127: Microarchitectural Load Port Data Sampling (MLPDS)
- CVE-2018-12130: Microarchitectural Fill Buffer Data Sampling (MFBDS)

For more information, see https://blogs.oracle.com/security/intelmds.

Oracle Cloud Infrastructure

Oracle has deployed technical mitigations across Oracle Cloud Infrastructure systems designed to prevent a malicious attacker’s virtual machine (VM) instance from accessing data from other VM instances.

However, if you manage your own operating systems (OS), you are advised to keep up with OS security patches to address this vulnerability.

The following sections contain the details of mitigations and actions.

Oracle Cloud Infrastructure Compute

For details and required actions related to the Compute service’s VM and bare metal instances, see Oracle Cloud Infrastructure Customer Advisory for MDS Impact on the Compute Service on page 3732.

Oracle Cloud Infrastructure Database

If you use Autonomous Data Warehouse and Autonomous Transaction Processing, you have no further action to take.

For details and required actions related to offerings for VM DB systems, bare metal DB systems, and Exadata DB systems, see Oracle Cloud Infrastructure Customer Advisory for MDS Impact on the Database Service on page 3735.

Oracle Cloud Infrastructure Container Engine for Kubernetes

To help secure your existing worker nodes for the Oracle Cloud Infrastructure Container Engine for Kubernetes Oracle recommends replacing your current node pools with new node pools. Please follow the instructions described in Upgrading the Kubernetes Version on Worker Nodes in a Cluster on page 930. All worker nodes created or upgraded after May 14th, 2019 are not impacted by this security issue.

Other Oracle Cloud Infrastructure Services

Technical mitigations designed to protect all other Oracle Cloud Infrastructure services against the MDS processor vulnerabilities have been deployed. Oracle will notify customers if additional maintenance activities are required.

Oracle Cloud Infrastructure Classic and Oracle Platform Service on Oracle Cloud Infrastructure Classic

For more information see Oracle Cloud Infrastructure Classic.

In response to the MDS processor vulnerabilities, Oracle is performing mandatory maintenance for Infrastructure and Platform Services on Oracle Cloud Infrastructure Classic.
Platform Service hosts managed by Oracle are being patched by Oracle. If you manage your own operating systems, you are advised to keep up with the appropriate OS security patches to address these vulnerabilities.

**Oracle Cloud Infrastructure Customer Advisory for MDS Impact on the Compute Service**

Intel disclosed four new speculative execution side-channel processor vulnerabilities affecting Intel processors. These vulnerabilities have received the following CVE identifiers:

- CVE-2019-11091: Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
- CVE-2018-12126: Microarchitectural Store Buffer Data Sampling (MSBDS)
- CVE-2018-12127: Microarchitectural Load Port Data Sampling (MLPDS)
- CVE-2018-12130: Microarchitectural Fill Buffer Data Sampling (MFBDS)

For more information, see [https://blogs.oracle.com/security/intelmds](https://blogs.oracle.com/security/intelmds).

Oracle has deployed technical mitigations across Oracle Cloud Infrastructure systems designed to prevent a malicious attacker’s virtual machine (VM) instance from accessing data from other VM instances.

You are advised to keep up with OS security patches to address this vulnerability. See Oracle Cloud Infrastructure Compute Content Impact on page 3732 for instructions to patch the OS on the instances you manage.

**Additional Guidance for Oracle Cloud Infrastructure Bare Metal Instances**

Bare metal instances in Oracle Cloud Infrastructure offer customers full control of a physical server. Oracle Cloud Infrastructure's network virtualization is designed and configured to protect these instances from unauthorized access of other instances on the Oracle Cloud Infrastructure network, including other customer instances, both VM instances and other bare metal instances.

However, for customers running their own virtualization stack on bare metal instances, the MDS vulnerabilities could allow a virtual machine to access privileged information from the underlying hypervisor or other VMs on the same bare metal instance. These customers should review Intel’s recommendations about these MDS vulnerabilities and make the recommended changes to their configurations, [https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html](https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html).

**Oracle Cloud Infrastructure Compute Content Impact**

Intel disclosed four new speculative execution side-channel processor vulnerabilities affecting Intel processors. These vulnerabilities have received the following CVE identifiers:

- CVE-2019-11091: Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
- CVE-2018-12126: Microarchitectural Store Buffer Data Sampling (MSBDS)
- CVE-2018-12127: Microarchitectural Load Port Data Sampling (MLPDS)
- CVE-2018-12130: Microarchitectural Fill Buffer Data Sampling (MFBDS)

For more information, see [https://blogs.oracle.com/security/intelmds](https://blogs.oracle.com/security/intelmds).

**Recommended Action**

Oracle recommends that customers patch the operating systems for their existing bare metal and virtual machine (VM) instances and verify that these OS updates include the patch for the MDS vulnerabilities. For VM instances, the Oracle Cloud Infrastructure team has implemented the necessary workarounds designed to mitigate for the MDS vulnerabilities. For bare metal instances using virtualization technology, you should also follow the following instructions:

If you are running your own virtualization stack or hypervisors on bare metal instances, you should apply the appropriate patch required to address the MDS processor vulnerabilities.

The information in the following sections detail the commands needed to update your running instances created with Oracle-Provided Images on page 629.
The following Oracle-provided image releases have been updated with the recommended patches, as a result instances created using these images or subsequent images include the recommended patches for the MDS vulnerabilities.

Oracle-provided images updated with recommended patches for the MDS vulnerability

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protections against the MDS processor vulnerabilities are enabled by default in Oracle Linux 8, CentOS 8, and Windows Server 2019.</td>
</tr>
</tbody>
</table>

- Oracle-Linux-6.10-2019.05.14-0
- Oracle-Linux-7.6-2019.05.14-0
- Oracle-Linux-7.6-Gen2-GPU-2019.05.14-0
- Windows-Server-2008-R2-Enterprise-Edition-VM-2019.05.14-0 (end of support)
- Windows-Server-2012-R2-Standard-Edition-VM-2019.05.15-0
- Windows-Server-2012-R2-Standard-Edition-VM-Gen2-E2-2019.05.15-0
- Windows-Server-2012-R2-Datacenter-Edition-BM-Gen2-2019.05.14-0
- Windows-Server-2012-R2-Datacenter-Edition-BM-Gen2-DenseIO-2019.05.15-0
- Windows-Server-2012-R2-Datacenter-Edition-BM-Gen2-2019.06.17-0
- Windows-Server-2016-Datacenter-Edition-BM-Gen2-2019.05.14-0
- Windows-Server-2016-Datacenter-Edition-BM-Gen2-DenseIO-2019.05.14-0
- Windows-Server-2016-Datacenter-Edition-BM-Gen2-2019.05.15-0
- CentOS-6.10-2019.05.15-0 (end of support)
- CentOS-7-2019.05.16-0 (end of support)
- Canonical-Ubuntu-14.04-2019.05.15-0 (end of support)
- Canonical-Ubuntu-16.04-2019.05.15-0
- Canonical-Ubuntu-16.04-Gen2-GPU-2019.05.15-0
- Canonical-Ubuntu-16.04-Minimal-2019.05.15-0
- Canonical-Ubuntu-18.04-2019.05.15-0
- Canonical-Ubuntu-18.04-Minimal-2019.05.15-0

Customers running instances created from imported third-party images should refer to the operating system (OS) vendor's guidance to patch the OS for the MDS vulnerability.

Patching Oracle Linux Instances

Oracle has released security patches for Oracle Linux 6, Oracle Linux 7, and Oracle VM Server for X86 products. In addition to the OS patches, customers should run the latest version of the microcode from Intel to mitigate these issues. For both bare metal and VM instances, please install the latest Ksplice via uptrack-upgrade.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>See Installing Ksplice Utrack Within the Oracle Cloud Infrastructure for how to install Ksplice.</td>
</tr>
</tbody>
</table>

For Oracle Linux, the patches for the MDS vulnerabilities are addressed by the same set of patches. For further information please see the following:


Oracle Cloud Infrastructure User Guide 3733
Bare metal instances must have the latest microcode updates from Intel. This step is not required for VM instances. To install the latest microcode updates on bare metal instances, run the following command:

```
# sudo yum update microcode_ctl
```

The required versions of microcode_ctl rpms are:

- **Oracle Linux 7**: microcode_ctl 2.1-47.0.4
- **Oracle Linux 6**: microcode_ctl 1.17-1002

No additional update is required. In addition to the microcode update, you should also patch your bare metal instances using the following set of instructions.

**To patch the OS for bare metal and VM instances with downtime**

The `yum-plugin-security` package allows you to use yum to obtain a list of all errata that are available for your system, including security updates. You can also use Oracle Enterprise Manager 12c Cloud Control or management tools such as Katello, Pulp, Red Hat Satellite, Spacewalk, and SUSE Manager to extract and display information about errata.

1. To install the `yum-plugin-security` package, run the following command:

   ```
   # sudo yum install yum-plugin-security
   ```

2. Use the `--cve` option to display the errata that correspond to a specified CVE, and to install those required packages, by running the following commands:

   ```
   # sudo yum updateinfo list --cve CVE-####-####
   # sudo yum update --cve CVE-####-####
   ```

   Replace `####-####` in the above commands with the relevant CVE numbers.

3. A system reboot will be required once the package is applied. By default, the boot manager will automatically enable the most recent kernel version. For more information on using yum update, visit Installing and Using the Yum Security Plugin.

4. After the system reboots, ensure that the following file is populated:

   ```
   cat /sys/devices/system/cpu/vulnerabilities/mds
   ```

**Patching Windows Instances**

**Protecting New Windows VM and Bare Metal Instances**

When you create a new VM or bare metal instance based on the latest Oracle-provided Windows images, the image includes the Microsoft-recommended patches to protect against the MDS vulnerability. Windows bare metal instances also include the latest microcode updates from Intel. To apply the MDS patch install the latest Windows updates and reboot the instance. You should ensure that you keep your instances updated with the latest patches as recommended by your OS vendor.

**Protecting Existing Windows VM and Bare Metal Instances**

To update the microcode for existing bare metal instances

Bare metal instances launched before the Oracle-provided Windows images were updated must have the latest microcode updates from Intel. You need to recycle your Windows bare metal instances in order to receive the latest Intel microcode update. This step is not required for VM instances.

1. Create a new custom image of your Windows bare metal instance, see Creating Windows Custom Images on page 668 for more information.
2. Terminate your existing Windows bare metal instance.
3. Open the navigation menu. Under Core Infrastructure, go to Compute and click Custom Images. Find the custom image you want to use.
4. Click the Actions icon (three dots), and then click Create Instance.
5. Provide additional launch options as described in Creating an Instance on page 695.

Once you have completed these steps, perform the steps in the next procedure to update the instance with the latest OS updates from Microsoft.

To patch the OS for bare metal and VM instances with downtime:

Windows images include the Windows Update utility, which you can run to get the latest Windows updates from Microsoft. You have to configure the security list on the subnet on which the instance is running to allow instances to access Windows update servers. See Windows OS Updates for Windows Images and Security Lists for more information.

1. Verify that you have installed the latest Windows OS security update from Microsoft.
   a. If automatic updates are turned on, the updates should be automatically delivered to the instance.
   b. To manually check for the latest update, select Start.
   c. In Settings select Updates & security and then select Windows Update.
   d. In Windows Update, click Check for updates.
   e. When you turn on automatic updates, this update will be downloaded and installed automatically. For more information about how to turn on automatic updates, see Windows Update: FAQ.

For additional details see Windows Server guidance to protect against speculative execution side-channel vulnerabilities.

Patching Ubuntu or CentOS Instances

The recommended patches to protect against the MDS vulnerabilities are included when you create a new VM or bare metal instance based on the latest Oracle-provided Ubuntu or CentOS images, see Microarchitectural Data Sampling (MDS) and MDS - Microarchitectural Store Buffer Data - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, and CVE-2019-11091. For existing VM or bare metal instances you should follow the patching guidance provided by the original OS vendor.

Note:

Any images published after May 14, 2019 listed in the image release notes will include the MDS patches. If using earlier images already launched, follow patching instructions.

Oracle Cloud Infrastructure Customer Advisory for MDS Impact on the Database Service

Intel disclosed 4 new speculative execution side-channel processor vulnerabilities affecting Intel processors. These vulnerabilities have received the following CVE identifiers:

- CVE-2019-11091: Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
- CVE-2018-12126: Microarchitectural Store Buffer Data Sampling (MSBDS)
- CVE-2018-12127: Microarchitectural Load Port Data Sampling (MLPDS)
- CVE-2018-12130: Microarchitectural Fill Buffer Data Sampling (MFBDS)

For more information, see https://blogs.oracle.com/security/intelmds.

Oracle has deployed technical mitigations across Oracle Cloud Infrastructure systems designed to prevent a malicious attacker’s virtual machine (VM) instance from accessing data from other VM instances.

Autonomous Data Warehouse and Autonomous Transaction Processing

Autonomous Data Warehouse provides fully managed databases optimized for running data warehouse workloads.
Autonomous Transaction Processing provides fully managed databases optimized for running online transaction processing and mixed database workloads.

Autonomous Data Warehouse and Autonomous Transaction Processing are not affected by MDS vulnerabilities. These services do not run on their own hypervisor and they do not allow for the execution of untrusted code in their services enclave. Customers can execute code within their own instances and each customer instance is isolated from that of another customer. No further customer action is currently required.

**Guidance for the DatabaseService on Bare Metal Instances**

The Database service on Oracle Cloud Infrastructure bare metal instances offer customers full control over their Oracle Database running on a physical server. Oracle Cloud Infrastructure's network virtualization is designed and configured to protect these instances from unauthorized access from other instances on the Oracle Cloud Infrastructure network, including other customer instances, both VM instances and other bare metal instances. As a result, the Database service on bare metal instances are not affected by the MDS vulnerabilities.

**Actions for Customers with VM DB Systems, Bare Metal DB Systems, or Exadata DB Systems**

Customers are advised to apply available patches at the earliest possible time. Use the following instructions to patch a running instance:

- For DB systems on bare metal instances, apply the OS patches following the instructions in Updating a DB System on page 1397.
- For DB systems on a VM instance, configured using the Oracle Cloud Infrastructure Database service, apply the OS patches following the instructions in Updating a DB System on page 1397.
- For the DB systems on a VM instance configured using the Oracle Platform Service Manager, apply the OS patches following the instructions in Applying Linux OS Security Patches by Using the dbaascli Utility.
- For Exadata DB systems, apply the OS patches following the instructions in Updating an Exadata Cloud Service Instance on page 1274.
Chapter 34

Security Advisor

This chapter explains how to use Security Advisor to create more secure resources.

Overview of Security Advisor

Oracle Cloud Infrastructure Security Advisor supports and reinforces what's required of the tenancy by Security Zones configurations. It does this by combining and streamlining existing workflows to efficiently create resources that meet baseline security requirements from the outset. Specifically, you can assign a new customer-managed encryption key to a resource at the time that you create the resource, even if you've never created a vault or encryption key before. Security zones require encryption using customer-managed keys where possible because no one but an authorized user can access the keys, thereby resulting in sensitive data that can only be decrypted and read by those explicitly allowed.

Streamlined workflows reduce complexity and decision-making. Where you would otherwise need to choose between configuration settings, Security Advisor provides only the more secure option. For example, Security Advisor only allows you to create master encryption keys that are 256 bits in length. Longer encryption keys provide greater security than shorter ones.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Security Advisor leverages the functionality of existing workflows, so the tenancy might not need new policies to grant permissions beyond what's already in place. To be sure, you can compare the tenancy's existing policies with the example permissions described in the chosen workflow. In particular, confirm that you have policies that grant access to Vault resources, especially if you haven't used the service previously.

The example policy statements make it possible for the specified groups to do anything allowed by Security Advisor. If, instead, you wanted to limit the creation of new vaults, you can write a policy that grants permission only to use vaults, rather than the level of access required to manage vaults. With permission to use vaults, a user can select an existing vault, but cannot create a new one. This does not change the options that Security Advisor presents, but it does affect whether all operations succeed when submitted.
Regions and Availability Domains

You can use Security Advisor in all Oracle Cloud Infrastructure commercial regions. For a list of regions, along with associated locations, region identifiers, region keys, and availability domains, see About Regions and Availability Domains on page 180.

Each service that integrates with Security Advisor has a single regional endpoint for all API operations, with one exception. The Vault service has one regional endpoint for the provisioning service that handles create, update, and list operations for vaults. For create, update, and list operations for keys, service endpoints are distributed across multiple independent clusters.

Limits on Resources

Security Advisor does not introduce resources and does not impose restrictions on your usage level of any resource. Security Advisor does, however, respect the limits instituted by other services.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

For instructions to view your usage level against the tenancy's resource limits, see Viewing Your Service Limits, Quotas, and Usage on page 216. For vaults, you can also get each individual vault's usage against key limits by viewing key and key version counts in the vault details.

Creating a Secure Bucket

This topic describes how to use Security Advisor to create a secure bucket. In this context, a secure bucket is one that is encrypted with a customer-managed key and therefore meets minimum security requirements established by security zones. The process involves creating not only the bucket, but also the Vault key that you want to use to encrypt the bucket, and then assigning the key to the bucket. (You cannot use Security Advisor to assign existing encryption keys, but you can use an existing vault to create a new key.)

Other security considerations exist outside Security Advisor, particularly regarding the use of resources after you create them. We strongly encourage you to learn more about Oracle Cloud Infrastructure Object Storage security features and best practices, and then implement them with your newly created resource. For more information, see Securing Object Storage on page 3700 and Using Your Own Keys for Server-Side Encryption on page 3491.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators:

- The following policy lets the specified group do everything with buckets and objects in the specified compartment:

  Allow group CreateSecureOSBucketGroup to manage object-family in compartment CompartmentABC

- The following policy lets the specified group do everything with vaults in the specified compartment, which might not be the same compartment as the bucket compartment. (If you prefer, you can write a policy that grants the use vaults permission instead. With that permission, the specified group can use existing vaults, but cannot create new ones.)

  Allow group CreateSecureOSBucketGroup to manage vaults in compartment CompartmentDEF
The following policy lets the specified group do everything with keys in the specified compartment, which must be the same compartment as the vault compartment:

```
Allow group CreateSecureOSBucketGroup to manage keys in compartment CompartmentDEF
```

The following policy lets the Object Storage service list, view, and perform cryptographic operations with all keys in the specified compartment:

```
Allow service ObjectStorage-<region_name> to use keys in compartment CompartmentDEF
```

In the preceding example, replace `<region_name>` with the appropriate region identifier, for example:

- objectstorage-us-phoenix-1
- objectstorage-us-ashburn-1
- objectstorage-eu-frankfurt-1
- objectstorage-uk-london-1
- objectstorage-ap-tokyo-1

To determine the region name value of an Oracle Cloud Infrastructure region, see Regions and Availability Domains on page 180.

For more information about how policies work, see How Policies Work on page 2136.

**Using the Console**

**To create a secure bucket**

1. Open the navigation menu. Under the Governance and Administration group, go to Security, and click Overview.
2. Click Create Secure Bucket.
3. Review the prerequisites for getting started, and then click Next when you're ready.
4. Do one of the following:
   - To create a master encryption key in an existing vault, click Choose existing vault.
   - To create a master encryption key in a new vault, click Create new vault.
5. Then, do one of the following:
   - If you chose to use an existing vault in the previous step, choose the compartment where the vault resides, and then choose the vault.
   - If you chose to create a new vault in the previous step, choose the compartment where you want to create the vault, and then enter a display name to identify the vault. Avoid entering confidential information. Optionally, make the vault a virtual private vault by selecting the Make it a virtual private vault check box. For more information about vault types, see Key and Secret Management Concepts on page 3953.
6. When you're ready, click Next.
7. Click Key Name, and then enter a name to identify the key. Avoid entering confidential information.
8. Regarding Key Shape: Length, the key length value is fixed at 256 bits to maximize security based on key length.
9. Optionally, if you want to import key material to create a key, select the Import external key check box. Importing key material requires you to first generate the key material and wrap it using a vault's public wrapping key. This means that you cannot use Security Advisor to create a key using imported key material without an existing vault. For more information about importing keys, see Importing Keys and Key Versions on page 3986.
10. Optionally, to apply tags, click Show Tagging Options. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure
if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. When you're ready, click Next.

10. On the Create Bucket page, specify the attributes of the bucket:

- **Bucket Name:** The system generates a default bucket name that reflects the current year, month, day, and time, for example `bucket-20190306-1359`. If you change this default to any other bucket name, use letters, numbers, dashes, underscores, and periods. Avoid entering confidential information.

- **Create in Compartment:** The compartment where you want the bucket to reside. This does not need to be the same compartment as the vault and key.

- **Storage Tier:** Select the tier in which you want to store your data. Available tiers include:
  - **Standard** is the primary, default Object Storage tier for storing frequently accessed data that requires fast and immediate access.
  - **Archive** is a special tier for storing infrequently accessed data that requires long retention periods. Access to data in the Archive tier is not immediate. Archived data must be restored before the data is accessible. For more information, see “Overview of Archive Storage on page 484” in the Oracle Cloud Infrastructure User Guide.
  - **Object Events:** Select Emit Object Events if you want to enable the bucket to emit events for object state changes. For more information about events, see Overview of Events on page 1784.
  - **Object Versioning:** Select Enable Object Versioning if you want Object Storage to create an object version each time the content changes or the object is deleted. For more information, see Using Object Versioning on page 3446.

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

When you're ready, click **Next**.

11. Review the summary of the resources that Security Advisor will create, and then click **Create Secure Bucket**.

### Creating a Secure File System

This topic describes how to use Security Advisor to create a secure file system. The process involves creating not only the file system, but also the Vault key that you want to use to encrypt the file system, and then assigning the key to the file system. (You cannot use Security Advisor to assign existing encryption keys, but you can use an existing vault to create a new key.)

Using Security Advisor to create a file system comes with some limitations. You cannot use Security Advisor to create a file system with a new mount target. You must reuse an existing mount target.

Other security considerations exist outside Security Advisor, particularly regarding the use of resources after you create them. We strongly encourage you to learn more about Oracle Cloud Infrastructure File Storage security features and best practices, and then implement them with your newly created resources. For more information, see Securing File Storage on page 3687 and About Security on page 1925.

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators:

- The following policy lets the specified group do everything with file systems and mount targets in the specified compartment:

```plaintext
Allow group CreateSecureFileStorageGroup to manage file-family in compartment CompartmentABC
```
The following policy lets the specified group do everything with vaults in the specified compartment, which might not be the same compartment as the file system compartment. (If you prefer, you can write a policy that grants the use vaults permission instead. With that permission, the specified group can use existing vaults, but cannot create new ones.)

```
Allow group CreateSecureFileStorageGroup to manage vaults in compartment CompartmentDEF
```

The following policy lets the specified group do everything with keys in the specified compartment, which must be the same compartment as the vault compartment:

```
Allow group CreateSecureFileStorageGroup to manage keys in compartment CompartmentDEF
```

The following policy lets the File Storage service list, view, and perform cryptographic operations with all keys in the specified compartment:

```
Allow service FssOciProd to use keys in compartment CompartmentDEF
```

In the preceding example, the policy refers to the File Storage service by the service principal name FssOciProd.

For more information about how policies work, see How Policies Work on page 2136.

**Using the Console**

**To create a secure file system**

1. Open the navigation menu. Under the Governance and Administration group, go to Security, and click Overview.
2. Click Create Secure File System.
3. Review the prerequisites for getting started, and then click Next when you're ready.
4. Do one of the following:
   - To create a master encryption key in an existing vault, click Choose existing vault.
   - To create a master encryption key in a new vault click Create new vault.
5. Then, do one of the following:
   - If you chose to use an existing vault in the previous step, choose the compartment where the vault resides, and then choose the vault.
   - If you chose to create a new vault in the previous step, choose the compartment where you want to create the vault, and then enter a display name to identify the vault. Avoid entering confidential information. Optionally, make the vault a virtual private vault by selecting the Make it a virtual private vault check box. For more information about vault types, see Key and Secret Management Concepts on page 3953.
6. When you're ready, click Next.
7. Click Key Name, and then enter a name to identify the key. Avoid entering confidential information.
8. Regarding Key Shape: Length, the key length value is fixed at 256 bits to maximize security based on key length.
9. Optionally, if you want to import key material to create a key, select the Import external key check box. Importing key material requires you to first generate the key material and wrap it using a vault's public wrapping key. This means that you cannot use Security Advisor to create a key using imported key material without an existing vault. For more information about importing keys, see Importing Keys and Key Versions on page 3986.
10. Optionally, to apply tags, click Show Tagging Options. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. When you're ready, click Next.
10. On the **Create File System** page, specify the attributes of the file system:

- **File System Information:**
  - **Compartment:** The compartment where you want the file system to reside. You must choose a compartment where you have the required existing mount target.
  - **Name:** File Storage creates a default name using "FileSystem-YYMMDD-HHMM". Optionally, change the default name for the file system. It doesn't have to be unique; an Oracle Cloud Identifier (OCID) uniquely identifies the file system. Avoid entering confidential information.
  - **Availability domain:** The availability domain within the current region where you want to place the file system.
  - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- **Export Information**
  Mount targets use exports to manage access to file systems. The path name uniquely identifies the file system within the mount target, and is used by an instance to mount the file system.

  - **Export Path:** The File Storage service creates a default export path using the file system name. Optionally, replace the default export path name with a new path name, preceded by a forward slash (/). For example, /fss. This value specifies the mount path to the file system (relative to the mount target IP address or hostname). Avoid entering confidential information.

    **Important:**
    The export path must start with a slash (/) followed by a sequence of zero or more slash-separated elements. For multiple file systems associated with a single mount target, the export path sequence for the first file system cannot contain the complete path element sequence of the second file system export path sequence. Export paths cannot end in a slash. No export path element can be a period (.) or two periods in sequence (..). No export path can exceed 1024 bytes. Lastly, no export path element can exceed 255 bytes. For example:

    Acceptable:
    
    `/example` and `/path`
    `/example` and `/example2`

    Not Acceptable:
    
    `/example` and `/example/path`
    `/ and /example`
    `/example/`
    `/example/path/ ../example1`

    **Caution:**
    If one file system associated to a mount target has '/' specified as an export path, you can't associate another file system with that mount target.

    **Note:**
    Export paths cannot be edited after the export is created. If you want to use a different export path, you must create a new export with the
For more information, see Paths in File Systems on page 2006.

- **Use Secure Export Options:** Select to set the export options to require NFS clients to use a privileged port (1-1023) as its source port. This option enhances security because only a client with root privileges can use a privileged source port. After the export is created, you can edit the export options to adjust security. See Working with NFS Export Options on page 1934 for more information.

  **Caution:** Leaving the Use Secure Export Options setting unselected lets unprivileged users read and modify any file or directory on the target file system.

- **Mount Target Information:**

  File systems must be associated with a mount target to be mounted by an instance. If you don't have a mount target in the selected availability domain in the compartment, you must choose a different availability domain or create the file system in a compartment and availability domain where you do have a mount target.

  When you're ready, click **Next**.

11. Review the summary of the resources that Security Advisor will create, and then click **Create Secure File System**.

**Creating a Secure Virtual Machine Instance**

This topic describes how to use Security Advisor to create a secure virtual machine (VM) instance. In this context, a secure instance is one with a boot volume that is encrypted with a customer-managed key and therefore meets minimum security requirements established by security zones. The process involves creating not only the instance and associated boot volume, but also the Vault key that you want to use to encrypt the volume, and then assigning the key to the volume. (You cannot use Security Advisor to assign existing encryption keys, but you can use an existing vault to create a new key.)

Using Security Advisor to create a virtual machine instance comes with some limitations. They include the following:

- You cannot configure private or public IP addresses for an instance.
- You cannot change the image build. It will always use the latest version.
- You cannot launch the instance on a dedicated virtual machine host, which lets you run the instance in isolation so that it is not running on shared infrastructure.
- You cannot specify the volume performance settings for the boot volume.
- You cannot use Security Advisor to generate SSH keys for you if you want to remotely connect to the instance by using Secure Shell (SSH). You must generate your own SSH keys and have the public key available when you create the instance.

Other security considerations exist outside Security Advisor, particularly regarding the use of resources after you create them. We strongly encourage you to learn more about Oracle Cloud Infrastructure Compute and Oracle Cloud Infrastructure Block Volume security features and best practices, and then implement them with your newly created resources. For more information, see Securing Compute on page 3677, Securing Block Volume on page 3675, and Best Practices for Your Compute Instance on page 594.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators:
Security Advisor

- The following policy lets the specified group list and use all components in Networking in the specified compartment. This includes virtual cloud networks (VCNs), subnets, gateways, virtual circuits, security lists, route tables, and so on.

```
Allow group CreateSecureVMGroup to use virtual-network-family in compartment CompartmentABC
```

- The following policy lets the specified group create and manage instance images in the specified compartment:

```
Allow group CreateSecureVMGroup to manage instance-family in compartment CompartmentABC
```

- The following policy lets the specified group do everything with vaults in the specified compartment, which might not be the same compartment as the instance compartment. (If you prefer, you can write a policy that grants the use vaults permission instead. With that permission, the specified group can use existing vaults, but cannot create new ones.)

```
Allow group CreateSecureVMGroup to manage vaults in compartment CompartmentDEF
```

- The following policy lets the specified group do everything with keys in the specified compartment, which must be the same compartment as the vault compartment:

```
Allow group CreateSecureVMGroup to manage keys in compartment CompartmentDEF
```

- The following policy lets the Block Volume service list, view, and perform cryptographic operations with all keys in the specified compartment. The Block Volume service is responsible for the boot volume attached to the instance.

```
Allow service blockstorage to use keys in compartment CompartmentDEF
```

For more information about how policies work, see How Policies Work on page 2136.

Using the Console

To create a secure virtual machine instance

1. Open the navigation menu. Under the Governance and Administration group, go to Security, and click Overview.
2. Click Create Secure Bucket.
3. Review the prerequisites for getting started, and then click Next when you're ready.
4. Do one of the following:
   - To create a master encryption key in an existing vault, click Choose existing vault.
   - To create a master encryption key in a new vault click Create new vault.
5. Then, do one of the following:
   - If you chose to use an existing vault in the previous step, choose the compartment where the vault resides, and then choose the vault.
   - If you chose to create a new vault in the previous step, choose the compartment where you want to create the vault, and then enter a display name to identify the vault. Avoid entering confidential information. Optionally, make the vault a virtual private vault by selecting the Make it a virtual private vault check box. For more information about vault types, see Key and Secret Management Concepts on page 3953.
6. When you're ready, click Next.
7. Click Key Name, and then enter a name to identify the key. Avoid entering confidential information.
8. Regarding Key Shape: Length, the key length value is fixed at 256 bits to maximize security based on key length.
8. Optionally, if you want to import key material to create a key, select the Import external key check box. Importing key material requires you to first generate the key material and wrap it using a vault's public wrapping key. This means that you cannot use Security Advisor to create a key using imported key material without an existing vault. For more information about importing keys, see Importing Keys and Key Versions on page 3986.

9. Optionally, to apply tags, click Show Tagging Options. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. When you're ready, click Next.

10. On the Create Compute Instance page, specify the attributes of the instance:

   - **Name**: A display name for the instance. You can add or change the name later. The name doesn't need to be unique, because an Oracle Cloud Identifier (OCID) uniquely identifies the instance. Avoid entering confidential information.
   - **Create in Compartment**: The compartment where you want to create the instance. This does not need to be the same compartment as the vault and key.
   - **Image or Operating System**: By default, an Oracle Linux 7.x image is used to boot the instance. You cannot use Security Advisor to create a virtual machine instance with a different image.
   - **Availability Domain**: The availability domain where you want to create the instance.
   - **Shape**: The default shape for the selected image and availability domain combination. You cannot use Security Advisor to create a virtual machine instance with a different shape. For more information about shapes, see Compute Shapes on page 655.

11. In the Configure networking section, configure the network details for the instance:

   - **Virtual cloud network compartment**: The compartment containing the network in which to create the instance.
   - **Virtual cloud network**: The network in which to create the instance. You can only choose an existing virtual cloud network (VCN). You cannot use Security Advisor to create a new VCN. If you have a VCN in a different compartment, click Change compartment, and then select a different compartment.
   - **Subnet**: A subnet within the cloud network to attach the instance to. Subnets are either public or private. Private means the instances in that subnet can't have public IP addresses. For a more secure instance, we recommend that you choose a private subnet. For more information, see Access to the Internet on page 2752. Subnets can also be either AD-specific or regional (regional ones have "regional" after the name). We recommend using regional subnets. For more information, see About Regional Subnets on page 2822.
   - **By default, when you create an instance in a public subnet, you can optionally assign the instance a public IP address. A public IP address makes the instance accessible from the internet. You cannot use Security Advisor to create a virtual machine instance with a public IP address.**

12. In the Boot volume section, configure the size and encryption options for the instance's boot volume:

   - **To specify a custom size for the boot volume, select the Specify a custom boot volume size check box. Then, enter a custom size from 50 GB to 32 TB.** The specified size must be larger than the default boot volume size for the selected image. See Custom Boot Volume Sizes on page 610 for more information.
   - **To encrypt data while the data is in transit between the instance and the attached boot volume, select the Use in-transit encryption check box.** The Vault service encryption key that you use to encrypt the boot volume data at rest will also be used for in-transit encryption. For more information, see Block Volume Encryption on page 504. Security zones require data to be encrypted in-transit, so you must select this check box to comply with security zone requirements.
13. In the **Add SSH keys** section, generate an SSH key pair or upload your own public key. Select one of the following options:

- **Choose SSH key files**: Upload the public key portion of your key pair. Either browse to the key file that you want to upload, or drag and drop the file into the box. To provide multiple keys, press and hold down the Command key (on Mac) or the CTRL key (on Windows) while selecting files.
- **Paste SSH keys**: Paste the public key portion of your key pair in the box.
- **No SSH keys**: Select this option only if you do not want to connect to the instance using SSH. You cannot provide a public key or save the key pair that is generated by Oracle Cloud Infrastructure after the instance is created.

14. Optionally, to configure tags, click **Show Tagging Options**. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

15. Review the summary of the resources that Security Advisor will create, and then click **Create Secure Instance**.

### Creating a Secure Block Volume

This topic describes how to use Security Advisor to create a secure block volume. In this context, a secure block volume is one that is encrypted with a customer-managed key and therefore meets minimum security requirements established by security zones. The process involves creating not only the block volume, but also the Vault key that you want to use to encrypt the volume, and then assigning the key to the volume. (You cannot use Security Advisor to assign existing encryption keys, but you can use an existing vault to create a new key.)

Using Security Advisor to create a block volume comes with some limitations. You cannot use Security Advisor to create a block volume with a backup policy. See **Policy-Based Backups** on page 547 for more information about backup policies.

Other security considerations exist outside Security Advisor, particularly regarding the use of resources after you create them. We strongly encourage you to learn more about Oracle Cloud Infrastructure Compute and Oracle Cloud Infrastructure Block Volume security features and best practices, and then implement them with your newly created resources. For more information, see **Securing Compute** on page 3677, **Securing Block Volume** on page 3675, and **Best Practices for Your Compute Instance** on page 594.

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators:

- The following policy lets the specified group do everything with block storage volumes, volume backups, and volume groups in the specified compartment:

  ```
  Allow group CreateSecureBlockVolumeGroup to manage volume-family in compartment CompartmentABC
  ```

- The following policy lets the specified group do everything with vaults in the specified compartment, which might not be the same compartment as the volume compartment. (If you prefer, you can write a policy that grants the use vaults permission instead. With that permission, the specified group can use existing vaults, but cannot create new ones.)

  ```
  Allow group CreateSecureBlockVolumeGroup to manage vaults in compartment CompartmentDEF
  ```
The following policy lets the specified group do everything with keys in the specified compartment, which must be the same compartment as the vault compartment:

```plaintext
Allow group CreateSecureBlockVolumeGroup to manage keys in compartment CompartmentDEF
```

The following policy lets the Block Volume service list, view, and perform cryptographic operations with all keys in the specified compartment:

```plaintext
Allow service blockstorage to use keys in compartment CompartmentDEF
```

For more information about how policies work, see How Policies Work on page 2136.

**Using the Console**

**To create a secure block volume**

1. Open the navigation menu. Under the Governance and Administration group, go to Security, and click Overview.
2. Click Create Secure Bucket.
3. Review the prerequisites for getting started, and then click Next when you're ready.
4. Do one of the following:
   - To create a master encryption key in an existing vault, click Choose existing vault.
   - To create a master encryption key in a new vault click Create new vault.
5. Then, do one of the following:
   - If you chose to use an existing vault in the previous step, choose the compartment where the vault resides, and then choose the vault.
   - If you chose to create a new vault in the previous step, choose the compartment where you want to create the vault, and then enter a display name to identify the vault. Avoid entering confidential information. Optionally, make the vault a virtual private vault by selecting the Make it a virtual private vault check box. For more information about vault types, see Key and Secret Management Concepts on page 3953.

When you're ready, click Next.

6. Click Key Name, and then enter a name to identify the key. Avoid entering confidential information.

7. Regarding Key Shape: Length, the key length value is fixed at 256 bits to maximize security based on key length.

8. Optionally, if you want to import key material to create a key, select the Import external key check box. Importing key material requires you to first generate the key material and wrap it using a vault's public wrapping key. This means that you cannot use Security Advisor to create a key using imported key material without an existing vault. For more information about importing keys, see Importing Keys and Key Versions on page 3986.

9. Optionally, to apply tags, click Show Tagging Options. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. When you're ready, click Next.

10. On the Create Block Volume page, specify the attributes of the volume:
   - **Block Volume Name**: A user-friendly name or description. Avoid entering confidential information.
   - **Compartment**: The compartment where you want to create the volume.
   - **Availability Domain**: Must be in the same availability domain as the instance you plan to use this block volume with.
   - **Volume Size and Performance**: The volume size must be between 50 GB and 32 TB. You can choose in 1 GB increments within this range. The default is 1024 GB. If you choose a size outside of your service limit, you may be prompted to request an increase. For more information, see Service Limits on page 215. The
default option for performance settings is **Balanced**. See [Block Volume Elastic Performance](#) on page 581 for more information about volume performance options.

- **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

When you're ready, click **Next**.

11. Review the summary of the resources that Security Advisor will create, and then click **Create Secure Block Volume**.
Chapter 35

Service Connector Hub

This chapter explains how to move data between Oracle Cloud Infrastructure services using Service Connector Hub.

Service Connector Hub Overview

Service Connector Hub is a cloud message bus platform that offers a single pane of glass for describing, executing, and monitoring movement of data between services in Oracle Cloud Infrastructure.

Note:
Service Connector Hub is not available in Oracle Cloud Infrastructure Government Cloud realms.

How Service Connector Hub Works

Service Connector Hub orchestrates data movement between services in Oracle Cloud Infrastructure.

Data is moved using service connectors. A service connector specifies the source service that contains the data to be moved, tasks to run on the data, and the target service for delivery of data when tasks are complete.

Service Connector Hub Concepts

The following concepts are essential to working with Service Connector Hub.

service connector
The definition of the data to be moved. Specifies a source service, target service, and optional tasks.

source
The service containing the data to be moved according to specified tasks. Example: Logging.

target
The service receiving the data from the source, according to specified tasks. A given target service may process, store, or deliver received data. Functions processes received data while Logging Analytics, Monitoring, Object Storage, and Streaming store received data. Notifications delivers received data.

task
Optional filtering to apply to the data before moving it from the source service to the target service.

trigger
The condition that must be met for the service connector to run. Currently the trigger is continuous; that is, service connectors run continuously.

Flow of Data

When a service connector runs, it receives data from the source service, completes optional tasks on the data (such as filtering), and then moves the data to the target service.
Availability

The Service Connector Hub service is available in all Oracle Cloud Infrastructure commercial regions. See About Regions and Availability Domains on page 180 for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

Resource Identifiers

Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

Ways to Access Service Connector Hub

You can access the Service Connector Hub service using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

Console: To access Service Connector Hub using the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Open the navigation menu. Under Data and AI, click Service Connector Hub.

You can also access Service Connector Hub from Logging in the Console: Open the navigation menu. Under Solutions and Platform, go to Logging, and then click Service Connectors.

API: To access Service Connector Hub through API, use Service Connector Hub API. To access this API using the Command Line Interface (CLI), use the designation for service connectors: oci sch service-connector. For more details about the CLI, see Command Line Reference for Service Connector Hub.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).
An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Access to Service Connector Hub

Administrators: For common policies that give groups access to Service Connector Hub, see Allow a group to manage service connectors on page 2160.

Write Access to Target Services

Note: Make sure any policy you create complies with your company guidelines.

To move data, you must give your service connector the required authorization to write to the specified target resource in the target service. (Service connectors can read all supported source services.)

A default policy providing the required authorization is offered when you use the Console to define the target service for a service connector. This policy is limited to the context of the service connector. You can either accept this default policy or make sure you have the proper authorizations in a group-based policy.

Default Policies for Target Services

This section details the default policies offered when you define a target service in a new or updated service connector in the Console.

Functions

Where this policy is created: The compartment where the function resides. The function is selected when you create or edit service connector.

```
ALLOW any-user TO use fn-function IN COMPARTMENT ID <target_function_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    request.principal.compartment.id='<serviceconnector_compartment_OCID>'
}
ALLOW any-user TO use fn-invocation IN COMPARTMENT ID <target_function_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    request.principal.compartment.id='<serviceconnector_compartment_OCID>'
}
```

Logging Analytics

Where this policy is created: The compartment where the log group resides. The log group is selected or entered when you create or edit a service connector.

```
ALLOW any-user TO use loganalytics-log-group IN COMPARTMENT ID <target_log_group_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    target.loganalytics-log-group.id=<log_group_OCID>,
    request.principal.compartment.id=<serviceconnector_compartment_OCID>
}
```
Monitoring

Where this policy is created: The compartment where the metric namespace resides. The metric namespace is selected or entered when you create or edit a service connector.

```plaintext
ALLOW any-user TO use metrics IN COMPARTMENT ID <target_metric_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    target.metrics.namespace='<metric_namespace>',
    request.principal.compartment.id='<serviceconnector_compartment_OCID>'
}
```

Notifications

Where this policy is created: The compartment where the topic resides. The topic is selected when you create or edit service connector.

```plaintext
ALLOW any-user TO use ons-topics IN COMPARTMENT ID <target_topic_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    request.principal.compartment.id='<serviceconnector_compartment_OCID>'
}
```

Object Storage

Where this policy is created: The compartment where the bucket resides. The bucket is selected when you create or edit service connector.

```plaintext
ALLOW any-user TO manage objects IN COMPARTMENT ID <target_bucket_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    target.bucket.name='<bucket_name>',
    request.principal.compartment.id='<serviceconnector_compartment_OCID>'
}
```

Streaming

Where this policy is created: The compartment where the stream resides. The stream is selected when you create or edit service connector.

```plaintext
ALLOW any-user TO use stream-push IN COMPARTMENT ID <target_stream_compartment_OCID>
WHERE ALL {
    request.principal.type='serviceconnector',
    target.stream.id='<stream_OCID>',
    request.principal.compartment.id='<serviceconnector_compartment_OCID>'
}
```

When reviewing group-based policies for required authorization to write to a target service, reference the default policy offered for that target service (see previous section) or see the policy details for the target service at Policy Reference on page 2167.

**Note:**
To accept the default policy for an existing service connector, simply edit the service connector. The default policy is offered whenever you create or edit a
service connector (the only exception is when the exact policy already exists in IAM, in which case the default policy is not offered).

For troubleshooting information, see Troubleshooting Service Connectors on page 3775.

**Limits on Service Connector Hub**

See Service Connector Hub Limits on page 231. Logging Limits on page 226 apply when service connectors read from Logging.

See ServiceLimits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

**Managing Service Connectors**

This section describes how to manage service connectors.

A service connector defines the flow of data between a source and target service.

**Prerequisites**

IAM policies: To use Service Connector Hub, you must be given the required type of access in a policy written by an administrator, whether you’re using the Console or the REST API with an SDK, CLI, or other tool.

To move data, you must give your service connector the required authorization to write to the specified target resource in the target service.

A default policy providing the required authorization is offered when you use the Console to define the target service for a service connector. This policy is limited to the context of the service connector. You can either accept this default policy or make sure you have the proper authorizations in a group-based policy.

For more information about service connector authorization, see Write Access to Target Services on page 3752.

If you get a response that you don’t have permission or are unauthorized, check with your administrator. You may need to check the policy for the current compartment. For more information on user authorizations, see Authentication and Authorization on page 3751.

**Using the Console**

**To create a service connector**

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you’re not sure which compartment to use, contact an administrator.
3. Click Create Service Connector.
4. On the **Create Service Connector** page, fill in the settings:
   
   - **Connector Name**: User-friendly name for the new service connector. Avoid entering confidential information.
   - **Description**: Optional identifier.
   - **Resource Compartment**: The compartment where you want to store the new service connector.
   - **Configure Service Connector**:
     
     - **Source**: Select the service containing the data you want to transfer from the following options.
       - **Logging**: Transfer log data from the Logging service. See [Logging Overview](#) on page 2574.
     - **Target**: Select the service that you want to transfer the data to.
       - **Functions**: Send data to a **function**.
       - **Logging Analytics**: Send data to a **log group**.
       - **Monitoring**: Send **metric** data points to the Monitoring service.
       - **Notifications**: Send data to a **topic**.
       - **Object Storage**: Send data to a **bucket**.
       - **Streaming**: Send data to a **stream**.
     - **Configure your source and task**:

   **Note:**

   By default, this page uses Basic mode. To toggle between Basic Mode and Advanced Mode, click **Switch to Advanced mode** (to the right of **Configure source connection**) or **Switch to Basic mode** (to the right of **Configure source and task**). Complex queries cannot be displayed in Basic mode. See [I can't view my query in Basic mode](#).
• Configure source connection:

<table>
<thead>
<tr>
<th>Source service</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Compartment</td>
</tr>
<tr>
<td>See Logging Overview on page 2574.</td>
<td>Log Group</td>
</tr>
<tr>
<td></td>
<td>Logs</td>
</tr>
</tbody>
</table>

• Configure task:

<table>
<thead>
<tr>
<th>Source service</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Audit Logs on page 2617: When _Audit is selected for Log Group:</td>
</tr>
<tr>
<td>See Logging Overview on page 2574.</td>
<td>• When Attribute is selected for Filter Type:</td>
</tr>
<tr>
<td></td>
<td>• Filter Type: Attribute</td>
</tr>
<tr>
<td></td>
<td>• Attribute Name</td>
</tr>
<tr>
<td></td>
<td>• Attribute Values</td>
</tr>
<tr>
<td></td>
<td>• When Event type is selected for Filter Type:</td>
</tr>
<tr>
<td></td>
<td>• Filter Type: Event type</td>
</tr>
<tr>
<td></td>
<td>• Service Name</td>
</tr>
<tr>
<td></td>
<td>• Event Type</td>
</tr>
<tr>
<td>Service Logs on page 2591, Custom Logs on page 2619: When another log group (not _Audit) is selected for Log Group:</td>
<td>• Property</td>
</tr>
<tr>
<td></td>
<td>• Operator</td>
</tr>
<tr>
<td></td>
<td>• Value</td>
</tr>
</tbody>
</table>

• Click Advanced Mode or Switch to Advanced Mode to view and edit the source connector and task using the Query Code Editor.

• Configure target connection: Select the Service Compartment (where the target service resides) and fill in additional fields as needed:
### Target service

<table>
<thead>
<tr>
<th>Additional fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function Application</strong>: Select the name of the function application that includes the function you want.</td>
</tr>
<tr>
<td><strong>Function</strong>: Select the name of the function you want to send the data to.</td>
</tr>
</tbody>
</table>

#### Note:

- Functions are invoked synchronously with 6MB of data per invocation. If data exceeds 6MB, then the service connector invokes the function again to move the over-limit data. Such over-limit invocations are handled sequentially.
- Functions execute for two minutes.
- Do not return data from functions to service connectors. Returned data is not read.

### Logging Analytics

| Log Group: Select the log group you want. |
## Target service
### Monitoring

<table>
<thead>
<tr>
<th>Additional fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Namespace</strong>: Select the <a href="#">metric namespace</a> that includes the metric you want. It can be an existing or new namespace.</td>
</tr>
</tbody>
</table>

**Note:**
When typing a new metric namespace, press ENTER to submit it.

**Metric Name**: Select the name of the [metric](#) that you want to send the data to. It can be an existing or new metric.

The following dimensions are included with your metric:

- **connectorId**: The OCID of the service connector that the metrics apply to.
- **connectorName**: The name of the service connector that the metrics apply to.
- **connectorSourceType**: The source service that the metrics apply to.

The timestamp of each metric data point is the timestamp of the corresponding log message.

## Notifications

<table>
<thead>
<tr>
<th>Additional fields</th>
</tr>
</thead>
</table>
| **Note:**

Log Group for Notifications is limited to _Audit_. |

**Topic**: Select the name of the [topic](#) that you want to send the data to.

**Message Format**: Select the option you want:

- **Send formatted messages**: Simplified, user-friendly layout.

  **Note:**
  To view supported subscription protocols and message types for formatted messages, see [Friendly Formatting](#).

- **Send raw messages**: Raw JSON blob.
Service Connector Hub

<table>
<thead>
<tr>
<th>Target service</th>
<th>Additional fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Storage</td>
<td><strong>Bucket</strong>: Select the name of the bucket that you want to send the data to.</td>
</tr>
</tbody>
</table>

**Note:**
- Batch rollover details:
  - Batch rollover size: 100 MB
  - Batch rollover time: 7 minutes
- Files saved to Object Storage are compressed using gzip.

| Streaming | **Stream**: Select the name of the stream that you want to send the data to. |

- To accept the default policy allowing this service connector to write to the target service, click **Create**. A link is provided for you to view the newly created policy.

You can get that authorization through this default policy or through a group-based policy. The default policy is offered whenever you use the Console to create or edit a service connector (the only exception is when the exact policy already exists in IAM, in which case the default policy is not offered). For more information about this authorization requirement, see **Write Access to Target Services** on page 3752.

**Note:**
- If you don't have permissions to accept the default policy, contact your administrator.

- **Show Advanced Options**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Create**.

Within a few minutes, the service connector begins moving data according to its configuration. The service connector applies tasks to data from the source service and then moves the data to the target service.

**To edit a service connector**

1. Open the navigation menu. Under **Data and AI**, click **Service Connector Hub**.
2. Choose the **Compartment** containing the service connector.
3. Click the name of the service connector you want to edit.
4. Click **Edit**.
5. Make your changes.

**Note:**
- If you did not previously create the default access policy to allow this service connector to write to the target service, you can do so now. You can get that authorization through this default policy or through a group-based policy. The default policy is offered whenever you use the Console to create or edit a service connector (the only exception is when the exact policy already exists in IAM, in which case the default policy is not offered). For more information about this authorization requirement, see **Write Access to Target Services** on page 3752.
6. Click **Save Changes**.

   If you updated the source service or tasks, then data movement may pause for a few minutes, as indicated by **Data Freshness metrics**. Within a few minutes, the service connector begins moving data according to its configuration. The service connector applies tasks to data from the source service and then moves the data to the target service.

**To update your service connector to use friendly message formats**

Friendly message formats are available with service connectors that use Notifications as target.

1. Open the navigation menu. Under **Data and AI**, click **Service Connector Hub**.
2. Choose the **Compartment** containing the service connector.
3. Click the name of the service connector you want to edit.
4. Click **Edit**.
5. Under **Configure target connection**, select the **Message Format** you want:
   - **Send formatted messages**: Simplified, user-friendly layout.
     - **Note**: To view supported subscription protocols and message types for formatted messages, see **Friendly Formatting**.
   - **Send raw messages**: Raw JSON blob.
     - **Note**: If you did not previously create the default access policy to allow this service connector to write to the target service, you can do so now. You can get that authorization through this default policy or through a group-based policy. The default policy is offered whenever you use the Console to create or edit a service connector (the only exception is when the exact policy already exists in IAM, in which case the default policy is not offered). For more information about this authorization requirement, see **Write Access to Target Services** on page 3752.

6. Click **Save Changes**.

   If you updated the source service or tasks, then data movement may pause for a few minutes, as indicated by **Data Freshness metrics**. Within a few minutes, the service connector begins moving data according to its configuration. The service connector applies tasks to data from the source service and then moves the data to the target service.

**To activate a service connector**

1. Open the navigation menu. Under **Data and AI**, click **Service Connector Hub**.
2. Choose the **Compartment** containing the service connector.
3. Click the name of the service connector you want to activate.
4. Click **Activate** and then confirm.

   The service connector immediately begins moving data according to its configuration, applying tasks to data in the source service and then moving the data to the target service.

**To deactivate a service connector**

1. Open the navigation menu. Under **Data and AI**, click **Service Connector Hub**.
2. Choose the **Compartment** containing the service connector.
3. Click the name of the service connector you want to deactivate.
4. Click **Deactivate** and then confirm.

   The service connector stops moving data.
To move a service connector to another compartment

**Note:**

Default policies stop working for moved service connectors. To give a moved service connector the required authorization, edit the service connector using the Console and accept the offered default policy. For more information about service connector authorization, see Write Access to Target Services on page 3752.

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment containing the service connector.
3. Click the name of the service connector you want to edit.
4. Click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.

To delete a service connector

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment containing the service connector.
3. Click the name of the service connector you want to deactivate.
4. Click Delete and then confirm.

The service connector stops moving data.

**Using the Command Line Interface (CLI)**

**To list service connectors**

Open a command prompt and run `oci sch service-connector list` to list service connectors in the specified compartment:

```bash
oci sch service-connector list --compartment-id <compartment_OCID>
```

**To get a service connector**

Open a command prompt and run `oci sch service-connector get` to get the specified service connector:

```bash
oci sch service-connector get --service-connector-id <service_connector_OCID>
```

**To create a service connector**

Open a command prompt and run `oci sch service-connector create` to create a service connector:

```bash
oci sch service-connector create --display-name "<display_name>" --compartment-id <compartment_OCID> --source [<source_in_JSON>] --tasks [<tasks_in_JSON>] --target [<targets_in_JSON>]
```

**To edit a service connector**

Open a command prompt and run `oci sch service-connector update` to edit a service connector:

```bash
oci sch service-connector update --service-connector-id <service_connector_OCID> --display-name "<display_name>" --source [<source_in_JSON>] --tasks [<tasks_in_JSON>] --target [<targets_in_JSON>]
```
To activate a service connector

Open a command prompt and run `oci sch service-connector activate` to activate the specified service connector:

```
oci sch service-connector activate --service-connector-id <service_connector_OCID>
```

To deactivate a service connector

Open a command prompt and run `oci sch service-connector deactivate` to deactivate the specified service connector:

```
oci sch service-connector deactivate --service-connector-id <service_connector_OCID>
```

To move a service connector to another compartment

Open a command prompt and run `oci sch service-connector change-compartment` to move the service connector to the specified compartment:

```
oci sch service-connector change-compartment --service-connector-id <service_connector_OCID> --compartment-id <destination_compartment_OCID>
```

To delete a service connector

Open a command prompt and run `oci sch service-connector delete` to delete the specified service connector:

```
oci sch service-connector delete --service-connector-id <service_connector_OCID>
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage service connectors:

- ActivateServiceConnector
- ChangeServiceConnectorCompartment
- CreateServiceConnector
- DeactivateServiceConnector
- DeleteServiceConnector
- GetServiceConnector
- ListServiceConnectors
- UpdateServiceConnector

Use these API operations to manage work requests:

- GetWorkRequest
- ListWorkRequests
- ListWorkRequestErrors
- ListWorkRequestLogs

Service Connector Hub Scenarios

Here are a few basic scenarios to help you understand the Service Connector Hub service and generally how the components work together.
Scenario: Alarm on Log Data

This topic explains how to set up alarms for log data.

This scenario involves creating a service connector and an alarm. The service connector (Service Connector Hub) processes and moves log data from Logging to Monitoring while the alarm fires when triggered by received log data.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Monitoring and Notifications.

The workflow for creating the service connector includes a default policy when needed to provide permission for writing to the target service.

Setting Up This Scenario

Setup is easy in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

Using the Console

This section walks through creating a service connector and an alarm using the Console and then updating the topic created with the alarm.

Note:

Another workflow for this scenario involves creating your topic and subscriptions first, then selecting this topic when you create your alarm.

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775 and Troubleshooting Notifications on page 3385.

Task 1: Create the service connector

This example walks through using the Console to create a service connector that filters VCN flow log data from Logging for rejected traffic and then moves this log data to a new metric in Monitoring.

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment where you want to create the service connector.
3. Click Create Service Connector.
4. On the **Create Service Connector** page, filter **VCN flow log data** to a new metric:
   - Type a **Connector Name** such as "VCN Flow Log Errors." Avoid entering confidential information.
   - Select the **Resource Compartment** where you want to store the new service connector.
   - Under **Configure Service Connector**, select your source and target services to move log data to a metric:
     - **Select Source:** Logging
     - **Select Target:** Monitoring
   - Under **Configure source connection**, select your **VCN flow log**:
     - **Compartment:** The compartment containing the VCN flow log data.
     - **Log Group:** The log group containing the VCN flow log data.
     - **Logs:** The log object name for your VCN flow logs.
   - Under **Configure task**, filter the log data to rejected traffic:
     - **Property:** data.action
     - **Operator:** =
     - **Value:** REJECT
     - If you are interested in rejected traffic for a particular port or address, add another filter. For example, select the property **data.destinationPort** or **data.destinationAddress**.
   - Under **Configure target connection**, enter the metric namespace and metric name that you want to use for the filtered log data:
     - Select the **Service Compartment** where you want to store the metric data points corresponding to the VCN flow log data for rejected traffic.
     - Enter a new **Namespace:** vcnlogs.
     - **Enter a new Metric Name:** rejectedtraffic
     - [Note:]
       
       When typing a new metric namespace, press ENTER to submit it.

5. If prompted to create a policy (required for access to create or update a service connector), click **Create**.
6. Click **Create**.

**Task 2: Create the alarm**

This example walks through using the Console to create an alarm that sends a message when Monitoring receives metric data points corresponding to VCN flow log data for rejected traffic. During this process, you'll create a topic and an email subscription.

1. Open the navigation menu. Under **Solutions and Platform**, go to **Monitoring** and click **Alarm Definitions**.
2. Click **Create alarm**.
3. On the **Create Alarm** page, under **Define alarm**, set up your threshold:
   - **Metric description:**
     - **Compartment:** (select the **compartment** specified in the previous task, where you are storing the metric data points corresponding to the VCN flow log data)
     - **Metric Namespace:** (enter the metric namespace that you specified in the service connector)
     - **Metric Name:** (enter the metric name that you specified in the service connector)
     - **Interval:** 1m
     - **Statistic:** Count
   - **Trigger rule:**
     - **Operator:** greater than
     - **Value:** 0
     - **Trigger Delay Minutes:** 1
4. Under Notifications, Destinations, set up an email notification:
   - Destination Service: Notifications Service
   - Compartment: (select the compartment where you want to create the topic and associated subscriptions)
   - Topic: Click Create a topic
     
     | Note: |
     |-------|
     | If you already created your topic and email subscription, you can select that topic here instead of creating a new one. |
   
   - Topic Name: Rejected Traffic Topic
   - Subscription Protocol: Email
   - Email Addresses: (type your email address here)
5. Click Save alarm.

Using the CLI

This section walks through creating the service connector, topic, subscriptions, and alarm using the CLI.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

1. Create a service connector: Open a command prompt and run the `oci sch service-connector create` command:

   ```bash
   oci sch service-connector create --display-name "<display_name>" --compartment-id <compartment_OCID> --source [<source_in_JSON>] --tasks [<tasks_in_JSON>] --target [<targets_in_JSON>]
   ```

2. Create a topic: Open a command prompt and run the `oci ons topic create` command:

   ```bash
   oci ons topic create --name "Alarm Topic" --compartment-id "<compartment_ocid>"
   ```

3. To this topic, add a subscription referencing your email address. Open a command prompt and run the `oci ons subscription create` command:

   ```bash
   oci ons subscription create --compartment-id "<compartment-ocid>" --topic-id "<topic-ocid>" --protocol "EMAIL" --subscription-endpoint "john.smith@example.com"
   ```

4. Create an alarm that defines the error threshold and references this topic as the destination: Open a command prompt and run the `oci monitoring alarm create` command:

   ```bash
   oci monitoring alarm create --display-name "My Alarm" --compartment-id "<compartment-ocid>" --metric-compartment-id "<compartment-ocid>" --namespace "oci_computeagent" --query-text "<yourmetric>[1m].count() > 0" --severity "INFO" --destinations "<topic-ocid>" --is-enabled true
   ```

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775 and Troubleshooting Notifications on page 3385.

Using the API

This section walks through creating the service connector, topic, subscription, and alarm using the API.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:
1. **CreateServiceConnector**: Create a service connector.

   **Example CreateServiceConnector request**

   ```
   POST /20200909/serviceConnectors
   Host: service-connector-hub.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
       "compartmentId": "<compartment_OCID>",
       "description": "My service connector description",
       "displayName": "My Service Connector",
       "source": {
           "kind": "logging",
           "logSources": [
               {
                   "compartmentId": "<compartment_OCID>",
                   "logGroupId": "<log_group_OCID>",
                   "logId": "<log_OCID>"
               }
           ],
           "target": {
               "compartmentId": "<compartment_OCID>",
               "kind": "metrics",
               "metric": "<yourmetric>",
               "metricNamespace": "<yournamespace>"
           },
           "tasks": [
               {
                   "condition": "data.action='REJECT'",
                   "kind": "logRule"
               }
           ]
       }
   }
   ```

2. **CreateTopic**: Create a topic.

   **Example CreateTopic request**

   ```
   POST /20181201/topics
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
       "name": "Alarm Topic",
       "compartmentId": "<compartment_OCID>"
   }
   ```

3. **CreateSubscription**: To this topic, add a subscription referencing your email address.

   **Example CreateSubscription request: Email**

   ```
   POST /20181201/subscriptions
   Host: notification.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {
       "topicId": "<topic_OCID>",
       "compartmentId": "<compartment_OCID>",
       "protocol": "EMAIL",
       "endpoint": "john.smith@example.com"
   }
   ```
4. **CreateAlarm**: Create an alarm that defines the memory threshold and references this topic.

**Example CreateAlarm request**

```
POST /20180401/alarms
Host: telemetry.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
    "displayName": "My Alarm",
    "compartmentId": "<compartment OCID>",
    "metricCompartmentId": "<compartment OCID>",
    "namespace": "<yournamespace>",
    "query": "<yourmetric>[1m].count() > 0",
    "severity": "INFO",
    "destinations":
        [
            "<topic OCID>"
        ],
    "isEnabled": true
}
```

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775 and Troubleshooting Notifications on page 3385.

**Scenario: Send Log Data to an Autonomous Database**

This topic explains how to send log data from Logging to an Autonomous Database using a function (Functions service).

This scenario involves creating a function and then referencing that function in a service connector (Service Connector Hub) to process and move log data from Logging to an Autonomous Database.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you're a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Functions.

The workflow for creating the service connector includes a default policy when needed to provide permission for writing to the target service.

**Setting Up This Scenario**

This scenario involves creating a service connector (Service Connector Hub) to send log data from Logging to an Autonomous Database (JSON).

Before you can create the service connector, you must set up an Autonomous JSON Database that you want to receive the log data and set up the function to copy that log data.

Autonomous JSON Database setup details:

- **Create the Autonomous JSON Database**
- Copy the ORDS base URL: From the detail page for the Autonomous Database, click Service Console, click Development, and then click Copy URL under RESTful Services and SODA.
• Create a "logs" collection to store the log data that will be moved by the function and service connector:

1. Go to the detail page for the Autonomous Database.
2. Click Tools and then click Open SQL Developer Web.
3. Log in with the admin user and the password you set when you created the database.
4. In SQL Developer Web, enter the following command:

   soda create logs

5. Click Run Statement.

To query documents in the collection after the service connector copies log data, enter the following command:

   soda get logs -f {}

Function setup details:

• Create the function
• Deploy the function
• Set the configuration values as follows:

  • ordsbaseurl
    Use the ORDS base URL you copied during setup of the database.
  • dbschema
  • dbuser
  • dbpwd
  • collection

  For more information, see Passing Custom Configuration Parameters to Functions on page 2085.

• (Optional) Invoke the function

Once the database and function are set up, you're ready to create the service connector. Creating the service connector is easy in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

Function code sample

The following code sample is for a function to send log data from the Logging service to an Autonomous Database. For instructions on creating and deploying functions, see Creating and Deploying Functions on page 2063.

Note:
The following code sample is not meant for production workloads. Update it for your production environment.

```python
import io
import json
import logging
import requests
from fdk import response

# soda_insert uses the Autonomous Database REST API to insert JSON documents
def soda_insert(ordsbaseurl, dbschema, dbuser, dbpwd, collection, logentries):
    auth=(dbuser, dbpwd)
    sodaurl = ordsbaseurl + dbschema + '/soda/latest/
    bulkinserturl = sodaurl + 'custom-actions/insert/' + collection + "/"
    headers = {'Content-Type': 'application/json'}
    resp = requests.post(bulkinserturl, auth=auth, headers=headers, data=json.dumps(logentries))
    return resp.json()
```
def handler(ctx, data: io.BytesIO=None):
    logger = logging.getLogger()
    logger.info("function start")

    # Retrieving the Function configuration values
    try:
        cfg = dict(ctx.Config())
        ordsbaseurl = cfg["ordsbaseurl"]
        dbschema = cfg["dbschema"]
        dbuser = cfg["dbuser"]
        dbpwd = cfg["dbpwd"]
        collection = cfg["collection"]
    except:
        logger.error('Missing configuration keys: ordsbaseurl, dbschema, dbuser, dbpwd and collection')
        raise

    # Retrieving the log entries from Service Connector Hub as part of the Function payload
    try:
        logentries = json.loads(data.getvalue())
        if not isinstance(logentries, list):
            raise ValueError
    except:
        logger.error('Invalid payload')
        raise

    # The log entries are in a list of dictionaries. We can iterate over the list of entries and process them.
    # For example, we are going to put the Id of the log entries in the function execution log
    logger.info("Processing the following LogIds:")
    for logentry in logentries:
        logger.info(logentry["oracle"]["logid"])

    # Now, we are inserting the log entries in the JSON Database
    resp = soda_insert(ordsbaseurl, dbschema, dbuser, dbpwd, collection, logentries)
    logger.info(resp)
    if "items" in resp:
        logger.info("Logs are successfully inserted")
        logger.info(json.dumps(resp))
    else:
        raise Exception("Error while inserting logs into the database: " + json.dumps(resp))

    # The function is done, we don't return any response because it would be useless
    logger.info("function end")
    return response.Response(ctx,
                            response_data="",
                            headers={"Content-Type": "application/json"})

Using the Console
This section walks through creating a service connector using the Console. Your function must be deployed.

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775.
Create a service connector

This example walks through using the Console to create a service connector. In this example, the service connector moves log data from Logging to an Autonomous Database using the function you created using the function code sample.

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment where you want to create the service connector.
3. Click Create Service Connector.
4. On the Create Service Connector page:
   - Type a Connector Name such as "Send Logs to My Autonomous Database." Avoid entering confidential information.
   - Select the Resource Compartment where you want to store the new service connector.
   - Under Configure Service Connector, select your source and target services to move log data to a metric:
     - Select Source: Logging
     - Select Target: Functions
   - Under Configure source connection, select a Compartment Name, Log Group, and Log.
   - Under Configure target connection, select the Function Application and Function corresponding to the function you created using the function code sample.
5. If prompted to create a policy (required for access to create or update a service connector), click Create.
6. Click Create.

Using the CLI

This section walks through creating a service connector using the CLI that moves log data to your function (which then moves the data to an Autonomous Database).

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- Create a service connector: Open a command prompt and run the `oci sch service-connector create` command:

```
oci sch service-connector create --display-name "<display_name>" --compartment-id <compartment_OCID> --source [<source_in_JSON>] --tasks [<tasks_in_JSON>] --target [<targets_in_JSON>]
```

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775.

Using the API

This section walks through creating the service connector using the API.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:
- CreateServiceConnector: Create a service connector that moves log data to your function (which then moves the data to an Autonomous Database).

Example CreateServiceConnector request

```
POST /20200909/serviceConnectors
Host: service-connector-hub.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
  "compartmentId": "<compartment_OCID>",
  "description": "My service connector description",
  "displayName": "My Service Connector",
  "source": {
```
Scenario: Archive Logs to Object Storage

This topic explains how to archive log data to a bucket in Object Storage.

This scenario involves creating a service connector. The service connector processes and moves log data from Logging to Object Storage.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Monitoring, Notifications, and Object Storage.

The workflow for creating the service connector includes a default policy when needed to provide permission for writing to the target service.

Setting Up This Scenario

Setup is easy in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

Using the Console

This example walks through using the Console to create a service connector that receives subnet log data from Logging and then moves this data to a bucket in Object Storage.

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775.

Create the service connector

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment where you want to create the service connector.
3. Click Create Service Connector.
4. On the **Create Service Connector** page, send subnet log data to a bucket:
   - Type a **Connector Name**, such as "Archive Logs." Avoid entering confidential information.
   - Select the **Resource Compartment** where you want to store the new service connector.
   - Under **Configure Service Connector**, select your source and target services to move log data to a metric:
     - **Select Source**: Logging
     - **Select Target**: Object Storage
   - Under **Configure source connection**, select your subnet log:
     - **Compartment**: The compartment containing the log data you want.
     - **Log Group**: The log group containing the log data you want.
     - **Logs**: The log object name for the log data you want.
   - Under **Configure target connection**, select the bucket where you want to archive this log data:
     - **Select the Service Compartment** where you want to store the received (filtered) log data.
     - **Select the Bucket** you want.

5. If prompted to create a policy (required for access to create or update a service connector), click **Create**.
6. Click **Create**.

**Using the CLI**

This example walks through using the CLI to create a service connector that receives subnet log data from Logging and then moves this data to a bucket in Object Storage.

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

- **Create a service connector**: Open a command prompt and run the `oci sch service-connector create` command:

```bash
oci sch service-connector create --display-name "<display_name>" --compartment-id <compartment_OCID> --source ["<source_in_JSON>"] --target ["<targets_in_JSON>"]
```

For help with troubleshooting, see [Troubleshooting Service Connectors](#) on page 3775.

**Using the API**

This example walks through using the API to create a service connector that receives subnet log data from Logging and then moves this data to a bucket in Object Storage.

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use the following operations:

- **CreateServiceConnector**: Create a service connector.

**Example CreateServiceConnector request**

```
POST /20200909/serviceConnectors
Host: service-connector-hub.us-phoenix-1.oraclecloud.com
<authorization and other headers>
{
    "compartmentId": "<compartment_OCID>",
    "description": "My service connector description",
    "displayName": "My Service Connector",
    "source": {
        "kind": "logging",
        "logSources": [
            {
                "compartmentId": "<compartment_OCID>",
                "logGroupId": "<log_group_OCID>"
            }
        ]
    },
    "target": {
        "serviceCompartment": "<service_compartment_OCID>",
        "bucket": "<bucket_name>",
        "isPublic": false
    }
}
```
Scenario: Analyze Logs

This topic explains how to send log data to Logging Analytics.

This scenario involves creating a log group and a service connector. The service connector (Service Connector Hub) processes and moves log data from Logging to the log group in Logging Analytics.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

If you’re a member of the Administrators group, you already have the required access to execute this scenario. Otherwise, you need access to Logging Analytics to create the log group and access to Service Connector Hub to create the service connector.

The workflow for creating the service connector includes a default policy when needed to provide permission for writing to the target service.

Setting Up This Scenario

Setup is easy in the Console. Alternatively, you can use the Oracle Cloud Infrastructure CLI or API, which lets you execute the individual operations yourself.

Using the Console

This section walks through creating a log group and a service connector using the Console.

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775.

Task 1: Create the log group

Use Logging Analytics to create the log group. For instructions, see Create Log Groups.

Task 2: Create the service connector

This example walks through using the Console to create a service connector that sends log data from Logging to the log group you created using Logging Analytics. In this example, the service connector filters VCN flow log data.

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment where you want to create the service connector.
3. Click Create Service Connector.
4. On the Create Service Connector page, filter VCN flow log data to your log group:
   - Type a Connector Name such as "VCN Flow Log Error Analysis."
   - Select the Resource Compartment where you want to store the new service connector.
   - Under Configure Service Connector, select your source and target services to move log data to the log group:
     - Select Source: Logging
     - Select Target: Logging Analytics
   - Under Configure source connection, select your VCN flow log:
     - Compartment: The compartment containing the VCN flow log data.
     - Log Group: The log group containing the VCN flow log data.
     - Logs: The log object name for your VCN flow logs.
   - Under Configure task, filter the log data to rejected traffic:
     - Property: data.action
     - Operator: =
     - Value: REJECT
     If you are interested in rejected traffic for a particular port or address, add another filter. For example, select the property data.destinationPort or data.destinationAddress.
   - Under Configure target connection, enter the log group that you want to send the filtered log data to:
     - Select the Service Compartment containing the log group.
     - Select the Logging Analytics Log Group (the log group you created).
5. If prompted to create a policy (required for access to create or update a service connector), click Create.
6. Click Create.

Using the CLI

This section walks through creating the log group and service connector using the CLI.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

1. Create a log group: Open a command prompt and run the `oci log-analytics log-group create` command:

   ```bash
   oci log-analytics log-group create --display-name "<display_name>" --compartment-id <compartment_OCID> --namespace-name "<namespace_name>"
   ```

2. Create a service connector: Open a command prompt and run the `oci sch service-connector create` command:

   ```bash
   oci sch service-connector create --display-name "<display_name>" --compartment-id <compartment_OCID> --source [<source_in_JSON>] --tasks [<tasks_in_JSON>] --target [<targets_in_JSON>]
   ```

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775 and Troubleshooting Notifications on page 3385.

Using the API

This section walks through creating the log group and service connector using the API.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations:
1. **CreateLogAnalyticsLogGroup**: Create a log group.

   **Example CreateLogAnalyticsLogGroup request**

   ```
   post /20200601/namespaces/<namespaceName>/logAnalyticsLogGroups
   Host: loganalytics.us-phoenix-1.oci.oraclecloud.com
   <authorization and other headers>
   {  
       "compartmentId": "<compartment_OCID>",
       "displayName": "My Log Group"
   }
   ```

2. **CreateServiceConnector**: Create a service connector.

   **Example CreateServiceConnector request**

   ```
   POST /20200909/serviceConnectors
   Host: service-connector-hub.us-phoenix-1.oraclecloud.com
   <authorization and other headers>
   {  
       "compartmentId": "<compartment_OCID>",
       "description": "My service connector description",
       "displayName": "My Service Connector",
       "source": {  
           "kind": "logging",
           "logSources": [  
               {  
                   "compartmentId": "<compartment_OCID>",
                   "logGroupId": "<log_group_OCID>",
                   "logId": "<log_OCID>"
               }
           ],
           "target": {  
               "compartmentId": "<compartment_OCID>",
               "kind": "loggingAnalytics",
               "logGroupId": "<logging_analytics_log_group_OCID>"
           },
           "tasks": [  
               {  
                   "condition": "data.action='REJECT'",
                   "kind": "logRule"
               }
           ]
       }
   }
   ```

For help with troubleshooting, see Troubleshooting Service Connectors on page 3775 and Troubleshooting Notifications on page 3385.

**Troubleshooting Service Connectors**

This topic covers troubleshooting techniques for Service Connector Hub.

**No data is being moved**

This section provides troubleshooting information for service connectors that don't appear to be moving data. For example service connectors, see Service Connector Hub Scenarios on page 3762.

Check these items:
• **Error metrics**: Determine if errors exist at the source service, target service or Service Connector Hub service.

**To view error metrics for a service connector**

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the **Compartment** that contains the service connector you want to view, and then click the service connector's name.
3. In the Resources menu, click Metrics (if necessary).
   
   The Metrics page displays a default set of charts for the current service connector.
4. Review the following metric charts:
   - Errors at Source
   - Errors at Target
   - Service Connector Hub Errors

**Authorization to write to the target service**: Make sure you have authorization, either through the default policy offered when creating or updating the service connector or through a group-based policy. See Write Access to Target Services on page 3752.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your accepted default policy may take a few minutes to propagate to regions that are not your home region. The service connector does not move data until the policy is propagated.</td>
</tr>
</tbody>
</table>

**I can’t view my query in Basic mode**

Check these items:

• **Query simplicity**: Update the query so that it only includes elements supported in Basic mode:
  
  • **Audit logs only**: Type-based filters can use the OR operator. Other filters must use the AND operator.
    
    Example:
    
    ```
    ((type = value1 OR type = value2) AND field = value3 AND field1 = value4)
    ```
  
  • **Any combination of logs (Service logs, custom logs, and Audit logs)**: Filters joined with the AND operator.
    
    Example:
    
    ```
    (field = value AND field1 != value1)
    ```

Examples of query complexity that are not supported in Basic mode:

• OR operator (except with type-based filters when only Audit logs are used)
• Functions (for example: `isNull()`)
• `select`
• `summarize`

**How do I know when issues occur?**

Check these items:
• **Data freshness**: Look for unexpected lapses of time between data movement.

**To view data freshness for a service connector**

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment that contains the service connector you want to view, and then click the service connector's name.
3. In the Resources menu, click Metrics (if necessary).
   
   The Metrics page displays a default set of charts for the current service connector.
4. Review the following metric charts:
   
   • Data Freshness

**To view data freshness for all service connectors in the tenancy**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Metric Namespace, select oci_service_connector_hub.
3. Review the following metric charts:
   
   • Data Freshness

### Viewing the State of a Work Request

This topic describes how to view the state of work requests associated with a given service connector.

**Note:**

The Service Connector Hub service does not use the common Work Requests API to support work request operations. Instead, Service Connector Hub work requests are supported by the Service Connector Hub API. See Using the Console to View Work Requests on page 260 for information on viewing work requests for other services.

### Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

### Monitoring Work Requests

Many of the Service Connector Hub service requests do not take effect immediately. In these cases, the request spawns an asynchronous workflow for fulfillment. To provide visibility for in-progress workflows, the Service Connector Hub service creates a work request object.

The work request states are:

**ACCEPTED**

The request is in the work request queue to be processed.

**IN_PROGRESS**

A work request record exists for the specified request, but there is no associated WORK_COMPLETED record.

**SUCCEEDED**

A work request record exists for this request and an associated WORK_COMPLETED record has the state SUCCEEDED.
FAILED
A work request record exists for this request and an associated WORK_COMPLETED record has the state FAILED.

CANCELING
The work request is in the process of canceling.

CANCELED
The work request has been canceled.

Using the API
For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these operations to monitor the state of work requests:

- GetWorkRequest
- ListWorkRequests
- ListWorkRequestErrors
- ListWorkRequestLogs

Example Messages
This topic shows examples of messages sent by service connectors that use Notifications as target.

A service connector with a Notifications target sends messages to all subscriptions for the specified topic. The contents and appearance of each message depends on the subscription protocol, such as Email.

For friendly formatting of email messages, select Formatted for the service connector's message format.

Email (Raw) and Slack

Text
{"data":
}
You are receiving notifications as a subscriber to the topic: sch_integ_test_topic_email (Topic OCID: ocid1.onstopic.oc1.ap-chuncheon-1.exampleid). To stop receiving notifications from this topic, unsubscribe.

Please do not reply directly to this email. If you have any questions or comments regarding this email, contact your account administrator.
Service Connector Hub Metrics

You can monitor the health, capacity, and performance of your service connectors by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the Service Connector Hub service in the oci_service_connector_hub metric namespace.

Resources: Service connectors.

Overview of the Service Connector Hub Service Metrics

The Service Connector Hub service metrics help you measure the number and type of connections between services in Oracle Cloud Infrastructure. You can use metrics data to diagnose and troubleshoot service connector issues.

To view a default set of metrics charts in the Console, navigate to the service connector you're interested in, and then click Metrics. You also can use the Monitoring service to create custom queries.
**Prerequisites**

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

Administrators: For common policies that give groups access to Service Connector Hub, see Allow a group to manage service connectors on page 2160.

**Available Metrics: oci_service_connector_hub**

The metrics listed in the following tables are automatically available for any service connectors you create. You do not need to enable monitoring on the resource to get these metrics.

Service Connector Hub service metrics include the following dimensions:

- **connectorId**
  
  The OCID of the service connector that the metrics apply to.

- **connectorName**
  
  The name of the service connector that the metrics apply to.

- **errorType**
  
  The type of error.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For information about common errors, see API Errors on page 4372.</td>
</tr>
</tbody>
</table>

- **region**
  
  The region that the metrics apply to.

- **sourceName**
  
  The name of the source service that the metrics apply to.

- **targetName**
  
  The name of the target service that the metrics apply to.
<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BytesReadFromSource</td>
<td>Bytes Read from Source</td>
<td>Bytes</td>
<td>Number of bytes read from the source</td>
<td>connectorId, connectorName, region, sourceName</td>
</tr>
</tbody>
</table>

**Note:**

- The value for this metric is cumulative. For example, when a service connector reads 1MB from the source, the service connector emits a `BytesReadFromSource` metric with a value of 1MB. However, let's say that the service connector is unable to write to the target. The next time the service connector reads (1MB) from the source, it will emit a `BytesReadFromSource` metric with a cumulative value of 2MB, which includes the 1MB from the first read. Let's say the service connector successfully writes to the target. The third time the service connector reads (1MB) from the source, it will emit the `BytesReadFromSource` metric with a cumulative value of 1MB.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BytesWrittenToTarget</td>
<td>Bytes Written to Target</td>
<td>Bytes</td>
<td>Number of bytes written to the target</td>
<td>connectorId, connectorName, region, targetName</td>
</tr>
</tbody>
</table>

**Note:**

Use this metric as a general indicator of success. BytesWrittenToTarget may not match BytesReadFromSource for data read from Logging to the following target services.

- Monitoring may translate multiple records into a single metric data point.
- Object Storage compresses data. For example, 10MB read may be converted into 1MB written.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataFreshness</td>
<td>Data Freshness</td>
<td>Milliseconds</td>
<td>Indicates age of the oldest processed record of the most recent set</td>
<td>connectorId&lt;br&gt;connectorName&lt;br&gt;region&lt;br&gt;sourceName&lt;br&gt;targetName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example, let's say you check this metric at 10:30. At 10:00, you received your last set of records at 10:00. Of the five records, three have a 10:00 timestamp while two have a 9:55 timestamp. In this example, the most recent set was received at 10:00; the oldest processed record had a 9:55 timestamp. At 10:35, the age is 35 minutes.</td>
<td></td>
</tr>
<tr>
<td>ErrorsAtSource</td>
<td>Errors at Source</td>
<td>Count</td>
<td>Number of errors that affect retrieving data from source</td>
<td>connectorId&lt;br&gt;connectorName&lt;br&gt;errorType&lt;br&gt;region&lt;br&gt;sourceName</td>
</tr>
<tr>
<td>ErrorsAtTarget</td>
<td>Errors at Target</td>
<td>Count</td>
<td>Number of errors that affect writing data to target</td>
<td>connectorId&lt;br&gt;connectorName&lt;br&gt;errorType&lt;br&gt;region&lt;br&gt;sourceName</td>
</tr>
<tr>
<td>LatencyAtSource</td>
<td>Latency at Source</td>
<td>Milliseconds</td>
<td>Time-to-first-byte when retrieving data from source. Useful for customers to troubleshoot with complex tasks (log rules).</td>
<td>connectorId&lt;br&gt;connectorName&lt;br&gt;region&lt;br&gt;sourceName</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>----------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>LatencyAtTarget</td>
<td>Latency at Target</td>
<td>Milliseconds</td>
<td>Time-to-first-byte when writing data to target</td>
<td>connectorId, connectorName, region, targetName</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>MessagesReadFromSource</td>
<td>Messages Read from Source</td>
<td>Count</td>
<td>Number of records read from the source</td>
<td>connectorId, connectorName, region, sourceName</td>
</tr>
</tbody>
</table>

**Note:**
The value for this metric is cumulative. For example, when a service connector reads a single message from the source, the service connector emits a `MessagesReadFromSource` metric with a value of 1. However, let's say that the service connector is unable to write to the target. The next time the service connector reads (1 message) from the source, it will emit a `MessagesReadFromSource` metric with a cumulative value of 2, which includes the message from the first read. Let's say the service connector successfully writes to...
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessagesWrittenToTarget</td>
<td>Messages Written to Target</td>
<td>Count</td>
<td>Number of records written to the target</td>
<td>connectorId, connectorName, region, targetName</td>
</tr>
</tbody>
</table>

**Note:**
- Use this metric as a general indicator of success.
- `MessagesWrittenToTarget` may not match `MessagesReadFromSource` for messages read from Logging to the following target services:
  - Monitoring may translate multiple records into a single metric data point.
  - Object Storage compresses data. For example, 10MB read may be converted into 1MB written.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceConnectorHubErrors</td>
<td>Service Connector Hub Errors</td>
<td>Count</td>
<td>Number of errors in Service Connector Hub that affect moving data from source to target</td>
<td>connectorId, connectorName, region</td>
</tr>
</tbody>
</table>
Using the Console
To view default metric charts for a single service connector

1. Open the navigation menu. Under Data and AI, click Service Connector Hub.
2. Choose the Compartment that contains the service connector you want to view, and then click the service connector's name.
3. In the Resources menu, click Metrics (if necessary).

The Metrics page displays a default set of charts for the current service connector.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for multiple service connectors

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Metric Namespace, select oci_service_connector_hub.

The Service Metrics page displays a default set of charts for the selected metric namespace. For more information about the emitted metrics, see the foregoing table. You can also use the Monitoringservice to create custom queries.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

Using the API
Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Query Reference for Service Connector Hub
Service Connector Hub supports a subset of the Logging Query Language Specification on page 2639.

Stream expressions are limited to following streaming operators:

- search

  Constructs a log stream from actual log objects.

  Example:

  ```
  search "<compartment_OCID>/loggroup1/logname1" "<compartment_OCID>/loggroup2/logname2" "<compartment_OCID>/loggroup3/logname3"
  ```

- where

  Filters the current log stream using a Boolean expression.

  Example 1:

  ```
  search "<compartment_OCID>/Audit" 
  | where type = 'com.oraclecloud.objectstorage.deleteobject'
  output: 
  {"specversion": "1.0", "type": 
   "com.oraclecloud.objectstorage.deleteobject", "source": 
   "<compartment_OCID>/myBucket",......}
  ```

  Example 2: Complex Boolean expression:

  ```
  search "<compartment_OCID>/Audit" 
  | where type = 'com.oraclecloud.objectstorage.deleteobject' or '
  'com.oraclecloud.objectstorage.getobject'
  ```
| where source = 'myBucket'
output:
{"specversion": "1.0", "type": "com.oraclecloud.objectstorage.deleteobject", "source": "<compartment_OCID>/myBucket"},.....
{"specversion": "1.0", "type": "com.oraclecloud.objectstorage.getobject", "source": "<compartment_OCID>/myBucket"},.....

Example 3: search without where:

search "<compartment_OCID>/application" | level = 'ERROR'

Example 4: Full text search. You can perform a full text search by specifying a filter on the entire content of the log. A search on logContent returns any log line where a value matches your string. This functionality supports wildcards:

search "<compartment_OCID>/application"
| where logContent = 'ERROR'  -- returns log lines with a value matching "ERROR"

search "<compartment_OCID>/application"
| where logContent = '*ERROR*'  -- returns log lines with a value containing "ERROR"

Functions are limited to scalar functions.
Chapter 36

Storage Gateway

This chapter explains how to use Storage Gateway to connect your on-premise applications with Oracle Cloud Infrastructure.

Overview of Storage Gateway

Storage Gateway is a cloud storage gateway that lets you connect your on-premises applications with Oracle Cloud Infrastructure. Applications that can write data to an NFS target can also write data to the Oracle Cloud Infrastructure Object Storage, without requiring application modification to uptake the REST APIs.

Important:

Storage Gateway is the evolution of the Storage Software Appliance that was launched with Oracle Cloud Infrastructure Classic. By migrating to Oracle Cloud Infrastructure Object Storage, you are using Storage Gateway with its enhanced file-to-object transparency and improved scale and performance.

Availability

The Storage Gateway service is available in all Oracle Cloud Infrastructure commercial regions. See About Regions and Availability Domains for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

Storage Gateway and Oracle Cloud Infrastructure Concepts

The following concepts are essential to working with Oracle Cloud Infrastructure Storage Gateway.

FILE SYSTEM

A Storage Gateway file system on a local host maps its files and directories to objects with the same names in a corresponding Oracle Cloud Infrastructure Object Storage bucket.

FILE SYSTEM CACHE

Storage Gateway's configurable file system cache enables asynchronous and optimized movement of data to the cloud. The file system cache serves as both a write buffer and a read cache for data storage and retrieval. The write buffer contains data that copied to the disk cache and queued for upload to Oracle Cloud Infrastructure. The read cache contains frequently retrieved data that’s accessible locally for read operations. Proper file system cache configuration is critical to Storage Gateway performance. See Configuring the Cache for File Systems on page 3797 for details.

METADATA

The metadata associated with a Storage Gateway file is stored as custom metadata for the corresponding object in Oracle Cloud Infrastructure Object Storage. Examples of file metadata include object id, creation date, modification date, size, and permissions. Storage Gateway caches all metadata for the file system locally.
NFSV4
NFS is an established and widely adopted distributed file system protocol for handling network storage. NFS lets client computers mount file systems on remote servers and access those remote file systems over the network as though they were local file systems. Storage Gateway performs the NFS to REST API translation needed to interact with Oracle Cloud Infrastructure Object Storage.

ORACLE CLOUD INFRASTRUCTURE
Oracle Cloud Infrastructure is a set of complementary cloud services that lets you build and run a wide range of applications and services in a highly available hosted environment. Oracle Cloud Infrastructure offers high-performance compute capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network.

TENANCY
A tenancy is a secure and isolated partition within Oracle Cloud Infrastructure where you can create, organize, and administer your cloud resources.

OBJECT STORAGE AND ARCHIVE STORAGE
Oracle Cloud Infrastructure offers two distinct storage tiers for you to store your unstructured data. Use the Object Storage Standard tier for data to which you need fast, immediate, and frequent access. Use the Archive Storage service’s Archive tier for data that you access infrequently, but which must be preserved for long periods of time. Both storage tiers use the same manageable resources (for example, objects and buckets). The difference is that when you upload a file to Archive Storage, the object is immediately archived. Before you can access an archived object, you must first restore the object to the Standard tier.

Note:
In the Storage Gateway documentation, generic references to Object Storage encompass both the Standard and Archive storage tiers.

Both storage tiers are simple to use, perform well, and scale to an unlimited capacity.

bucket
An Object Storage bucket is a logical container for storing objects. A file system created in Storage Gateway maps to a corresponding bucket by the same name in Object Storage. A bucket is associated with a single Oracle Cloud Infrastructure compartment. The compartment has policies that determine what actions a user can perform on the bucket the objects it contains.

object
An individual file or directory written to a Storage Gateway file system on an NFS share creates an identically named object in the target Object Storage bucket. An object is composed of the object itself and metadata about the object.

NAMESPACE
A logical entity that serves as a top-level container for all Oracle Cloud Infrastructure Object Storage buckets and objects. The namespace enables you to control bucket naming within your tenancy. Each tenancy has one unique and uneditable Object Storage namespace that is global, spanning all compartments and regions. Bucket names must be unique within your tenancy.

COMPARTMENT
A collection of Oracle Cloud Infrastructure-related resources. Only users and groups with access permissions explicitly granted by an administrator can access the resources. Compartments help you organize resources and make it easier to control access to those resources. Oracle Cloud Infrastructure automatically creates a root compartment when a tenancy is provisioned. An administrator can then create more compartments within the root compartment and add access rules for those compartments. A bucket can exist in only one compartment.
How Storage Gateway Works

Storage Gateway is installed in an Oracle Cloud Infrastructure compute instance or as a Linux Docker instance on one or more hosts in your on-premises data center. Applications store and retrieve objects from Oracle Cloud Infrastructure Object Storage through file systems that you create in Storage Gateway.

Storage Gateway exposes an NFS mount point that can be mounted to any host that supports an NFSv4 client. The Storage Gateway mount point maps to an Object Storage bucket.

There is file-to-object transparency between Storage Gateway and Object Storage:

- A Storage Gateway file system directory on a local host maps to a bucket with an identical name in Oracle Cloud Infrastructure Object Storage.
- Any file written to a Storage Gateway file system is written as an object with the same name in the associated Object Storage bucket. The system stores associated file attributes as object metadata.
- You can access Object Storage objects directly using native APIs, SDKs, third-party tools, the HDFS connector, and the Oracle Cloud Infrastructure CLI and Console. You use the Refresh operation in Storage Gateway to ingest any data that was added or modified directly in Object Storage.

Enterprise applications typically work with files in nested directories. Object Storage buckets, and the objects within those buckets, exist in a flat hierarchy. Storage Gateway flattens the directory hierarchy into nested object prefixes in Object Storage. See Interacting With Object Storage on page 3805 for details.

Recommended Uses and Workloads

The following summarizes some of the ways that you can use Storage Gateway.

DATA TRANSFER

Use Storage Gateway to move data from your on-premises host to Oracle Cloud Infrastructure. Storage Gateway is not a replacement for general-purpose network attached storage (NAS), though it behaves similarly to NAS. Use Storage Gateway’s integrated Cloud Sync feature to transfer and synchronize data to Oracle Cloud Infrastructure.

CLOUD TIERING

Use Storage Gateway to expand the capacity of on-premises storage solutions without capital expenditures. Configuring and connecting a Storage Gateway file system with a large cache to Oracle Cloud Infrastructure Object Storage provides unlimited scale to create a workflow in which files get automatically moved to the cloud and retrieved only on demand. Even though on-demand retrieval is slower than access to local storage, capital expenditures or changes to existing tools and software are not required.

BACKUPS

Use Storage Gateway to move files to Oracle Cloud Infrastructure Archive Storage as a cost-effective backup solution. You can move individual files and compressed or uncompressed ZIP or TAR archives. Storing secondary copies of data is an ideal use case for Storage Gateway.

ARCHIVAL

Storage Gateway is ideal for archive use cases.

DISASTER RECOVERY

Storage Gateway lets traditional applications move data to highly durable object storage. When you need to recover data, create a fresh instance of Storage Gateway to return the data from Object Storage.

Uses and Workloads Not Supported

Storage Gateway does not support the following uses and workloads.

WINDOWS OPERATING SYSTEM

Storage Gateway does not currently support the Windows operating environment or Windows solutions.
GENERAL-PURPOSE NETWORK STORAGE

Storage Gateway isn't a general-purpose storage filer and must not be used as a replacement for traditional network storage appliances.

FILE SYNC AND SHARE

Though Storage Gateway is an effective data mover, it’s not a replacement for file sync and share services. Evaluate Oracle services like Oracle Document Cloud service if you need file sync and share functionality.

CONTENT COLLABORATION

Storage Gateway does not support multiple Storage Gateway instances simultaneously reading from and writing to a single Object Storage bucket. Do not use Storage Gateway as a tool for distributed teams to collaborate on creating and managing content.

FREQUENTLY MODIFIED FILES

Do not use Storage Gateway if you expect your data to be modified frequently. Each time a file is modified and closed, Storage Gateway creates an updated version and uploads it to Object Storage as a new object. Frequently modified data results in substantial inefficiency, in terms of both bandwidth consumption and capacity utilization.

renaming large directory trees

Renaming directories in the Storage Gateway works well for a small directory tree. However, renaming a parent directory with many children can be slow. The service updates the object ID of every corresponding child object in the object store to reflect the new path. If you do start a rename, ensure that the action finishes by monitoring the Pending Uploads field in the Storage Gateway user interface.

Security Considerations

ADMIN PASSWORD

Because Storage Gateway administrators can create, modify, and delete file systems, follow these password guidelines:

• Set a strong password.
• Ensure that the password is secure.
• Share passwords with others only on a need-to-know basis.

DOCKER

Storage Gateway runs inside a Docker container for security and isolation. Follow these Docker-related guidelines and recommendations:

• Avoid or minimize Docker instance operations.
• Avoid logging in to the Docker container. If there is a genuine requirement to log in to the Docker container, use extreme caution to avoid service disruption. Do not change the Docker configuration or the Docker instance unless instructed to do so by Oracle support personal.
• Although the NFS protocol controls access to the file system from clients, Storage Gateway file systems are also locally mounted inside the Docker container. To prevent unauthorized access to file system data, ensure that a Docker container is accessible only by an administrator or an authorized user.
• Configure the Docker host to limit user access to the Storage Gateway Docker container.
• Files and directories in a Docker container are also visible in the Docker host - typically file systems and directories that are provisioned in the Docker host and mapped to the container. Set the appropriate
ownership and modes to ensure that only an administrator or an authorized user can access these folders. We recommend the following:

- A dedicated Storage Gateway host.
- Limit who can access the Storage Gateway host.
- Set firewall rules to limit access to the Docker host and Docker container.
- Implement backup and retention policies for the files associated with Storage Gateway.

ACCESS CONTROL

Default file system export options are too permissive. Set more restrictive export options so that only trusted NFS clients can access the file system data and metadata. Modify the advanced file system settings for NFS Allowed Hosts and NFS Export Options to restrict access to a file system. In addition to NFS protocol security, you can also set up and configure a firewall on the host to further control access to the file system. UID/GID/modes control access to files and directories. Set the appropriate ownership mode to protect sensitive data.

OBJECT STORAGE

Files in a file system are uploaded to Oracle Cloud Infrastructure and stored as objects in an Object Storage bucket. Associated file attributes are stored as object metadata. Access control for Object Storage is different from access control for a traditional file system. Anyone with permission to read or modify any object in the bucket can read or modify all objects in the bucket. To protect sensitive data, set up Oracle Cloud Infrastructure IAM policies to limit who can access objects in the bucket.

Storage Gateway transfers data to Oracle Cloud Infrastructure using HTTPS, which encrypts data packets in flight between Storage Gateway and the cloud. Data written to Object Storage is always automatically encrypted in the cloud.

Limits on Storage Gateway Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

Other limits include:

- Ensure that the number of file systems per Storage Gateway doesn't exceed 10. For best performance, host each file system on a dedicated Storage Gateway.
- Ensure that the number of objects stored in a Storage Gateway file system doesn't exceed 100 million. For datasets that consist of more than 100 million objects, distribute the objects across multiple Storage Gateways.
- Ensure that you configure adequate local storage for file system cache. Storage Gateway warns you if you have configured less than the recommended 500 GB.
- The minimum amount of memory required for any Storage Gateway file system is 16 GB.
  - File systems with up to 50 million files require 32 GB of memory.
  - Large file systems with up to 100 million files require 64 GB of memory.
- The number of files in the cache is limited to 20,000 regardless of the specified cache size in bytes.
- To improve the efficiency of file ingestion, cloud upload operations, and to reduce the number of objects in the namespace, bin-pack or zip small files before writing them to Storage Gateway.

Storage Gateway Release Notes

Release notes provide version-specific release information and important Storage Gateway issues that you need to be aware of:

https://docs.cloud.oracle.com/iaas/releasenotes/services/storage-gateway/

Features of Storage Gateway

This topic highlights key features of Storage Gateway.
POSIX-Compliant NFS Access to Oracle Cloud Infrastructure Object Storage

Using Storage Gateway, your applications can interact with Oracle Cloud Infrastructure Object Storage through standard NFSv4 protocols. You connect Storage Gateway file systems to Object Storage buckets. Storage Gateway stores files as objects in an Oracle Cloud Infrastructure Object Storage bucket and supports multipart uploads for large objects. Object Storage does not, however, support symbolic links, hard links, or special device files.

Note:
Storage Gateway does not support the setgid POSIX function.

Data Integrity with Checksum Verification

The built-in data integrity checks ensure that data is validated as it moves through the data path from Storage Gateway to Oracle Cloud Infrastructure Object Storage. Checksum verification helps ensure data integrity. Metadata integrity checks ensure that the metadata is in a consistent state. The checksum for each file can be read using a custom interface.

Large File Support

The Oracle Cloud Infrastructure Object Storage service supports multipart uploads for faster, more efficient, and resilient uploads. Storage Gateway can use multipart upload for files larger than 128 MB. With multipart uploads, individual parts of an object can be uploaded in parallel to reduce the amount of time you spend uploading. Multipart uploads also minimize the impact of network failures by letting you retry a failed part upload instead of requiring you to retry an entire object upload. See Using Multipart Uploads on page 3477 for details.

Beginning with version 1.3, Storage Gateway provides partial update capabilities to:

- Reduce upload latency.
- Improve the use of available network bandwidth.
- Reduce the minimum required cache size.
- Enable ingestion of single files that are larger than the Storage Gateway cache size.

Storage Gateway's partial update capability leverages the Object Storage service multipart upload functionality to break a large file into smaller parts, and then upload the parts in parallel. After uploading, the service reconstructs them as a single object. With partial update, the service can upload only the modified file parts and reconstruct the object using the unchanged parts that already exist in Object Storage. The service does not need to overwrite the existing object by uploading the entire file.

Since the full file does not have to exist within the Storage Gateway cache at one time, partial update enables the service to ingest single files that are larger than the allocated cache size.

The default file part size is 1GB, with a maximum size of 10TB for the full file. Although the part size is configurable per file system, Oracle does not recommend that you use custom sizes. Custom part sizes do not improve upload performance, but can reduce the maximum supported full file size. The maximum file size is 10,000 times the file part size, with a hard cap of 10TB. If you customize the file part size, you do not need to restart the Storage Gateway, but you must reconnect to the affected file system.

All file parts in the cache are managed by the least recently used (LRU) cache management policy.

To use partial update for objects stored in the Archive Storage tier, you must first restore the object. See Upgrading Storage Gateway on page 3845 for information about upgrading your Storage Gateway system to use partial update.

Support for Data Archival

In addition to uploading to buckets in the Object Storage Standard tier, Storage Gateway supports uploading to and restoring objects from buckets in the Archive Storage tier.

When you create a file system, you specify the storage tier in which to create the corresponding Object Storage bucket.
• The default Standard Object Storage tier is used for storing data to which you need fast, immediate, and frequent access.
• The Archive Storage tier is used for storing data that is accessed infrequently and requires long retention periods.

While Archive Storage is more cost effective than Object Storage for preserving cold data, you must first restore the objects before you can access them. The restoration process can take up to four hours depending on the size of the object. See Overview of Archive Storage on page 484 and Restoring Files and Objects from Archive Storage on page 3832 for details.

Storage Gateway supports Oracle Cloud Infrastructure Object Storage object lifecycle policies to manage the archiving and deletion of objects in a bucket according to a pre-defined schedule. Using object lifecycle policies, you can specify bucket creation in the Standard Object Storage tier, and then create a policy to schedule the subsequent movement of data to the Archive Storage tier. This lifecycle policy archival method is useful if you have on-premises applications that generate intermediary or temporary files and directories that are inappropriate for immediate archival. See Using Object Lifecycle Management on page 3466 for details.

Automated Object Deletion

When you delete a Storage Gateway file from a file system, the corresponding object in Object Storage is automatically deleted.

Quick Access to Select Files with Cache Pinning

Storage Gateway lets you pin files to the file system cache for quick access. You can pin files to the cache for file systems connected to either the Object Storage Standard or Archive tier.

When you write a file to your Storage Gateway file system, the file is initially stored in the file system cache, and then asynchronously uploaded to your Oracle Cloud Infrastructure bucket. After a file has been uploaded, the cache manager can remove the file from the file system cache. To meet the cache threshold specified for the file system, cache is reclaimed using the Least Recently Used (LRU) cache management policy. If you want specific files to be available in the cache for quick access, you can pin the files to the file system cache. Once pinned, files are not removed from the file system cache until you explicitly unpin them.

Storage Gateway Health Check

The Storage Gateway performs automated "health checks" on the system to monitor the status of the following:

• Storage Gateway services and resources
• Local storage, file system cache, metadata storage, and log storage

Integrated Cloud Transfer and Synchronization (Cloud Sync)

Storage Gateway provides an integrated cloud transfer and synchronization feature called Cloud Sync that lets you back up and transfer files on local storage to and from Oracle Cloud Infrastructure Object Storage buckets. This new feature replaces the independent, downloadable cloud sync utility that was available in the previous Storage Gateway version.

You can use the Storage Gateway management console or CLI to create, monitor, and manage Cloud Sync jobs similar to other enterprise NAS backup/replication offerings. Cloud Sync runs as part of the Storage Gateway software inside the Docker instance on the host.

Getting Started With Storage Gateway

This topic provides recommendations for getting started with Storage Gateway.
Recommended Reading

- If you have not done so already, read Overview of Storage Gateway on page 3790. That topic describes:
  - Key concepts for understanding both Storage Gateway and Object Storage.
  - Important security considerations.
  - Recommended uses and workloads.
  - Uses and workloads to avoid.
- Configuring the cache for file systems is key to Storage Gateway. Read Configuring the Cache for File Systems on page 3797 to understand the importance of the file system cache and the guidelines for configuring the cache when you add a file system.
- To understand the prerequisite tasks and requirements for interacting with Object Storage, read Interacting With Object Storage on page 3805.

Next Steps for Setting Up Storage Gateway

Key topics for setting up Storage Gateway include:

- Installing Storage Gateway on page 3807
- Logging In to the Storage Gateway Management Console on page 3815
- Creating Your First File System on page 3816
- Mounting File Systems on Clients on page 3823

Next Steps for Using Storage Gateway

Key topics for using and managing Storage Gateway include:

- Managing File Systems on page 3820
- Managing Storage Gateway on page 3828
- Monitoring Storage Gateway on page 3834

Configuring the Cache for File Systems

Storage Gateway caches frequently retrieved data on the local host, minimizing the number of REST API calls to Oracle Cloud Infrastructure Object Storage and enabling faster data retrieval. You configure the cache for a file system when you create the file system. See Creating Your First File System on page 3816 and Adding a File System on page 3820.

About File System Cache

The file system cache serves as both a read cache and a write buffer for data storage and retrieval. The read cache contains frequently retrieved data that’s accessible locally for read operations. The write buffer contains data that has been copied to the disk cache and queued for upload to your Oracle Cloud Infrastructure tenancy.

When you retrieve data from Oracle Cloud Infrastructure, the data is stored in the Storage Gateway read cache. The read cache allows subsequent I/O operations to that data at local disk speed.

When the read cache is full or reaches the configured limit, Storage Gateway removes files from the cache based on a least recently used (LRU) algorithm. Files pending upload to your tenancy are not removed from cache. You can also preserve files that you do not want removed from cache.

For more information on how to preserve files in the read cache, see Preserving Files in the File System Cache on page 3801.

When an application transfers files through an NFS share, the files are written to the write buffer. The write buffer can contain many files that are queued and pending upload. If the host on which Storage Gateway is installed fails or Storage Gateway stops abruptly, the pending upload operations persist on the local disk. When Storage Gateway restarts, the pending upload operations resume and the data is uploaded to Oracle Cloud Infrastructure.
Configuring Local Storage for File Systems and Cache

Storage Gateway uses local storage attached to the server (or virtual server) for hosting the file systems and cache. Files written to a file system in Storage Gateway are uploaded to the associated Object Storage bucket, with a portion of the file set maintained locally in the file system as a warm cache.

For optimal performance, reliability, and fault tolerance, follow these guidelines when configuring the local Storage Gateway storage:

• Allocate dedicated local storage for each Storage Gateway file system, and associated metadata and logs.
• Multiple disks (hard disk drives or solid-state drives) in a RAID10 set provide an optimal balance of performance, reliability, and fault tolerance. Alternatively, you can use RAID6.

  Important:
  Avoid RAID0 or single disk (no RAID) because of the potential for data loss upon disk failure.

• Provision sufficient space to accommodate the read cache and the write buffer (for ingesting new files) without ever becoming more than 80% full.

  In general, provision file system cache storage that is at least 1.5 times the size of the file set that you want to hold in the read cache. For example, assume that the entire file set requires 50 TB of space. You expect frequent access to 10% (5 TB) of that file set. Ensure that the file system cache storage has at least 7.5 TB of usable capacity. If the cache size reaches a near-full threshold, any data ingestion results in an out of space error in Storage Gateway.

• When you provision local storage at installation time, Oracle recommends that you configure the read cache to be equal to the file system cache size minus the desired write buffer size. If the file system cache is less than 300 GB, Storage Gateway generates a warning message.

Determining File System Cache Size

The Storage Gateway file system cache serves as both a read cache and a write buffer. You can specify the maximum size of the read cache. The write buffer uses any remaining available space in the file system cache. You do not explicitly specify a size for the write buffer.

  Important:
  Oracle recommends that you configure the read cache to be equal to the file system cache size minus the desired write buffer size.

Read Cache Size

The default maximum read cache size is 300 GB if the file system cache size is greater than 300 GB. Changing the default maximum read cache size is optional. The appropriate size depends on Storage Gateway workload. While the default setting for the read cache is appropriate for most workloads, consider increasing the size if Storage Gateway must retrieve a significant amount of data from the cloud.

Use the following guidelines to determine the appropriate setting for the read cache size:

• Do not set the read cache maximum equal to the size of the file system cache. Doing so allocates 100% of the space for the read cache and leaves no capacity for ingesting new files. If there is no available space for new file ingestion, Storage Gateway stops ingesting data and begins evicting files from the read cache to create space. Always preserve some space in the file system cache for ingestion.

• Set the read cache size to equal the amount of data that you anticipate to be accessed frequently, while leaving enough capacity for the write buffer.

  Note:
  If the total file system cache size is less than 300 GB, Storage Gateway automatically sets the read cache maximum size to 20% of the file system cache. The system does not honor custom read cache configuration settings for a file system cache less than 300 GB.
After you calculate the optimal file system cache size, you can configure the read cache when creating the file system or adjust it after monitoring the workload. See Adding a File System on page 3820 and Changing the Properties of a File System on page 3826.

**Write Buffer Size**

Optimizing the space available for the write buffer is an important part of determining the appropriate file system cache size. The write buffer size increases when data is ingested in Storage Gateway and decreases after the data is uploaded to the cloud.

**Important:**
- When the write buffer uses all available file system cache space, further data ingestion is blocked until a portion of the existing files are uploaded and evicted from the cache.
- Oracle recommends that you allow a minimum of 300 GB for the write buffer under any circumstances.

Use the following guidelines to determine the space needed for the write buffer:

- Identify the amount of data to be uploaded in Storage Gateway. If a large amount of data is uploaded, the Storage Gateway write buffer can reach its maximum size. Exceeding the write buffer leads to I/O failure as the file system cache has no space available. If you cannot regulate data ingestion, you can increase the file system cache space to avoid I/O failure. You can regulate I/O by pausing after a certain amount of data is ingested or by periodically allowing uploads to complete before ingesting more data. For example, you can use this approach for backups run as cron jobs when the file system cache space is less than the amount of data to be ingested.
- Calculate the amount of data that is ingested on any typical day or week in Storage Gateway. Also, calculate the amount of data that is uploaded over a time period, based on the available bandwidth or historical data. Ensure that the difference between these calculations does not exceed the write buffer size.
- Some applications can handle I/O failure, and then resume writing data. In this case, consider setting the cache size to the amount of data that you’d like the application to tolerate before the cache space can be reclaimed.

As stated earlier, you want to avoid completely filling the file system cache. The write buffer grows by the difference between the ingest rate and the upload rate. The file system cache size must be larger than the read cache plus the total number of bytes buffered at any point during the job. If you have workloads that upload large amounts of data in parallel, you can use the following equation to determine the amount of space needed by the write buffer.

\[
WB \geq D \times (1 - UR/IR) + E
\]

**WB** = Recommended write buffer size  
**D** = Total uploaded dataset size  
**UR** = Upload rate (The upload rate is the lesser of the actual upload rate or the disk read speed.)  
**IR** = Ingestion rate (disk write speed)  
**E** = Extra margin (Oracle recommends at least 50 GB.)

**Note:**  
This equation applies only if the upload rate is less than the ingest rate.

Run the following command to measure your system's ingestion rate:

```
sudo docker exec -it ocisg python /opt/oracle/gateway/python/packages/ocisg_helper/disk_speed_test.py
```

**Example output:**

```
Write speed:
2.1 GB copied in 9.4 seconds (228 MB/s)
```
Read speed:
2.1 GB copied in 6.8 seconds (315 MB/s)

If read and writes occur in parallel during the job, the read and write speeds are about 50% of the returned values.

Run the following command to measure your system's upload rate:

```
sudo docker exec ocisg cat /mnt/gateway/cache-phoenix/:::diag:oci-network-speed-test
```

Example output:

```
Average Upload Speed = 125 MB/s
```

**Example 1**

Daily dataset is 500 GB
Upload rate = 2 MB/s
Disk read = 600 MB/s
Ingestion rate (Disk write) = 600 MB/s
Apply the equation:
WB >= 500 GB * (1 - (2/600)) + 50 GB
WB >= 549 GB
In this case, the upload rate is very slow compared to the ingestion rate, so the entire dataset needs to fit in the write buffer.

**Example 2**

Daily dataset is 1 TB
Upload rate = 300 MB/s
Disk read = 400 MB/s
Ingestion rate (Disk write) = 100 MB/s
In this case, we recommend the minimum write buffer size of 300 GB, since the upload rate is higher than the ingestion rate.

**Example 3**

Daily dataset is 5 TB
Upload rate = 250 MB/s
Disk read = 400 MB/s
Ingestion rate (Disk write) = 300 MB/s
Apply the equation:
WB >= 5 TB * (1 - (250/300)) + 50 GB
WB >= 0.88 TB
WB is 880 GB.
Note:

Storage Gateway begins throttling I/O when the free cache space falls below 15 GB. Determine if the application is able to handle the throttling or if you want to provision more cache space.

Preserving Files in the File System Cache

When you write a file to your file system, the file is initially stored in the file system cache, and then uploaded to your Oracle Cloud Infrastructure tenancy. After a file has been uploaded, the cache manager can remove the file from the file system cache. To meet the cache threshold specified for the file system, cache is reclaimed using the Least Recently Used (LRU) cache management policy. If you want specific files to be available in the cache for quick access, you can pin the files to the file system cache. Once pinned, files are not removed from the file system cache until you explicitly unpin them. You can view the Maximum Read Cache Size in GiB for a selected file system in the management console under Settings.

You can pin files connected to both Standard and Archive storage tiers to file system cache. Files that you write to a file system are always uploaded to your tenancy, regardless of whether the files are pinned to the cache.

If the file that you want to pin to cache is not present in the cache, the file is automatically downloaded to the cache if the file system is connected to a Standard storage tier. If that file belongs to a file system connected to an Archive storage tier, you must first restore the file before the file can be downloaded to the cache. See Restoring Files and Objects from Archive Storage on page 3832 for details.

Important:

- By default, the cache pinning feature is enabled on all file systems.
- When selecting the files for cache pinning, consider the overall cache threshold and calculate the residual cache space that remains available for normal cache operations. For example, assume that your cache threshold is 1 TB and you estimate that the files you want to pin to cache occupy 300 GB. That leaves 700 GB of usable space in your cache after pinning the files.
- When you restore a file from the Archive storage tier, the file moves to the Standard storage tier. The file remains in Standard storage for 24 hours or the retention duration you specify. The continued availability of the file in the cache depends on the LRU operation. However, if you pin such a file to the cache, the restored file remains in the cache until you unpin the file.

Enabling and Managing Cache Pinning

To perform cache pinning operations for a file system, run the following command from the NFS client on which the file system is mounted:

```
cat /path/to/mountpoint/<file_path>:::cache:cache_command[:argument]
```

The following table lists the cache pinning operations and the corresponding command and argument for each operation:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Cache Command</th>
<th>Argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable cache pinning for a file system. By default, cache pinning is enabled for all file systems.</td>
<td>set-preserve-option</td>
<td>true</td>
</tr>
<tr>
<td>Operation</td>
<td>Cache Command</td>
<td>Argument</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Get the cache pinning status for a file system.</td>
<td>get-preserve-option</td>
<td>No argument</td>
</tr>
<tr>
<td>Disable cache pinning for a file system.</td>
<td>set-preserve-option false</td>
<td></td>
</tr>
<tr>
<td>List the files that are pinned to the cache.</td>
<td>list-preserve</td>
<td>No argument</td>
</tr>
<tr>
<td>Remove deleted files from the preserve list.</td>
<td>list-preserve-update</td>
<td>No argument</td>
</tr>
<tr>
<td>Add a file to the preserve list.</td>
<td>add-preserve</td>
<td>No argument</td>
</tr>
<tr>
<td>Remove a file from the preserve list.</td>
<td>remove-preserve</td>
<td>No argument</td>
</tr>
<tr>
<td>Clear the preserve list.</td>
<td>clear-preserve</td>
<td>No argument</td>
</tr>
</tbody>
</table>

**Example Commands**

- To enable cache pinning for the myFS file system:

  ```
  cat /mnt/gateway/myFS/:::cache:set-preserve-option:true
  ```

- To get the cache pinning status for myFS:

  ```
  cat /mnt/gateway/myFS/:::cache:get-preserve-option
  ```

  If cache pinning is enabled for the file system, the output of this command is `true`. Otherwise, the output is `false`.

- To disable cache pinning for the myFS file system:

  ```
  cat /mnt/gateway/myFS/:::cache:set-preserve-option:false
  ```

- To add a file `myFile` of the myFS file system to the preserve list:

  ```
  cat /mnt/gateway/myFS/myFile:::cache:add-preserve
  ```

- To find out which files are added to the preserve list of the myFS file system:

  ```
  cat /mnt/gateway/myFS/:::cache:list-preserve
  ```

  Sample output of the preceding command:

  ```
  ["/doNotDelete.txt", "/myFileMetadata", "/myFile"]
  ```

- To remove the file `myFile` from the preserve list:

  ```
  cat /mnt/gateway/myFS/myFile:::cache:remove-preserve
  ```
To update the preserve list when the output of the `cache:list-preserve` command indicates that a pinned file has been removed from the file system:

```
cat /mnt/gateway/myFS/:::cache:list-preserve-update
```

Sample of the original preserve list:

```
["/doNotDelete.txt", "/myFileMetadata"]
```

Output of the `cache:list-preserve` command after the file `myFileMetadata` is removed from the cache:

```
["/doNotDelete.txt", "Status: 1 files appear to no longer exist. Please run list-preserve-update"]
```

Output of the `cache:list-preserve-update` command:

```
["/doNotDelete.txt"]
```

To clear the preserve list for a file system:

```
cat /mnt/gateway/myFS/:::cache:clear-preserve
```

**Understanding Storage Gateway Performance**

This topic covers the performance characteristics of Storage Gateway and the ways you can maximize its efficiency.

**Performance Characteristics**

It is important to understand the basic performance characteristics of Storage Gateway:

- Because there is transactional overhead for each file, Storage Gateway generally exhibits better performance with large files than with small files. Storage Gateway can only upload data as fast as your connection and the storage host allows. Storage Gateway buffers the data in local disk storage while waiting to upload to Oracle Cloud Infrastructure. Once a file is uploaded, the file's local copy can be removed from the cache to free up space. If file system cache space falls below 10 GB, application I/O and file/directory creation can fail.
- Storage Gateway does not support frequently modified files such as logs, databases, or virtual disks. Storage Gateway depends on the closing of a file to trigger an upload of that file. If a file never closes or is modified frequently, the upload event cannot successfully occur.
- Upload throughput to Object Storage (WAN) is typically slower than NFS client throughput (LAN). As a result, Storage Gateway can accumulate a large amount of data that is pending upload.
- You can attach Storage Gateway to an existing Object Storage bucket that contains data. The service is optimized for this type of initialization. Storage Gateway can initialize about 700 thousand files per hour with a hard disk drive-based cache. It can initialize about 7 million files per hour with an NVMe SSD-based cache.

**Factors That Affect Performance**

To get the maximum performance benefits from Storage Gateway, follow the practices documented at Best Practices for Using Storage Gateway on page 3842.

In addition to having sufficient memory and file system cache space, Oracle recommends that you use SSDs to help improve NFS ingestion rate.

Storage Gateway is tuned for maximum upload and download performance by default. No additional tuning is needed.
Performance Testing

While measuring performance is complex and open to variability, we have observed the following in performance benchmark tests with 10-Gb/s link speed:

<table>
<thead>
<tr>
<th>Workload (Upload/Download)</th>
<th>Configuration</th>
<th>Average Upload Throughput</th>
<th>Average Download Throughput</th>
</tr>
</thead>
</table>
| Single large file of 400 GB | CPU: 8 cores  
Memory: 32GB  
Disk Read: 340 MB/s  
Disk Write: 234 MB/s  
Link Speed: 10 Gb/s (1.25 GB/s) | 239 MB/s | 195 MB/s |
| Multiple files of 10-50 GB (Total data = 400GB) | CPU: 8 cores  
Memory: 32GB  
Disk Read: 340 MB/s  
Disk Write: 234 MB/s  
Link Speed: 10 Gb/s (1.25 GB/s) | 260 MB/s | 225 MB/s |

Note:
Using FastConnect with Storage Gateway makes optimal use of full link speed. We have customers using FastConnect with 10-Gb/s link speed and have seen each gateway achieve 400–450 MB/s uploads to Oracle Cloud Infrastructure. See FastConnect Overview on page 3173 for more information.

Testing Network Bandwidth

Storage Gateway provides a diagnostic command that you can use to test the bandwidth in your environment and ensure that you get the expected upload and download speeds. The amount of data transferred depends on these factors:

Bandwidth * Delay Product (bits) = total_available_bandwidth (bits/sec) x round_trip_time (sec)

Note:
Different buckets can have different upload and download speeds. The round_trip_time can vary by region.

To run the diagnostic command:
You need root permissions to run the diag command.
1. Using SSH, log in to the host on which you installed Storage Gateway.
2. Run the `diag` command, specifying the Storage Gateway file system name:

```
[root@ocisg-ashburn opc]# sudo docker exec ocisg cat /mnt/gateway/<file_system_name>/:::diag:oci-network-speed-test
```

The `diag` command responds with the average upload speed, for example:

```
Average Upload Speed = 217 MB/s
```

## Interacting With Object Storage

This topic helps you understand the Oracle Cloud Infrastructure Object Storage environment and how it interacts with a Storage Gateway.

### Creating the Required IAM Users, Groups, and Policies

An Oracle Cloud Infrastructure administrator must perform prerequisite tasks in preparation for data movement between Storage Gateway and Object Storage. If you are new to Oracle Cloud Infrastructure, we recommend that you read Setting Up Your Tenancy on page 122.

To use Oracle Cloud Infrastructure, you must be granted security access in a *policy* by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which *compartment* you should work in.

Access to resources is provided to groups using policies and then inherited by the users that are assigned to those groups. For details on creating groups, see Managing Groups on page 2419.

For Storage Gateway, an administrator creates these groups with the following policies:

<table>
<thead>
<tr>
<th>Allow group <code>&lt;group_name&gt;</code> to manage buckets in compartment <code>&lt;compartment_name&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow group <code>&lt;group_name&gt;</code> to manage objects in compartment <code>&lt;compartment_name&gt;</code></td>
</tr>
</tbody>
</table>

### Content Consistency Between Storage Gateway and Object Storage

Changes to the files in Storage Gateway, including create, write, update, and delete, eventually are consistent with Object Storage. Uploads are asynchronous and buffered for performance, so Storage Gateway file changes might not yet be reflected in Object Storage.

You can access, modify, and upload objects directly to a bucket using Object Storage native APIs, SDKs, the CLI, the Console, or the HDFS connector. Objects modified in these ways do not appear as files in Storage Gateway until you click **Refresh** in the Storage Gateway management console.

### Name Restrictions

Storage Gateway file and file system names must adhere to Object Storage bucket and object name restrictions and guidelines.

Use the following guidelines for naming file systems:

- Use from 1 to 256 UTF-8 characters.
- Valid characters are letters (upper or lower case), numbers, hyphens, underscores, and periods.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names cannot contain a slash (/) character because this character delimits Object Storage bucket and object names.</td>
</tr>
</tbody>
</table>
- Avoid entering confidential information.
• Make the name unique within a Storage Gateway instance.

Use the following guidelines for naming files:
• Use from 1 to 1024 characters.
• Valid characters are letters (upper or lower case), numbers, and characters other than linefeed, newline, and NULL.
• Use only Unicode characters for which the UTF-8 encoding does not exceed 1024 bytes. Clients are responsible for URL-encoding characters.
• Avoid entering confidential information.
• Make the name unique within the bucket. Do not use the name of an existing object within the bucket when naming an object unless you intend to overwrite the existing object with the contents of the new or renamed object.

Custom Metadata
POSIX file and directory attributes are stored in custom metadata. These attributes include uid, gid, mode, atime, ctime, and mtime. If existing objects in Object Storage are missing the required custom metadata, Storage Gateway assigns the following default values:
• uid=0
• gid=0
• mode=0644 for file and 0755 for directory

The custom metadata is not updated in Object Storage until a file operation triggers Storage Gateway to update the file in Object Storage. Timestamp metadata (atime, ctime, and mtime) are expressed in milliseconds. Access modes are expressed in octal and include file/directory bit.

The custom metadata names follow these guidelines:
• Only ASCII characters.
• A maximum of 128 bytes.

The custom metadata values follow these guidelines:
• Only UTF-8 characters.
• A maximum of 256 bytes.

Understanding Directory and File Hierarchy Translations in Object Storage
Within an Object Storage namespace, buckets and objects exist in a flat hierarchy. Storage Gateway flattens the file system directory hierarchy into nested object prefixes in Object Storage.

For directories:
• A Storage Gateway file system called myFS that contains a directory called myDir, appears in Object Storage as:

n/<os_namespace>/b/myFS/o/myDir/

• A Storage Gateway file system called myFS that contains a myDir subdirectory called mySubDir, appears in Object Storage as:

n/<os_namespace>/b/myFS/o/myDir/mySubDir/

You can distinguish a Storage Gateway directory from a Storage Gateway file in the following ways:
• Directories have a trailing slash /.
• Directory size or length is 0 (zero).

For files:
• A Storage Gateway file system called `myFS` that contains a directory called `myDir` with a file called `file1`, appears in Object Storage as:

```
/n/<os_namespace>/b/myFS/o/myDir/file1
```

• A Storage Gateway file system called `myFS` that contains a `myDir` subdirectory called `mySubDir` with a file called `file2`, appears in Object Storage as:

```
/n/<os_namespace>/b/myFS/o/myDir/mySubDir/file2
```

You can distinguish a Storage Gateway file from a Storage Gateway directory in the following ways:

• Directories have a trailing `/` and files do not.
• File length can be 0 (zero) or non-zero, but directory length is always 0 (zero).

### Internal Storage Gateway Objects

Storage Gateway creates some special internal objects in Object Storage. These objects have a `/gateway` directory prefix. For example:

```
/n/<object_storage_namespace>/b/<bucket>/o///gateway
```

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not modify or remove the objects in the special <code>/gateway</code> directory. These objects are critical for Storage Gateway operation.</td>
</tr>
</tbody>
</table>

### Installing Storage Gateway

This topic provides instructions for installing the Storage Gateway software.

### Prerequisites

These instructions assume that you are familiar with the administration and configuration commands of the operating system on your host machine. To install Storage Gateway, your host system must meet certain hardware and software requirements.

### Hardware Recommendations and Requirements

To run Storage Gateway, the host machine must meet the following requirements:

• Two dual-core CPUs or better. Oracle recommends 4-core CPUs.
• Minimum memory requirements:
  • 16 GB for required for any Storage Gateway file system.
  • 32 GB for file systems up to 50 million files.
  • 64 GB for file systems up to 100 million files.
• The recommended local storage disk size is 600 GB, which includes 500 GB for the file system cache, 80 GB for metadata storage, and 20 GB for log storage.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision local storage before installing Storage Gateway. For best performance, allocate dedicated local storage file systems for the Storage Gateway cache, the metadata, and the logs. The installation script prompts you for the paths to your Storage Gateway file system cache, metadata storage, and log storage locations. Follow the disk size recommendations provided by the installer.</td>
</tr>
</tbody>
</table>
Oracle recommends that you use the XFS file system for the file system cache, metadata, and logs. XFS is a 64-bit file system designed for parallel I/O. Parallel I/O allows a system to scale based on the number of I/O threads and file system bandwidth.

## Software Requirements

- Oracle Linux 7 with UEK Release 4 or later.

**Note:**
If you create an Oracle Cloud Infrastructure Compute instance to host Storage Gateway, the instance creation wizard provides an option to choose the operating system image.

- Docker 1.12.6 or newer. Docker is an open platform for building, shipping, and running distributed applications. For more information, see [https://www.docker.com/](https://www.docker.com/).
- NFSv4.

**Note:**
The Storage Gateway installation software automatically installs Docker and the NFS protocol.

## Hosting Storage Gateway on an Oracle Cloud Infrastructure Compute Instance

To host Storage Gateway on an Oracle Cloud Infrastructure Compute instance, you need:

- An SSH key pair in PEM format.
  - To create a key pair, see [Managing Key Pairs on Linux Instances](#) on page 693.
  - If your public key is not in PEM format, use the following command to convert it:

```
ssh-keygen -f <key_name>.pub -e -m pem
```

- An Oracle Cloud Infrastructure user account with an API signing key (the public key from your SSH key pair).
  - If you need to create a user account, see [To create a user](#) on page 2417.
  - To upload an API signing key to an existing user account, see [To add an API signing key](#) on page 2461.
- A virtual cloud network (VCN) and related resources. For help with creating a VCN, see [VCNs and Subnets](#) on page 2821.

The following configuration points apply to your VCN:

- Do not select the **Use DNS Hostnames in this VCN** check box unless you plan to use DNS hostnames for your Storage Gateway Compute instance.
- The security list must include a rule to allow SSL (443) ingress.
- After you install the Storage Gateway software your host machine, you must add a security list rule to allow communication with the management console port. More information appears on this page after the Storage Gateway installation instructions.
- A Compute instance. See [Creating an Instance](#) on page 695.

The VM.Standard2.4 Compute shape meets the minimum required specifications for Storage Gateway. Large file systems might require an image with more resources.

- A Block Volume. See [Creating a Volume](#) on page 515.
  - The recommended disk size is 600 GB.
  - Attach the volume to your Compute instance. See [Attaching a Volume](#) on page 517.
  - If you specify **Volume Attachment Types** on page 501 as the volume attachment type, you must also connect and mount the volume from the instance for the volume to be usable. For more information, see [Volume Attachment Types](#) on page 501 and [Connecting to a Volume](#) on page 524.
Installing Storage Gateway

You can install Storage Gateway on an Oracle Cloud Infrastructure Compute instance or an on-premises host that meets the hardware and software requirements.

To install the Storage Gateway software

1. Connect to your Compute instance or on-premises host.
   
   For help with connecting to an Oracle Cloud Infrastructure Compute instance, see Connecting to an Instance on page 733.

2. If your host volume is new, you might need to format and mount the disk.

   Tip:
   
   This task describes the simplest way to create a functional file system to host a Storage Gateway. It uses one device and file system to host the cache, metadata, and log volumes. You specify the paths to those volumes later in this procedure. To optimize performance for your system, you can:
   
   • Create a separate device and file system for each of the cache, metadata, and log volumes.
   • Create a single device, but create logical volumes and file systems for the cache, metadata, and log volumes.

To format the disk and create a file system:

   a. Run fdisk:

      ```
      sudo fdisk /dev/sdb
      ```

      (Optional) Press **m** to view the *fdisk* options.

   b. Choose command **g** - create a new empty GPT partition table.

   c. Choose command **w** - write table to disk and exit.

   d. Create an XFS (file system).

   To make file system volume extensive, we recommend using LVM to create logical partitions that can span across one or more physical hard drives. First, the hard drives are divided into physical volumes, then those
physical volumes are combined to create the volume group and finally the logical volumes are created from
volume group. Follow these steps:

1. Create a volume group.

   ```bash
   sudo vgcreate <volume_group_name> <device>
   ```

2. Create a logical volume.

   ```bash
   sudo lvcreate -l 100%FREE -n <logical_volume_name> <volume_group_name>
   ```

3. Create an XFS file system.

   ```bash
   sudo mkfs.xfs /dev/<volume_group_name>/<logical_volume_name>
   ```

4. Mount the XFS file system.

   ```bash
   sudo mount /dev/<volume_group_name>/<logical_volume_name> <directory_path>
   ```

To mount the formatted volume:

a. Create a mount directory:

   ```bash
   sudo mkdir /ocisg
   ```

b. Mount the drive:

   ```bash
   sudo mount /dev/sdb /ocisg
   ```

3. Download the Storage Gateway 1.3 tar archive.

4. Use the SFTP tool of your choice to copy the tar archive into the /tmp folder of the host machine.

5. On the host machine, change directory to /tmp and extract the files from the tar archive:

   ```bash
   cd /tmp
   sudo tar xvfz ocisg-1.3.tar.gz
   ```

   This command extracts the files from the tar archive into a subdirectory named ocisg-1.3.

6. Change directory to ocisg-1.3 and run the installation script as sudo or root user:

   ```bash
   cd ocisg-1.3
   ```
sudo ./ocisg-install.sh

Optionally, you can specify the following `ocisg-install.sh` script flags:

- **-a** Runs the installation in advanced configuration mode, which lets you specify ports and the Docker network mode.

  In addition to prompting you for the paths to the metadata storage, cache storage, and log storage, advanced configuration mode also prompts you for:

  - The Docker network mode (host or bridge).
    
    Bridge mode is the default. It allows multiple instances of Storage Gateway to run on the same host.
    Host mode improves network performance. If you plan to run only one instance of Storage Gateway on the host, Oracle recommends host mode. If you encounter issues with host mode, try bridge mode or contact [My Oracle Support](https://support.oracle.com).
  
  - The host port to use for the management console.
  
  - The host port to use for NFS access.
  
  - The host port to use for the HTTP REST service.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each host port specification, you can designate a port or press Enter to let Storage Gateway dynamically allocate the port. You can use the <code>ocisg configure port</code> command to change the ports</td>
</tr>
</tbody>
</table>
• **-d** Installs Storage Gateway at the location you specify instead of the default location of /opt/ocisg. For example:

```bash
sudo ./ocisg-install.sh -d /opt/storagegateway
```

• **-h** Displays the installation script help information.

• **-p** Specifies that Storage Gateway is running behind a proxy server. You can specify multiple proxy arguments. For example:

```bash
```

• **-q** Runs the installation in quiet mode.

If you supply the paths to the Storage Gateway cache, metadata, and log storage locations using `-m <path_to_metadata_storage>`, `-c <path_to_cache_storage>`, and `-l <path_to_log_storage>`, you are not prompted for input. For example:

```bash
sudo ./ocisg-install.sh -q -m /ocisg/metadata -c /ocisg/cache -l /ocisg/log
```

**Note:**

Ignore the devicemapper warning message if it appears during the installation.

The script guides you through the Storage Gateway installation. Depending on your host machine configuration, some steps can require your input:

1. Docker does not appear to be installed. Do you want to install docker engine with yum? [y/N]
   
   Press y, and then press Enter.

   The installation script automatically installs Docker and configures the storage driver for use with Storage Gateway.

**Important:**

If Docker is already installed on your system, the installation script does not automatically configure the storage driver and returns a warning message:

```
Checking that docker is installed and using the correct version
Found docker version Docker version 18.03.1-01, build 0d51d18
The storage appliance requires to set devicemapper as the docker storage driver.
Please follow the setup link below to enable devicemapper and rerun the install.
```
b. **NFS server does not appear to be enabled. Do you want to enable NFS?** [y/N]

Press y, and then press **Enter**.

c. When prompted, press **Enter** accept the default installation location.

d. When prompted, specify the paths to your Storage Gateway cache, metadata, and log storage locations.

The following examples represent paths for a simple system. Your setup might include paths to separate devices and file systems for each location.

1. Enter a path for the file system cache. For example:

   /oci$g/sg/cache

2. Enter the path for metadata storage. For example:

   /oci$g/sg/metadata

3. Enter the path for log storage. For example:

   /oci$g/sg/log

If you receive warnings about cache, metadata, and log storage existing on the same volume, enter y to proceed with the installation.

After a successful installation, the script provides the following information:

- The URL to log in to the Storage Gateway management console.
- The NFS port number.
- An example command for mounting your Storage Gateway file systems.

If you installed Storage Gateway on a Compute instance, see **Security List Requirements for Compute Instance Installations** on page 3813.

### Security List Requirements for Compute Instance Installations

If you installed Storage Gateway on an Oracle Cloud Infrastructure Compute instance, that instance must be able to receive HTTPS connections from other hosts and allow communication with the Storage Gateway management console. To open the necessary port, add an ingress rule to the security list governing the instance's host subnet. To learn about VCN security control, see **Security Lists** on page 2850.

**Important:**

This installation task assumes that your existing security list already allows traffic to port 443, as described in the **Prerequisites** on page 3807 section of this page. If port 443 is not open, you must add a security list rule to open it.

**To add a security list rule**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the name of the cloud network (VCN) that hosts your Compute instance.
3. Click **Security Lists**.
4. Click the name of the security list that governs the subnet hosting your Compute instance.
5. Click **Edit All Rules**.
6. Add an ingress rule:
   
a. Leave **Stateless** unmarked.
   
b. Select CIDR for the **Source Type**.
   
c. Enter `0.0.0.0/0` to indicate all IP addresses.
   
d. Select **TCP** as the **IP Protocol**.
   
e. Enter **All** in the **Source Port Range** field.
   
f. Specify your Storage Gateway management console port in the **Destination Port Range** field. For example:

   ```
   32769
   ```

   If you do not know the management console port for your Storage Gateway installation, run the following command on the host machine:

   ```
   sudo ocisg info
   ```

   The management console port appears at the end of the management console URL:

   ```
   Management Console: https://exampleCompute:32769
   ```

7. Click **Save Security List Rules**.

   You can now connect to the compute instance using the public IP address (https://<public_IP_address>). See [Getting the Instance Public IP Address and Initial Windows Password](#) on page 78 for details.

### Verifying and Updating the Storage Driver in Docker

To verify the storage driver in Docker:

1. **Start docker:**

   ```
   sudo systemctl start docker
   ```

2. **Verify the information in docker:**

   ```
   sudo docker info
   ```

3. **Look for Storage Driver in the output. For example:**

   ```
   Containers: 0
   Running: 0
   Paused: 0
   Stopped: 0
   Images: 0
   Server Version: 18.03.1-ol
   Storage Driver: overlay2
     Backing Filesystem: xfs
     Supports d_type: true
     Native Overlay Diff: false
   Logging Driver: json-file
   Cgroup Driver: cgroupfs
   Plugins:
     Volume: local
     Network: bridge host macvlan null overlay
     Log: awslogs fluentd gcplogs gelf journald json-file logentries splunk syslog
   Swarm: inactive
   Runtimes: runc
   Default Runtime: runc
   Init Binary: docker-init
   containerd version: 773c489c9c1b21a6d78b5c538cd395416ec50f88
   runc version: 4fc53a81fb7c994640722ac585fa9ca548971871
   ```
init version: 949e6fa
Security Options:
seccomp
Profile: default
selinux
Kernel Version: 4.1.12-124.15.4.el7uek.x86_64
Operating System: Oracle Linux Server 7.5
OSType: linux
Architecture: x86_64
CPUs: 4
Total Memory: 13.45GiB
Name: ocisg-mahesh
Docker Root Dir: /var/lib/docker
Debug Mode (client): false
Debug Mode (server): false
Registry: https://index.docker.io/v1/
Labels:
Experimental: false
Insecure Registries:
127.0.0.0/8
Live Restore Enabled: false
Registries: docker.io (secure)

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore the devicemapper warning message if it appears.</td>
</tr>
</tbody>
</table>

If Storage Driver is not devicemapper, do the following:

a. Stop docker:

```
sudo systemctl stop docker
```

b. Look for /etc/docker/daemon.json in the host.

If the file daemon.json does not exist, create it.

c. In the daemon.json file, set the storage-driver variable to devicemapper:

```
{
   "storage-driver": "devicemapper"
}
```

d. Restart docker:

```
sudo systemctl start docker
```

e. Verify the information in docker:

```
sudo docker info
```

Look for Storage Driver in the output and verify that the storage driver is devicemapper.

**Next Step**

[Logging In to the Storage Gateway Management Console on page 3815]

**Logging In to the Storage Gateway Management Console**

Use the Storage Gateway management console to create, manage, and monitor file systems.
Storage Gateway provides the URL to access the management console after a successful installation. When you access the management console for the first time, a wizard prompts you to create the administrator credentials and your first file system.

**Note:**

Storage Gateway uses a self-signed certificate for the HTTPS connection. Your browser might warn that the SSL certificate couldn’t be verified. If you entered the correct public IP address of the Storage Gateway instance, you can safely ignore this warning. The steps to ignore this warning and go to the management console vary depending on the browser you use.

**To log in to the management console:**

1. Enter one of the following URLs in a supported web browser:
   - If you installed the software on an on-premises host, enter the URL provided at the end of the Storage Gateway installation script:
     ```
     https://<storagegateway_hostname>:<port_number>
     ```
     For example:
     ```
     https://myStorageGatewayHost:3775
     ```

     **Note:**
     If you cannot access Storage Gateway using the hostname, contact your network administrator. Depending on your network configuration, your Storage Gateway hostname might need to be added to DNS or you might need to use an IP address rather than the hostname.
   - If you installed the software in an Oracle Cloud Infrastructure compute instance, enter the URL as follows:
     ```
     https://<instance_public_IP_address>:<port_number>
     ```
     For example:
     ```
     https://192.168.14.5:3775
     ```

     **Note:**
     See [Getting the Instance Public IP Address](#) on page 67 for details.

   The console log-in page appears. The page prompts you to set and confirm a password for the Storage Gateway admin user.

2. Enter a password that meets the following requirements:
   - From 8 to 32 characters.
   - At least one special character, one numerical character, one uppercase character, and one lowercase character.

**Next Step**

[Creating Your First File System](#) on page 3816

**Creating Your First File System**

This topic guides you through creating your first Storage Gateway file system.

Think of a file system as a namespace containing a dataset that’s accessible through Storage Gateway. A Storage Gateway file system in this context represents a mapping between a directory on your on-premises host and a bucket
in Oracle Cloud Infrastructure Object Storage. When you create a Storage Gateway file system, you define the connection credentials that Storage Gateway uses to connect to your Oracle Cloud Infrastructure tenancy.

When you log in to the management console for the first time, a wizard prompts you to create the administrator credentials and your first file system.

To create your first file system

1. Log in to the management console.
2. Click **File Systems** on the upper-right area of the management console.
3. Click **Create File System**.
4. Enter the required information in **Create a File System**:

   - **File System Name**: A unique, friendly name for the file system. Avoid entering confidential information. Use the following guidelines when naming a file system:
     - Use from 1 to 256 characters.
     - Valid characters are letters (upper or lower case), numbers, hyphens, underscores, and periods.

   **Important**: The name cannot contain the following:
   - A slash (/) character because this character delimits bucket and object names in Oracle Cloud Infrastructure Object Storage
   - The strings "pub" or "priv"

   If an Object Storage bucket by this file system name doesn’t exist in your tenancy, the bucket is created.

   If a corresponding Object Storage bucket by this file system name exists in your tenancy and there is data in the bucket, Storage Gateway works asynchronously to sync the bucket and file system contents.

   - **Select the Object Storage tier in which you want to store your data**

   **Important**: Once set, you cannot change the storage tier in which a bucket resides.

   You can use the Oracle Cloud Infrastructure Object Storage object lifecycle policies feature to manage the archiving and deletion of objects in a bucket according to a predefined schedule. See **Using Object Lifecycle Management** on page 3466 for details.

   - **Standard**: The Standard tier is the primary default Object Storage tier for storing data that requires frequent and fast access. See **Overview of Object Storage** on page 3392 for more information.
   - **Archive**: The Archive tier is a special tier for storing data that is accessed infrequently and requires long retention periods. See **Overview of Archive Storage** on page 484 for more information. Access to data in the Archive tier is not immediate since you must restore archived data before it’s accessible (see **Restoring Files and Objects from Archive Storage** on page 3832).

   - **Object Storage endpoint**: Required. The Object Storage API endpoint for your service instance. To find the object storage API endpoint for your Oracle Cloud Infrastructure Object Storage tenancy, see the API documentation for Oracle Cloud Infrastructure Object Storage.

   **Important**: The following information is required to connect your Storage Gateway file systems to Oracle Cloud Infrastructure. See **Required Keys and**
OCIDs on page 4179 for detailed information on how to generate the required keys and where to obtain these OCIDs.

- **Compartment OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage compartment.
- **Tenant OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage tenancy.
- **User OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage user.
- **Public Key's Finger Print**: Required. Your Oracle Cloud Infrastructure Object Storage public key fingerprint.
- **Private Key**: Required. Your Oracle Cloud Infrastructure Object Storage private key.
- **Private Key Passphrase**: Required if a passphrase was specified during key creation. Your Oracle Cloud Infrastructure Object Storage private key passphrase.

**Note:**

Your private key and passphrase are securely stored in the Storage Gateway docker. The Storage Gateway installation generates a pair of public and private keys. The system uses the public key to encrypt sensitive data.

5. **Click Save.**

The values you entered must match your Oracle Cloud Infrastructure credentials. If you get an error message, verify your entries, update any incorrect values, and click **Save** again.
6. Click **Show Advanced File System Configuration**.

Enter the required configuration information or click **Use Default** to accept the default values:

- **NFS Allowed Hosts**: A comma-separated list of hosts allowed to connect to the NFS export. You can also specify * to allow all hosts to connect.
  
  For example: 2001:db8:9:e54::/64, 192.0.2.0/24

- **NFS Export Options**: The NFS export options.
  
  Example: rw, sync, insecure, no_subtree_check, no_root_squash

  **Important:**

  Do not specify the fsid option.

- **Concurrent Uploads**: The number of concurrent uploads to Oracle Cloud Infrastructure.
  
  This field indicates the maximum number of files that can be concurrently uploaded in Storage Gateway. If the value is 15, the concurrent file uploads can be between 1-15.

  The allowed range is from 1 to 30.

- **Sync Policy**: The metadata operations are flushed to the disk based on the sync policy, but do not affect on-disk consistency. Currently, only **Posix Standard** is supported. Only the synchronous transactions (like fsync, ODSYNC, and OSYNC) are committed to the disk. All other transactions are handled asynchronously.

- **Cloud Read-ahead**: The number of blocks to be downloaded and used to **read ahead** when reading files for improved performance.

  Default value: 50

- **Maximum Read Cache Size in GiB**: The maximum read cache.

  When the read cache is full or reaches the configured limit, Storage Gateway removes files from the cache based on a least recently used (LRU) algorithm. Files pending upload to your tenancy are not removed from cache. You can also preserve files that you do not want removed from cache.

  **Note:**

  The number of files in cache is limited to 20,000, regardless of the specified cache size in bytes.

  See [Configuring the Cache for File Systems](#) on page 3797 for details.

  The default value depends on how you provisioned local storage before installing Storage Gateway. The recommended local storage disk size is 600 GB (500 GB for file system cache, 80 GB for metadata, 20 GB for log). If you followed the documented recommendations, the default value for the read cache is approximately 300 GB.

7. Click **Save**.

The file system is created and appears in the **File Systems** listing.

**Next Steps**

Connect the file system to a directory on the Storage Gateway host. For more information, see [Connecting a File System](#) on page 3822.

You can also do the following in the management console:

- Set up the NFS export. This directory acts as a mount point. For more information, see [Mounting File Systems on Clients](#) on page 3823.
- Add more file systems. For more information, see [Adding a File System](#) on page 3820.
- View the details of a file system. For more information, see [Viewing the Details of a File System](#) on page 3825.
Managing File Systems

A Storage Gateway file system connects a directory on a local host to an Object Storage bucket in Oracle Cloud Infrastructure. This topic describes how to manage Storage Gateway file systems.

Adding a File System

You can add file systems in Storage Gateway and connect each file system to an Object Storage bucket in your tenancy.

To add a file system

1. Log in to the management console.
2. Click File Systems on the upper-right area of the management console.
3. Click Create File System.
4. Enter the required information in Create a File System:
   - **File System Name**: A unique, friendly name for the file system. Avoid entering confidential information. Use the following guidelines when naming a file system:
     - Use from 1 to 256 characters.
     - Valid characters are letters (upper or lower case), numbers, hyphens, underscores, and periods.
     - **Important**: The name cannot contain the following:
       - A slash (/) character because this character delimits bucket and object names in Oracle Cloud Infrastructure Object Storage
       - The strings "pub" or "priv"
   
   If an Object Storage bucket by this file system name doesn’t exist in your tenancy, the bucket is created.
   
   If a corresponding Object Storage bucket by this file system name exists in your tenancy and there is data in the bucket, Storage Gateway works asynchronously to sync the bucket and file system contents.
   
   - **Select the Object Storage tier in which you want to store your data**
     - **Important**: Once set, you cannot change the storage tier in which a bucket resides.
     - You can use the Oracle Cloud Infrastructure Object Storage object lifecycle policies feature to manage the archiving and deletion of objects in a bucket according to a predefined schedule. See Using Object Lifecycle Management on page 3466 for details.
     - **Standard**: The Standard tier is the primary default Object Storage tier for storing data that requires frequent and fast access. See Overview of Object Storage on page 3392 for more information.
     - **Archive**: The Archive tier is a special tier for storing data that is accessed infrequently and requires long retention periods. See Overview of Archive Storage on page 484 for more information. Access to data in the Archive tier is not immediate since you must restore archived data before it’s accessible (see Restoring Files and Objects from Archive Storage on page 3832).
     - **Object Storage endpoint**: Required. The Object Storage API endpoint for your service instance. To find the object storage API endpoint for your Oracle Cloud Infrastructure Object Storage tenancy, see the API documentation for Oracle Cloud Infrastructure Object Storage.
     - **Important**: The following information is required to connect your Storage Gateway file systems to Oracle Cloud Infrastructure. See Required Keys and
OCIDs on page 4179 for detailed information on how to generate the required keys and where to obtain these OCIDs.

- **Compartment OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage compartment.
- **Tenant OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage tenancy.
- **User OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage user.
- **Public Key's Finger Print**: Required. Your Oracle Cloud Infrastructure Object Storage public key fingerprint.
- **Private Key**: Required. Your Oracle Cloud Infrastructure Object Storage private key.
- **Private Key Passphrase**: Required if a passphrase was specified during key creation. Your Oracle Cloud Infrastructure Object Storage private key passphrase.

**Note:**

Your private key and passphrase are securely stored in the Storage Gateway docker. The Storage Gateway installation generates a pair of public and private keys. The system uses the public key to encrypt sensitive data.

5. Click **Save**.

The values you entered must match your Oracle Cloud Infrastructure credentials. If you get an error message, verify your entries, update any incorrect values, and click **Save** again.
6. Click **Show Advanced File System Configuration**.

Enter the required configuration information or click **Use Default** to accept the default values:

- **NFS Allowed Hosts**: A comma-separated list of hosts allowed to connect to the NFS export. You can also specify * to allow all hosts to connect.
  
  For example: 2001:db8:9:e54::/64,192.0.2.0/24

- **NFS Export Options**: The NFS export options.
  
  Example: rw, sync, insecure, no_subtree_check, no_root_squash

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not specify the fsid option.</td>
</tr>
</tbody>
</table>

- **Concurrent Uploads**: The number of concurrent uploads to Oracle Cloud Infrastructure.

  This field indicates the maximum number of files that can be concurrently uploaded in Storage Gateway. If the value is 15, the concurrent file uploads can be between 1-15.

  The allowed range is from 1 to 30.

- **Sync Policy**: The metadata operations are flushed to the disk based on the sync policy, but do not affect on-disk consistency. Currently, only **Posix Standard** is supported. Only the synchronous transactions (like fsync, ODSYNC, and OSYNC) are committed to the disk. All other transactions are handled asynchronously.

- **Cloud Read-ahead**: The number of blocks to be downloaded and used to *read ahead* when reading files for improved performance.

  Default value: 50

- **Maximum Read Cache Size in GiB**: The maximum read cache.

  When the read cache is full or reaches the configured limit, Storage Gateway removes files from the cache based on a least recently used (LRU) algorithm. Files pending upload to your tenancy are not removed from cache. You can also preserve files that you do not want removed from cache.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of files in cache is limited to 20,000, regardless of the specified cache size in bytes.</td>
</tr>
</tbody>
</table>

  See **Configuring the Cache for File Systems** on page 3797 for details.

  The default value depends on how you provisioned local storage before installing Storage Gateway. The recommended local storage disk size is 600 GB (500 GB for file system cache, 80 GB for metadata, 20 GB for log). If you followed the documented recommendations, the default value for the read cache is approximately 300 GB.

7. Click **Save**.

The file system is created and appears in the **File Systems** listing.

### Connecting a File System

After you create a file system, you must connect the file system to an Oracle Cloud Infrastructure Object Storage bucket before you can store and retrieve data through the file system.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If network connectivity with Oracle Cloud Infrastructure is lost, your file system is disconnected.</td>
</tr>
</tbody>
</table>

**To connect a file system**

1. Log in to the Storage Gateway management console.
2. On the **Dashboard** tab, identify the file system that you want to connect to your Object Storage bucket.
3. Click Connect.

If a bucket with the same name as the file system exists in Object Storage, the file system is connected to that bucket. Any existing data cached in the Storage Gateway file system is deleted to ensure consistency with the data stored in the bucket. If a bucket by that name doesn’t exist, the bucket is created and the file system is connected to the bucket. If the compartment OCID was specified during file system creation, then the bucket is created in that compartment. Otherwise, the bucket is created in the root compartment by default.

**Important:**

You can mount a read/write file system on only one Storage Gateway at a time.

If the file system that you're importing is connected to another Storage Gateway, the **File System: Claim Ownership** window appears. You can claim ownership and confirm that the other Storage Gateway can be disconnected. Enter the following information, and then click **Claim Ownership**:

- Public key finger print
- Private key
- Private key passphrase

Claiming ownership ensures that you don't inadvertently connect a new file system to a bucket that's already connected to another Storage Gateway file system.

### Mounting File Systems on Clients

Each Storage Gateway file system maps a directory to an Oracle Cloud Infrastructure Object Storage bucket. To establish the connection between Storage Gateway and an NFS client, you must mount the Storage Gateway file system on the NFS client.

Any Linux/UNIX NFS client certified to work with NFSv4 server running on Oracle Linux 7.x is compatible with Storage Gateway.

**Note:**

Storage Gateway does not currently support NFS clients running on Windows or Mac OS.

### To mount a Storage Gateway file system

1. Log in to the Storage Gateway host.
2. Start Storage Gateway:

   ```
   sudo ocisg up
   ```

3. Find the NFS port number:

   ```
   sudo ocisg info
   ```

   Note the NFS port number from the output. For example:

   **Management Console:** https://myStorageGatewayHost.example.com:32775

   **If you have already configured a OCISG File System via the Management Console, you can access the NFS share using the following port.**

   **NFS Port:** 32774
Example: mount -t nfs -o vers=4, port=32774
myStorageGatewayHost.example.com:/<OCISG File System name> /local_mount_point

In the sample output:

- myStorageGatewayHost.example.com is the Storage Gateway host name.
- 32775 is the management console port number.
- 32774 is the NFS port number.

4. Log in to the NFS client from which you want to access your service instance through Storage Gateway.
5. Create a directory on the NFS client.
6. Mount the file system on the directory that you created on the NFS client:

```
sudo mount -t nfs -o vers=4, port=<NFS_port_number> <storage_gateway_host_name>:/<ocisg_file_system_name> /<local_mount_point>
```

In this command:

- Replace `<NFS_port_number>` with the NFS port number you noted earlier.
- Replace `<storage_gateway_host_name>` with the server name or IP address of the server on which Storage Gateway is installed.
- Replace `<ocisg_file_system_name>` with the file system name that you want to mount.
- Replace `<local_mount_point>` with the path to the directory you created on the NFS client.

For example:

```
sudo mount -t nfs -o vers=4, port=32774 myStorageGatewayHost.example.com:/myFirstFS /home/xyz/abc
```

In this example,

- 32774 is the NFS port.
- myStorageGatewayHost.example.com is the Storage Gateway host name.
- myFirstFS is the file system name.
- /home/xyz/abc is the path to the directory abc on the NFS client.

The Storage Gateway file system is now mounted on the NFS client directory. You can now access the Storage Gateway file system from the NFS client.

For more information, see Using Storage Gateway File Management Operations on page 3831.

**To mount a Storage Gateway file system automatically after a reboot**

You can mount a Storage Gateway NFS share either on directly to the host or remotely. When Storage Gateway restarts, the mount point may encounter residual file handle issues depending on the readiness of the fuse mount. The fuse mount takes some time to be available for a Storage Gateway restart.

Using an `/etc/fstab` entry to automount a Storage Gateway file system is **not supported**. Instead, you can set up an optional `cron` job for this purpose.

The `cron` job ensures the NFS share to be mounted only when the fuse mount is ready. However, this solution only works when the mount point is on the same Storage Gateway host. You must remount the NFS share to address file handling issues if it is mounted remotely.

1. Log in to the Storage Gateway host.
2. Create an executable script called `mountSgFilesystem.sh` and save it to an accessible location:

```
#!/bin/sh
#$1 - ip address
#$2 - nfs port
```

Oracle Cloud Infrastructure User Guide 3824
Viewing the Details of a File System

You can view the configuration details of a file system and monitor the upload activity through the management console of Storage Gateway.

To view the details of a file system

1. Log in to the management console.
2. Click the name of the file system.
   - The Details tab displays the Oracle Cloud Infrastructure service type, storage tier, and the identity domain associated with your tenancy. If the file system is connected, you can see mount point connection information to help you with mounting that file system. For example:

   **NFS Client Mount Command:** `mount -t nfs -o vers=4,port=\$1:/$3 $1:/$3 $4
break
fi
sleep 30
done`

   - The Settings tab displays the following details:
     - Details of the tenancy and scope specified for the file system.
     - File system properties.
     - NFS and cache settings for the file system.

   You can edit these settings. If you make changes, remember to click **Save**.

   If your file system is connected, you can also see:
   - The Activity tab, which shows ongoing and pending file upload activity.

   If you contact Oracle Support Services about any issue with the file system, you might need to provide the file system log to help diagnose the issue. To view or download the file system log, click **View Streaming Logs** near the lower-right corner of the Details tab.

   - The Completed Uploads tab, which shows the last 100 files that were uploaded to Oracle Cloud Infrastructure Object Storage during the current browser session.

   **Note:**

   The file list doesn’t persist across browser sessions. If you refresh the page or open the Completed Uploads tab in another browser after the files are uploaded, the list will be empty.

   - You can also disconnect the file system. See **Disconnecting a File System** on page 3826.
Changing the Properties of a File System

You can change the properties of a file system using the Storage Gateway management console.

To change the properties of a file system

1. Log in to the management console.
2. In the Dashboard, click the name of the file system that you want to edit.
3. In the Settings tab, edit the file system properties and advanced settings, such as the cache limits.
4. Click Save.
5. For the changes to take effect, disconnect and reconnect the file system.

Refreshing a File System

The auto-refresh feature triggers file system refreshes based on a time interval you specify. The system schedules the next refresh after any in-progress refresh completes. That means the elapsed time between the beginning of any two successive refreshes is equal to the specified auto-refresh interval plus the time required to run a file system refresh.

Use the following command to configure the auto-refresh feature:

```
ocisp set <file_system_name> dataset.refreshInterval=<interval_in_minutes>
```

The configuration command works on created and connected file systems. The configuration does not take effect until the file system is disconnected and reconnected or the Storage Gateway application restarts. To apply the changes, run:

```
ocisp down
cocisp up
```

Attribute caching can cause NFS clients to be unaware of files, corresponding to new objects in the bucket, that are created in a Storage Gateway file system during a refresh. You can use the noac mount option to turn off attribute caching. Turning off attribute caching can affect system performance.

When you run a refresh, the system reads attributes and fetches information about all objects in the corresponding bucket. Use a larger refresh interval for buckets with many objects.

**Note:**

After you refresh a file system, or create one for a bucket that already contains objects, Oracle recommends that you check for any files that might have been missed due to network connectivity issues.

To check for missing files, run the following command:

```
zgrep -ni "failed to get the object for" <path_to_gateway_logs>/<file_system_name>.*
```

For example, if the path to the gateway logging directory is `/ocisp/log` and the file system name is `my-fs-1`, the command is:

```
zgrep -ni "failed to get the object for" /ocisp/log/my-fs-1.*
```

Files listed in the output of this command were not successfully registered with the gateway. If any file names appear in the list, refresh the file system again.

Disconnecting a File System

When a file system is disconnected, no one can access or modify that file system.
We recommend disconnecting file systems that are not in use. Disconnecting a file system frees up the resources associated with that file system, making those resources available to file systems that are active (connected).

**To disconnect a file system**

1. Log in to the management console.
2. In the **Dashboard**, click the name of the file system that you want to disconnect.
3. Click **Disconnect**.

   When you disconnect a file system, the bucket to which the file system was previously connected and the contents of that bucket remain intact.
4. For the changes to take effect, disconnect and reconnect the file system.

You can resume storing and retrieving data by connecting the file system again. You can delete the disconnected file system when you no longer need it. For more information, see [Deleting a File System](#) on page 3828.

**Importing an Existing File System**

Before you import an existing file system from another Storage Gateway, ensure that any pending file uploads to Oracle Cloud Infrastructure Object Storage are complete.

**To import an existing file system**

1. Log in to the management console.
2. Click the **Create File System** navigation link.
3. Click **Create File System** in the navigation pane on the left.

   The **Create a File System** page appears.
4. Enter the required information in **Create a File System**.
   For the file system name, enter the name of the existing file system that you want to import to this Storage Gateway.
5. Click **Save**.
6. Select the options that you’d like to enable in the file system.
7. Click **Show Advanced** and enter the required information.
8. Click **Save**.

   The file system is created and appears on the **Dashboard** tab.
9. Click **Connect** for the file system that you want to import.

   a. If the file system that you’re importing is connected to another Storage Gateway, the **File System: Claim Ownership** window appears so you can claim ownership and confirm that the other Storage Gateway can be disconnected. Enter the following information and click **Claim Ownership**:
   
   - Public key finger print
   - Private key
   - Private key passphrase

   b. If you connect to a file system that previously belonged to a different gateway, you must restart the new owning gateway:

```
oci_sg down
oci_sg up
```
10. Mount the file system to a directory on the Storage Gateway host and set up the NFS export. For example:

```bash
sudo mount -t nfs -o vers=4,port=<NFS_port_number> <storage_gateway_host_name>:/<ocisg_file_system_name> /<local_mount_point>
```

In this command:
- Replace `<NFS_port_number>` with the NFS port number you noted earlier.
- Replace `<storage_gateway_host_name>` with the server name or IP address of the server on which Storage Gateway is installed.
- Replace `<ocisg_file_system_name>` with the file system name that you want to mount.
- Replace `<local_mount_point>` with the path to the directory you created on the NFS client.

**Deleting a File System**

You can delete a file system from Storage Gateway when you no longer need it.

**To delete a file system:**

1. Log in to the management console.
2. On the **Dashboard**, identify the file system that you want to delete.
   
   **Important:**
   When you disconnect a file system, the bucket to which the file system was previously connected and the contents of that bucket remain intact.
   Deleting a file system does not automatically delete the objects in the bucket. If you want to remove objects from the Object Storage bucket, set the **Delete Old File Versions** property for the file system and delete all the files before disconnecting the file system.

3. Ensure that the file system is disconnected. If it’s still connected, click **Disconnect**.
4. After the file system is disconnected, click its name.
   The details of the file system appear.
5. Click **Delete**.
   The file system is deleted from Storage Gateway.

**Managing Storage Gateway**

This topic describes some basic Storage Gateway management tasks.

**Managing Storage Gateway Using the CLI**

You can use the `ocisg` command line interface (CLI) to manage Storage Gateway. To use the CLI, open an `ssh` connection and log in to the host on which you installed Storage Gateway.

**Note:**
You can use the `ocisg` command line interface (CLI) to create, manage, and monitor Storage Gateway Cloud Sync jobs. See **Using Storage Gateway Cloud Sync** on page 3837 for details.

The CLI supports the following Storage Gateway management tasks:
- **To start Storage Gateway:**

  ```bash
  sudo ocisg up
  ```
• To stop Storage Gateway:

```
sudo ocisg down
```

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the server with a Storage Gateway system fails, you can reinstall and start a new one. All the configuration and system data is automatically downloaded and applied. The pending upload and download activities resume when the new Storage Gateway system runs.</td>
</tr>
<tr>
<td>If a disk cache is unrecoverable on the Storage Gateway server, data might be lost since the file might not have been transferred to the bucket in your tenancy. To ensure efficient data protection, see Best Practices for Using Storage Gateway on page 3842.</td>
</tr>
</tbody>
</table>

• To view details about Storage Gateway and how to access the management console:

```
sudo ocisg info
```

• To find the version of Storage Gateway:

```
sudo ocisg version
```

• To configure Storage Gateway to use a proxy server for connections to Oracle Cloud Infrastructure Object Storage:

```
sudo ocisg configure proxy <proxy_server_URL>
```

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>After configuring the proxy server, you must stop and restart Storage Gateway.</td>
</tr>
</tbody>
</table>

By default, no proxy server is specified.

• To remove previously configured proxy server details in Storage Gateway:

```
sudo ocisg configure proxy [remove]
```

• To configure Storage Gateway to use SSL when communicating with the management console and REST APIs:

```
sudo ocisg configure ssl true
```

SSL is enabled by default.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>After configuring Storage Gateway to use SSL, you must stop and restart Storage Gateway.</td>
</tr>
</tbody>
</table>

To disable SSL:

```
sudo ocisg configure ssl false
```
To specify ports for the Storage Gateway services:

```bash
sudo ocisg configure port <service> <port_number>
```

- `<service>`: Specify `admin`, `nfs`, or `rest`.
- `<port_number>`: Ensure that the port number you specify is not already in use on the Storage Gateway host.

By default, the port number is assigned dynamically for the Storage Gateway services when you start Storage Gateway.

**Note:**
For the port assignment to take effect, you must stop and start Storage Gateway.

To remove the static port assignment for a service:

```bash
sudo ocisg configure port <service> remove
```

To allocate memory for the Storage Gateway host:

```bash
sudo ocisg configure memory <memory_in_GB>
```

To remove the memory allocation:

```bash
sudo ocisg configure memory remove
```

By default, Storage Gateway uses 4 GB of the available memory on the host server. You can delete the memory information by using the `remove` parameter.

**Note:**
After configuring memory for Storage Gateway, you must stop and restart Storage Gateway.

To specify the docker network mode:

```bash
sudo ocisg configure network mode
```

The mode can be either `host` or `bridge`.

The default mode is `bridge`. In this mode, you can run multiple instances of Storage Gateway on your host.

In the `host` mode, you can run only a single instance of Storage Gateway. Network performance is better in `host` mode.

**Note:**
After specifying the docker network mode, you must stop and restart Storage Gateway.

To change the Storage Gateway admin password:

```bash
sudo ocisg do password:reset
```

Set a new password:

```bash
sudo ocisg password:set <new_password>
```

Enter a password that meets the following requirements:

- Uses from 8 to 32 characters.
- Includes at least one special character, one numerical character, one uppercase character, and one lowercase character.
• To view help for the available commands:
  
  `sudo ocisg help`

**Using Storage Gateway File Management Operations**

This topic describes how to use the Storage Gateway file management operations.

**Important:**

Exercise caution when using the REST API, Java library, or any other client to retrieve, create, update, or delete objects directly in a bucket that’s mapped to a file system in Storage Gateway. Until you **Refresh** the Storage Gateway file system, Storage Gateway is not aware of the changes and data is inconsistent between Storage Gateway and Object Storage.

**Uploading Files to Buckets**

Before you connect the file system to the Oracle Cloud Infrastructure Object Storage bucket, make a note of the Oracle Cloud Infrastructure Object Storage tenancy details such as namespace, tenant OCID, and compartment OCID.

Copy the files to the mounted directory on the Storage Gateway or the NFS client host. Storage Gateway writes the files to the disk cache. The system queues and asynchronously uploads the files to an Object Storage bucket. Corresponding objects are created in the storage tier you specified during file system creation, either **Standard** or **Archive**. See Creating Your First File System on page 3816 or Managing File Systems on page 3820 for details.

**Note:**

Storage Gateway automatically performs multipart upload for files larger than 128 MB. See Using Multipart Uploads on page 3477 for details.

You can view files uploaded to your tenancy during the current browser session. See the **Completed Uploads** tab in Viewing the Details of a File System on page 3825.

**Reading Files**

When you write a file to a Storage Gateway file system, the system stores the file in the local disk cache. You can read the file directly from the mounted directory. Storage Gateway asynchronously copies the file to the corresponding Object Storage bucket in your tenancy. To retrieve the data from the bucket using Storage Gateway, read the files from the mounted directory.

If space is available, Storage Gateway automatically places the files in the read cache. If the file is in the read cache, you can retrieve the file immediately. If the file is not available in the read cache and it is stored in the **Archive** tier, you must restore the object. For more information, see Restoring Files and Objects from Archive Storage on page 3832.

**Note:**

You cannot read or write to a file that is stored in the **Archive** tier and does not exist in the read cache. This action returns an Input/Output error.

Storage Gateway checks data integrity using checksum verification on uploads. The system might not be able to perform data integrity validation on a partial read, since checksum verification works only on a whole file or object.

To read the upload checksum for a file in a file system, run the following command from the NFS client on which the file system is mounted:

```
sudo docker exec ocisg bash -c "cd /mnt/gateway/${filesystem} && cat ${filepath}:::meta:csm"
```
Restoring Files and Objects from Archive Storage

You can initiate a file restore from the Storage Gateway command line. You can also initiate an object restore from Archive Storage in Oracle Cloud Infrastructure. You can read the corresponding file using Storage Gateway after the object has been restored to Object Storage.

Note:

Storage Gateway supports Oracle Cloud Infrastructure Object Storage object lifecycle policies to manage the archiving and deletion of objects in a bucket according to a pre-defined schedule. Using object lifecycle policies, you can specify bucket creation in the Standard Object Storage tier, and then create a policy to schedule the subsequent movement of data to the Archive Storage tier. This lifecycle policy archival method is useful if you have on-premises applications that generate intermediary or temporary files and directories that are inappropriate for immediate archival. See Using Object Lifecycle Management on page 3466 for details.

Restoring Archived Files Using the Storage Gateway Command Line

To restore one or more archived files

Open a command prompt on the Storage Gateway host and run the `ocisg archive restore` command. Specify the full path to a directory or to a file.

```
ocisg archive restore <file_system_name> <full/path/to/directory/or/file> [<#_of_hours>]
```

By default, the file remains restored for 24 hours after restoration. However, you can optionally specify `[<#_of_hours>]` with an integer value of from 1 to 240 hours.

For example, to restore all the files in a directory:

```
ocisg archive restore myFS myDir/mySubDir 240
```

For example, to restore a single file:

```
ocisg archive restore myFS myDir/mySubDir/file2 240
```

To check the archive status of one or more files

You can get the archive status for all files in a file system, for all files in a directory, or for an individual file.

Open a command prompt on the Storage Gateway host and run the `ocisg archive restore-status` command.

```
ocisg archive restore-status <file_system_name> [<full/path/to/directory/or/file>]
```

The status can be one of the following:

- Archived
- In progress
- Restored

For example, to check the archive status for all files in a file system:

```
ocisg archive restore-status myFS
```
To check the archive status for all files in directory:

```
ocissg archive restore-status myFS myDir/mySubDir
```

To check the archive status for an individual file:

```
ocissg archive restore-status myFS myDir/mySubDir/file2
```

To check the restoration job status for a file system

You can get the status for all restoration jobs that have been initiated for a file system.

Open a command prompt on the Storage Gateway host and run the `ocissg archive restore-jobs` command.

```
ocissg archive restore-jobs <file_system_name>
```

For example:

```
ocissg archive restore-jobs myFS
```

### Restoring Archived Files Using Oracle Cloud Infrastructure

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Oracle Cloud Infrastructure to restore archived objects, use the Refresh operation in Storage Gateway to display the data that was added or modified directly in Object Storage.</td>
</tr>
</tbody>
</table>

To restore an archived object using the Oracle Cloud Infrastructure Console

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You need OBJECT_RESTORE permissions to restore Archive Storage objects.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Choose the compartment your bucket is in.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click **Objects** under **Resources**.
   A list of folders (if enabled) and objects in the bucket are displayed.
5. Expand any folders and subfolders as needed to locate the object that you want to restore.
6. To restore a single object, click the Actions icon (three dots) to the right of the object you want to restore, and then click **Restore**. To restore multiple objects, select the check boxes to the left of each object you want to restore, then click **Restore**.
7. Optionally, specify the **Time Available for Download in Hours**.
   By default, you have 24 hours to download an object after restoration. However you can alternatively specify a download time of from 1 to 240 hours. You can find out how much download time is remaining by looking at **Available for Download** in object Details or by looking at the Actions icon (three dots) menu to the right of **Download**. Refresh the browser to obtain up-to-date remaining download time information.
   After the allotted download time expires, the object returns to Archive Storage.
8. Click **Restore Objects**.
   Error messages are generated if there is a problem with restoring the selected objects. You can optionally click **Retry failed restore option**.
Storage Gateway

**To check the status of an object restoration using the Oracle Cloud Infrastructure Console**

1. Open the navigation menu. Under Core Infrastructure, click Object Storage.
2. Choose the compartment your bucket is in.
   A list of buckets is displayed.
3. Click the bucket name that contains your object.
4. Click Objects under Resources.
   A list of objects in the bucket is displayed.
5. Click the Actions icon (three dots) to the right of the object you want to check the restoration or download status of, then click Details.
6. Check the Status.
   Status displays one of the following:
   - Archived
   - Restoring
   - Restored

**To restore an archived object using the Oracle Cloud Infrastructure CLI**

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You need OBJECT_RESTORE permissions to restore Archive Storage objects.</td>
</tr>
</tbody>
</table>

```
oci os object restore --namespace <object_storage_namespace> --bucket-name <archive_bucket_name> --name <archived_object_name> [--hours <#_of_hours>]
```

By default, you have 24 hours to download an object after restoration. However, you can optionally specify --hours with an integer value of download time of from 1 to 240 hours.

**To check the status of an object restoration using the Oracle Cloud Infrastructure CLI**

```
oci os object restore-status --namespace <object_storage_namespace> --bucket-name <archive_bucket_name> --name <archived_object_name>
```

**Deleting Files**

Remove the files that you no longer need from the NFS client by deleting them from the directory on which the file system is mounted.

**Monitoring Storage Gateway**

This topic describes how to monitor Storage Gateway file system upload activity, system health, and storage usage. The topic also describes how to view system notifications and how to receive notifications in email.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring file system activity in the Storage Gateway management console consumes system resources. Monitoring file system activity is not recommended when Storage Gateway is under high load.</td>
</tr>
</tbody>
</table>

**Monitoring Upload Activity**

When you upload a file to a file system, you can view the status of the upload activity. The Activity tab shows the ongoing and pending upload activity in a file system.
To monitor upload activity

1. Log in to the management console.
2. Click File Systems in the upper-right corner of the management console.
3. On the File Systems page, select a file system.
4. Click Activity.

You can see the upload progress of the file in the Uploading pane.

Monitoring System Health Status

You can monitor the overall system health status using System Status on the right side of the management console.

Storage Gateway performs an automated "health check" on the system to monitor the status of:

- Storage Gateway resources and services.
- Local storage, file system cache, metadata storage, and log storage.

System Status shows the result of Storage Gateway health analysis, either Healthy or Unhealthy.

System Status also provides information on:

- Any system warnings or errors.
- Local I/O Mode, which depends on local disk usage:
  - Normal
    The available disk space is greater than 10 GB in Storage Gateway. You can upload files in Storage Gateway and upload them to your Oracle Cloud Infrastructure tenancy.
  - Rejecting I/O
    The available disk space is less than 10 GB in Storage Gateway. Storage Gateway runs in protection mode and does not allow any writes to its local disk. All read operations work normally. All Storage Gateway metadata operations fail except for deletions and truncation.
    To return to Normal mode, you must wait until all ongoing upload activities complete and the files are removed from the read cache.
  - Throughput
    The approximate upload throughput to Object Storage. If there is no recent activity, Throughput shows Idle.
  - Available Read Cache
    The amount of read cache available. For optimal performance, reliability, and fault tolerance, follow the guidelines for configuring cache storage. See Configuring Local Storage for File Systems and Cache on page 3798 for details.
  - Pending Uploads
    The number of files or directories, for all file systems, awaiting upload to Object Storage. If Pending Uploads is 0 (zero), all files and directories have been uploaded.

Monitoring Storage Usage

You can track the storage usage and availability.

To monitor storage usage

1. Log in to the management console.
2. Click System in the upper-right corner of the management console.
3. Click **System Stats**.

   The system data appears in three panes:
   
   • **Local Storage**
   • **Local I/O**
   • **Local Resources**

**Local Storage**

This pane provides a graphical representation of the amount of storage being used and the available free storage on the Storage Gateway host. You can see:

• Available local storage.
• Storage used for pending uploads and preserved cache files.
• Storage used for metadata.
• Storage used for logging.
• Storage used for other applications.

**Local I/O**

This pane displays the local I/O mode of Storage Gateway based on the local disk space usage on the Storage Gateway host.

**Local Resources**

This pane shows the overall memory usage and availability for Storage Gateway from the following fields:

• **Available Cores**: The number of CPUs being used by Storage Gateway.
• **Maximum Memory Available to Storage Gateway**: The total RAM available for Storage Gateway.
• **Memory Used by Storage Gateway**: The amount of memory being used by the file systems in Storage Gateway.
• **Free Memory**: The amount of free RAM available in Storage Gateway host.

**Viewing System Notifications**

The **System Notifications** tab shows system notifications and helps you track overall system performance.

**To view system notifications**

1. Log in to the management console.
2. Click **System** in the upper-right corner of the management console.
3. Click **System Notifications**.

   You can view a list of warnings or critical system notifications.

**Configuring Email Notification**

You can configure Storage Gateway to notify you by email about system health and Cloud Sync job completion.

**To configure email notification**

1. Log in to the management console.
2. Click **System** in the upper-right corner of the management console.
3. Click **System Notifications**.
4. If email notifications are not yet configured, click **Click here to configure**.
5. Enter the required information for the following fields:
   
   • SMTP server.
   • Email addresses to receive notifications.
6. Click **Show Advanced Options** and enter the required information in the advanced configuration fields:
   - SMTP port.
   - SMTP User name.
   - SMTP Password.
   - Sender’s Email Address.

   The default value is: noreply@oracle.com

7. Click **Save**.

8. Click **Test Email Notification** to verify that the specified email address receives a system notification email.

**Using Storage Gateway Cloud Sync**

Use Cloud Sync to move on-premises datasets from a local NFS-mounted file system to Storage Gateway, where the data is then moved asynchronously to Oracle Cloud Infrastructure Object Storage. You can also use Cloud Sync to synchronize Storage Gateway file system changes back to the local file system.

Cloud Sync generates the following for each sync job:

- Sync status (Created, Running, Completed, Failed, or Canceled).
- Number of files and directories to be copied from the source to the target.
- File and directory upload progress.
- Number of files and directories uploaded to the target.
- Time the job started, the time the job ended, and the run duration.
- The number of files skipped. (Cloud Sync skips non-regular files, such as symlinks, in the source directory.)
- A list of skipped files.

You can use the Storage Gateway management console or the command line interface (CLI) to create, manage, and monitor Cloud Sync jobs.

**About Cloud Sync**

Cloud Sync is an enhanced wrapper around the Linux `rsync` command and relies on `rsync` to detect new and changed files using size and modification time. Cloud Sync also relies on `rsync` to verify the files once the data transfer is complete using checksums of the files. Cloud Sync calls the Storage Gateway diagnostic commands to provide detailed data movement progress and status between your local server, Storage Gateway, and Oracle Cloud Infrastructure.

**Understanding Failure Behavior**

Because the file system is mounted over NFS locally, the NFS client running on the host handles any issues resulting from file system availability or connectivity.

Cloud Sync does the following:

- Reports and logs any failures to list or copy specific files (for example, resulting from permission issues).
- Monitors and reports on the pending and completed uploads to Object Storage.

Storage Gateway handles any connectivity and access issues to Object Storage and performs retry operations as needed.

**Prerequisites for Cloud Sync**

- Create the Storage Gateway file system that serves as either the source or target destination for the sync operation. A file system on the Storage Gateway host maps to a bucket with an identical name in Oracle Cloud Infrastructure Object Storage. See Creating Your First File System on page 3816 or Adding a File System on page 3820 for details.
- Obtain the proper credentials to mount the file system share from the local server.
The local server source must:

- Have names services set up correctly so that UIDs and GIDs are preserved and are not remapped to nobody.
- Be exported with root permissions to read and traverse the entire source tree.
- The filesystem to be synced needs to be NFS mounted to a mount point under `/cloudsync/mounts/`

### Important:

If a Storage Gateway file system serves as the source, set the auto-refresh for new objects in the bucket to be synced using CloudSync. Use the following command to set the file system refresh at regular intervals:

```
ocisg set file_system_name
    dataset.refreshInterval=interval_in_minutes
```

Restart Storage Gateway, then run the following commands to apply the changes:

```
ocisg down
ocisg up
```

See [Managing File Systems](#) on page 3820 for more information.

## Using the Management Console

You can use the Storage Gateway management console to create, manage, and monitor Cloud Sync jobs.

**To create a Cloud Sync job that syncs all files and directories at the specified source location**

1. Log in to the management console.
2. Click **Cloud Sync** in the upper-right corner of the management console.

   By default, a list of all the Cloud Sync jobs that have already been created is displayed.

3. Click **Create Cloud Sync Job**.
4. In **Create Cloud Sync Job** page, specify the attributes of the job:
   - **Job Name**: Required. A unique, user-friendly name for the job. Avoid entering confidential information.
   - **Source Path**: Path to the Cloud Sync source directory containing the files to sync.
     - If you are syncing a local file system to Oracle Cloud Infrastructure, specify the source path as:
       ```plaintext
       /cloudsync.mounts/<user_mount>[/<path_to_directory>]
       ```
     - If you are syncing Oracle Cloud Infrastructure to a local file system, specify the source path as:
       ```plaintext
       <storage_gateway_file_system>/<path_to_directory>
       ```
   - **Target Path**: Path to the Cloud Sync target directory for the synced files.
     - If you are syncing a local file system to Oracle Cloud Infrastructure, specify the target path as:
       ```plaintext
       <storage_gateway_file_system>/<path_to_directory>
       ```
     - If you are syncing Oracle Cloud Infrastructure to a local file system, specify the target path as:
       ```plaintext
       /cloudsync.mounts/<user_mount>[/<path_to_directory>]
       ```
   - **Enable Auto-Deletion**: Enable this option if you want Cloud Sync to automatically delete files from the target when:
     - Files are deleted from the source.
     - Source files have been renamed.
     
     By default, when a file is deleted on the source, Cloud Sync does not automatically delete the file on the target unless you enable **Enable Auto-Deletion**. Also, when a source file is renamed, the file with the old name is deleted and a file with the new name is created. By default, Cloud Sync does not delete the file with the old name on the target (retaining both a file with the old name and a file with the new name) unless you choose **Enable Auto-Deletion**.
     
     The names of all deleted files are stored in a job-specific log directory.

5. Click **Create Cloud Sync Job**.

A Cloud Sync job is created and displayed in the list of jobs.

**To list Cloud Sync jobs**

1. Log in to the management console.
2. Click **Cloud Sync** in the upper-right corner of the management console.
   
   By default, a list of all the Cloud Sync jobs is displayed.
3. Optionally, you can filter the job listing by status (Created, Running, Completed, Failed, or Canceled) and type of Cloud Sync job (upload or download) by clicking one of the **Quick Filters**.

**To run a Cloud Sync job**

1. Log in to the management console.
2. Click **Cloud Sync** in the upper-right corner of the management console.
3. In the list of jobs, find the Cloud Sync job that you want to run.
4. Click **Run** to the right of the job name.

Cloud Sync runs the job. The management console displays the status of the job just below the job name.

**To get the status of a Cloud Sync job**

1. Log in to the management console.
2. Click **Cloud Sync** in the upper-right corner of the management console.
3. In the list of jobs, find the Cloud Sync job for which you want status.

   The management console displays the status of the job (Created, Running, Completed, Failed, or Canceled) just below the job name.

**To cancel a Cloud Sync job**

You can only cancel a job if it is running.

1. Log in to the management console.
2. Click **Cloud Sync** in the upper-right corner of the management console.
3. In the list of jobs, find the Cloud Sync job that you want to cancel.

   **Tip:**
   
   Use **Quick Filters** to get a list of **Running** jobs.

4. Click **Cancel** to the right of the job name.

**To delete a Cloud Sync job**

You cannot delete a running job.

1. Log in to the management console.
2. Click **Cloud Sync** in the upper-right corner of the management console.
3. In the list of jobs, find the created, canceled, or failed Cloud Sync job that you want to delete.
4. Click **Delete** to the right of the job name.

**Using the CLI**

You can use the `ocisg` command line interface (CLI) to create, manage, and monitor Cloud Sync jobs. Using `ssh`, log in to the host on which you installed Storage Gateway to use the CLI.

**To create a Cloud Sync job that syncs all files and directories at the specified source location**

Open a command prompt and run `ocisg cloudsync create` to create a job:

```bash
```

--schedule is an option to automate the Cloud Sync job so it runs according to the specified schedule. Set the schedule value using the format used for cron jobs. For example, `--schedule="*/5 * * * *"` runs the job every five minutes.

--auto-delete is an option to direct Cloud Sync to automatically delete files from the target when files are deleted from the source, and old names of files that have been renamed. By default, Cloud Sync does not automatically delete the files on the target unless you specify this option. The names of all deleted files are stored in a job-specific log directory.

--parallel=<number> is an option to specify the number of processes for data synchronization. By default, the number of processes is set to one. With a single process using a hard disk drive, you can expect a sync rate of 60-70 MB/s. If your system has higher disk throughput, you can use the number of processes that is proportional to the available bandwidth. Oracle recommends from two to five processes for optimal performance. The maximum number of processes allowed is 10.

--files-from=<file> is an option to specify a set of files that you want to sync to the target. If you do not set this option, the service syncs all files. The `<file>` should be a file under the `/cloudsync/` directory. For example, `--files-from="/cloudsync/files.list"`. 
--exclude-from=<file> is an option to specify a set of files that you want to exclude from the Cloud Sync job. The <file> should be a file under the /cloudsync/ directory. For example, `--exclude-from="/cloudsync/exclude.list"`.

--verify-contents is an option to enable verification of the destination contents against the source. If you do not explicitly enable verification, new files added to Cloud Sync sources after the job has started are not reported as errors when they do not appear in the destination.

Avoid entering confidential information.

The Cloud Sync job is created and displayed in the list of jobs.

**To list Cloud Sync jobs**

Open a command prompt and run `ocisg cloudsync list` to list jobs:

```
sudo ocisg cloudsync list [-s <status>] [<job_name_or_type>]
```

Optionally, you can filter the list of jobs by specifying job status (Created, Running, Completed, Failed, or Canceled). You can also list a single job by specifying the name of that job.

For example:

```
sudo ocisg cloudsync list sync_to_os1
```

**To run a Cloud Sync job**

Open a command prompt and run `ocisg cloudsync run` to run a job:

```
sudo ocisg cloudsync run <job_name>
```

For example:

```
sudo ocisg cloudsync run sync_to_os1
```

**To get the status of a Cloud Sync job**

Open a command prompt and run `ocisg cloudsync status` to get the status of a job:

```
sudo ocisg cloudsync status <job_name>
```

For example:

```
sudo ocisg cloudsync status sync_to_os1
```

**To cancel a Cloud Sync job**

You can cancel a job only if the job is in progress.

Open a command prompt and run `ocisg cloudsync cancel` to cancel a job:

```
sudo ocisg cloudsync cancel <job_name>
```

For example:

```
sudo ocisg cloudsync cancel sync_to_os1
```

**To delete a Cloud Sync job**

Open a command prompt and run `ocisg cloudsync delete` to delete a job:

```
sudo ocisg cloudsync delete <job_name>
```
For example:

```
sudo ocisg cloudsync delete sync_to_os1
```

### Best Practices for Using Storage Gateway

Apply the recommendations found in the following topics to optimize the manageability, performance, reliability, and security of your Storage Gateway.

- [Security Considerations](#) on page 3793
- [Understanding Storage Gateway Performance](#) on page 3803
- [Configuring Local Storage for File Systems and Cache](#) on page 3798
- [Determining File System Cache Size](#) on page 3798
- [Recommended Uses and Workloads](#) on page 3792
- [Uses and Workloads Not Supported](#) on page 3792
- [Renaming Directory Trees](#)
- [Limits on Storage Gateway Resources](#) on page 3794

### Troubleshooting Storage Gateway

This topic covers some common Storage Gateway issues and how to address them.

**I installed docker and NFS on my host, but I can’t install Storage Gateway**

1. Add the docker group to the existing groups in your host:
   ```
sudo groupadd docker
   ```
2. Add your user id to the docker group:
   ```
   usermod -a -G docker <username>
   ```
3. Shut down your host:
   ```
   shutdown -r now
   ```
4. Log in to your host and run the Storage Gateway installation script:
   ```
   sudo ./ocisg-install.sh
   ```

**I can’t access the management console**

1. Run the `ocisg info` command:
   ```
   sudo ocisg info
   ```
   If Storage Gateway is not running, start Storage Gateway:
   ```
   sudo ocisg up
   ```
2. Make a note of the management console port number from the output:
   ```
   Management Console: https://myStorageGatewayHost.example.com:32775
   ```
   If you have already configured a OCISG File System via the Management Console, you can access the NFS share using the following port.
   ```
   NFS Port: 32774
   ```
Example: `mount -t nfs -o vers=4,port=32774 myStorageGatewayHost.example.com:/<OCISG File System name> / local_mount_point`

In the example, `myStorageGatewayHost.example.com` is the Storage Gateway host name and 32775 is the management console port number.

3. Ensure that Storage Gateway is running `docker` on the Storage Gateway host.
4. Check that the management console port number in the output from `ocisg info` matches the port you’re using to access the management console.
5. Ensure that you are using `https` if you have enabled SSL. SSL is enabled by default.

I am unable to mount a file system

1. Run the `ocisg info` command:

   `sudo ocisg info`

   If Storage Gateway is not running, start Storage Gateway:

   `sudo ocisg up`

2. Make a note of the management console port number and NFS port number from the output:

   Management Console: https://myStorageGatewayHost.example.com:32775

   If you have already configured a OCISG File System via the Management Console, you can access the NFS share using the following port.

   NFS Port: 32774
Example: mount -t nfs -o vers=4,port=32774
myStorageGatewayHost.example.com:/<OCISG File System name> /local_mount_point

In the sample output:
• myStorageGatewayHost.example.com is the Storage Gateway host name.
• 32775 is the management console port number.
• 32774 is the NFS port number.
• Log in to the NFS client from which you want to access your service instance through Storage Gateway.
• Create a directory on the NFS client.
• Mount the file system on the directory that you created on the NFS client:

```
sudo mount -t nfs -o vers=4,port=<NFS_port_number> <storage_gateway_host_name>:/<ocisg_file_system_name> /<local_mount_point>
```

In this command:
• Replace `<NFS_port_number>` with the NFS port number.
• Replace `<storage_gateway_host_name>` with the server name or IP address of the server on which Storage Gateway is installed.
• Replace `<ocisg_file_system_name>` with the name of the file system you want to mount.
• Replace `<local_mount_point>` with the path to the directory you created on the NFS client.

For example:

```
sudo mount -t nfs -o vers=4,port=32774
myStorageGatewayHost.example.com:/myFirstFS /home/xyz/abc
```

In this example,
• 32774 is the NFS port number.
• myStorageGatewayHost.example.com is the Storage Gateway host name.
• myFirstFS is the file system name.
• /home/xyz/abc is the path to the directory abc on the NFS client.
• Ensure that Storage Gateway is running `docker` on the Storage Gateway host.
• Ensure that the NFS protocol is running:

```
sudo systemctl enable nfs-server
```

• Check that the NFS port number in the output from `ocisg info` matches the port you’re using to connect to with your NFS client.

### I cannot delete a bucket after canceling a Cloud Sync job

If you cancel an active or stalled Cloud Sync job and disconnect the file system, you might not be able to delete the associated Object Storage bucket. If file uploads were in progress when you canceled the job, the Object Storage service might expect a commit that never completed. In this case, the service does not allow bucket deletion and returns the error "multipart upload pending". You can use the CLI to resolve the issue.

1. List the bucket’s pending multipart uploads:

```
oci os multipart list -bn <bucket_name>
```

Be sure to note the relevant object names and upload IDs.
2. Delete all pending uploads:

   ```sh
   oci os multipart abort -bn <bucket_name> --object-name <object_name> --upload-id <upload_id>
   ```

3. Delete the bucket:

   ```sh
   oci os bucket delete -ns <object_storage_namespace> --name <bucket_name>
   ```

### Additional NFS Troubleshooting

The Storage Gateway installation software installs the NFS, if needed, and automatically configures it. After the installation, the NFS is configured and a file system created. You can then mount the filesystem from a remote client. Sometimes this mount can fail.

To troubleshoot a mount failure:

1. Ensure that the NFS port is included in the Storage Gateway's subnet security list and that it is available there. If the port does not appear in the subnet security list, add it and retry the mount.
2. Run `rpcinfo -p`. The command should return:

   ```
   100003 4 tcp 2049 nfs
   ```

   This result means that NFS is ready, available, and the mount succeeds.
3. If `nfs` does not appear in the response to the `rpcinfo -p` command, enable and restart both `rpcbind` and `NFS`:

   ```
   sudo systemctl enable rpcbind
   sudo systemctl enable nfs
   sudo systemctl start rpcbind
   sudo systemctl start nfs
   ```

4. Run the `rpcinfo -p` command again to verify that NFS is now available.
   
   a. If NFS still is not available, reboot the Storage Gateway.
   b. Run the `rpcinfo -p` command again to confirm.
5. If you remain unable to mount the file system, contact My Oracle Support.

### Contacting Oracle Support

If you need technical support or help with Storage Gateway, you can go to My Oracle Support and create a service request. See Creating a Service Request Using the Console on page 126 for information.

### Upgrading Storage Gateway

Storage Gateway notifies you when there is a new version available for you to download and install:

- A pop-up notification appears in the management console after you log in.
- A small banner notification appears at the top of the Dashboard.
- If you have configured email notifications, the system sends an email notification. See Configuring Email Notification on page 3836 for details.

**Important:**

If you are upgrading from Storage Gateway 1.0, underlying database and schema changes require you to recreate your Storage Gateway file systems. See Recreating Your File Systems on page 3846 for details.
Before You Begin

- Plan for downtime appropriately since the upgrade takes some time to complete. The downtime varies depending on the system resources, the number of file systems, and the number of files.
- Wait for any pending or ongoing write operations from the NFS client instances to complete, then unmount all file systems.
- Wait for pending uploads to Oracle Cloud Infrastructure Object Storage to complete. On the Dashboard under System Status, ensure that the Pending Uploads field shows 0.
- Disconnect all of the file systems.
- Ensure that there is no ongoing activity in the Activity tab for each file system in the management console.

Important:

To enable partial update capabilities in Storage Gateway, there must be no pending uploads for any associated file systems before the upgrade. The upgrade process purges the existing local cache across all Storage Gateway file systems.

Upgrading Storage Gateway

To upgrade to Storage Gateway 1.3

1. Log in to your Storage Gateway host.
2. Download the Storage Gateway 1.3 tar archive.
3. Extract the files from the downloaded ocisg-1.3.tar.gz file:

```bash
  tar xzvf ocisg-1.3.tar.gz
```

This command extracts the file's contents to a subdirectory named ocisg-1.3.
4. Change directory to ocisg-1.3:

```bash
  cd ocisg-1.3
```
5. Run the installation script as sudo or root user:

```bash
  sudo ./ocisg-install.sh
```

If you encounter any interruption during the upgrade, such as lost connectivity, rerun the installation script to resume the upgrade.

If you are upgrading from Storage Gateway 1.0, you must recreate the file systems that were created in the 1.0 version of the Storage Gateway software. Connect the file systems in the management console and claim ownership if there’s a bucket ownership prompt. Storage Gateway version 1.3 rebuilds the local metadata for existing buckets in Object Storage. The more objects there are in the buckets, the more time it takes to rebuild the metadata.

Recreating Your File Systems

When you created file systems in Storage Gateway 1.0, corresponding Oracle Cloud Infrastructure Object Storage buckets were created. Recreate those file systems in Storage Gateway so that you can connect to the same buckets and automatically see the files that have already been uploaded to Object Storage.

When you recreate Storage Gateway file systems, data that you already uploaded to Oracle Cloud Infrastructure Object Storage is automatically included in the newly created file system.

To recreate your file systems

1. Log in to the management console.
2. Click File Systems on the upper-right area of the management console.
3. Click Create File System.
4. Enter the required information in **Create a File System**:

- **File System Name**: A unique, friendly name for the file system. Avoid entering confidential information. Use the following guidelines when naming a file system:
  - Use from 1 to 256 characters.
  - Valid characters are letters (upper or lower case), numbers, hyphens, underscores, and periods.

**Important:**

The name **cannot** contain the following:

- A slash (/) character because this character delimits bucket and object names in Oracle Cloud Infrastructure Object Storage
- The strings "pub" or "priv"

If an Object Storage bucket by this file system name doesn’t exist in your tenancy, the bucket is created.

If a corresponding Object Storage bucket by this file system name exists in your tenancy and there is data in the bucket, Storage Gateway works asynchronously to sync the bucket and file system contents.

- **Select the Object Storage tier in which you want to store your data**

**Important:**

Once set, you cannot change the storage tier in which a bucket resides.

You can use the Oracle Cloud Infrastructure Object Storage object lifecycle policies feature to manage the archiving and deletion of objects in a bucket according to a predefined schedule. See Using Object Lifecycle Management on page 3466 for details.

- **Standard**: The Standard tier is the primary default Object Storage tier for storing data that requires frequent and fast access. See Overview of Object Storage on page 3392 for more information.
- **Archive**: The Archive tier is a special tier for storing data that is accessed infrequently and requires long retention periods. See Overview of Archive Storage on page 484 for more information. Access to data in the Archive tier is not immediate since you must restore archived data before it’s accessible (see Restoring Files and Objects from Archive Storage on page 3832).

- **Object Storage endpoint**: Required. The Object Storage API endpoint for your service instance. To find the object storage API endpoint for your Oracle Cloud Infrastructure Object Storage tenancy, see the API documentation for Oracle Cloud Infrastructure Object Storage.

**Important:**

The following information is required to connect your Storage Gateway file systems to Oracle Cloud Infrastructure. See Required Keys and OCIDs on page 4179 for detailed information on how to generate the required keys and where to obtain these OCIDs.

- **Compartment OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage compartment.
- **Tenant OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage tenancy.
- **User OCID**: Required. Unique identifier of your Oracle Cloud Infrastructure Object Storage user.
- **Public Key's Finger Print**: Required. Your Oracle Cloud Infrastructure Object Storage public key fingerprint.
- **Private Key**: Required. Your Oracle Cloud Infrastructure Object Storage private key.
- **Private Key Passphrase**: Required if a passphrase was specified during key creation. Your Oracle Cloud Infrastructure Object Storage private key passphrase.

**Note:**

Your private key and passphrase are securely stored in the Storage Gateway docker. The Storage Gateway installation generates a pair
Storage Gateway

5. Click Save.

The values you entered must match your Oracle Cloud Infrastructure credentials. If you get an error message, verify your entries, update any incorrect values, and click Save again.

6. Click Show Advanced File System Configuration.

Enter the required configuration information or click Use Default to accept the default values:

- **NFS Allowed Hosts**: A comma-separated list of hosts allowed to connect to the NFS export. You can also specify * to allow all hosts to connect.
  
  For example: 2001:db8:9:e54::/64, 192.0.2.0/24

- **NFS Export Options**: The NFS export options.
  
  Example: rw, sync, insecure, no_subtree_check, no_root_squash

  **Important:**

  Do not specify the fsid option.

- **Concurrent Uploads**: The number of concurrent uploads to Oracle Cloud Infrastructure.
  
  This field indicates the maximum number of files that can be concurrently uploaded in Storage Gateway. If the value is 15, the concurrent file uploads can be between 1-15.
  
  The allowed range is from 1 to 30.

- **Sync Policy**: The metadata operations are flushed to the disk based on the sync policy, but do not affect on-disk consistency. Currently, only Posix Standard is supported. Only the synchronous transactions (like fsync, ODSYNC, and OSYNC) are committed to the disk. All other transactions are handled asynchronously.

- **Cloud Read-ahead**: The number of blocks to be downloaded and used to read ahead when reading files for improved performance.
  
  Default value: 50

- **Maximum Read Cache Size in GiB**: The maximum read cache.
  
  When the read cache is full or reaches the configured limit, Storage Gateway removes files from the cache based on a least recently used (LRU) algorithm. Files pending upload to your tenancy are not removed from cache. You can also preserve files that you do not want removed from cache.

  **Note:**

  The number of files in cache is limited to 20,000, regardless of the specified cache size in bytes.

See Configuring the Cache for File Systems on page 3797 for details.

The default value depends on how you provisioned local storage before installing Storage Gateway. The recommended local storage disk size is 600 GB (500 GB for file system cache, 80 GB for metadata, 20 GB for log). If you followed the documented recommendations, the default value for the read cache is approximately 300 GB.

7. Click Save.

The file system is created and appears in the File Systems listing.

Uninstalling Storage Gateway

This topic describes how to uninstall Storage Gateway.

Uninstalling

To uninstall Storage Gateway
1. Log in to the on-premises host or compute instance from which you want to uninstall Storage Gateway.
2. Stop Storage Gateway:
   
   ```
   sudo ocisg down
   ```
3. If the ocisg_data container exists in docker ps -a output, remove it:
   
   ```
   sudo docker rm -v ocisg_data
   ```
4. Delete the image in docker:
   
   ```
   sudo docker rmi $(sudo docker images| grep ocisg | awk '{print $3}')
   ```
5. Delete all the files in /usr/bin/ that begin with ocisg:
   
   ```
   sudo rm /usr/bin/ocisg*
   ```
6. View the contents of the file gateway_config:
   
   ```
   cat /etc/gateway_config
   ```

   **Sample output:**

   ```
   $ cat /etc/gateway_config
   DATASTORAGE=/ocisg/cache
   MDSTORAGE=/ocisg/metadata
   LOGSTORAGE=/ocisg/log
   PROXY=
   USE_SSL=
   MEMORY=
   NETWORK=bridge
   HTTP_FRAMEWORK=
   ADMINPORT=443
   NFSPORT=32769
   RESTPORT=32768
   ```

   • Delete the DATASTORAGE directory, for example:
     
     ```
     sudo rm -rf /ocisg/cache
     ```
   • Delete the MDSTORAGE directory, for example:
     
     ```
     sudo rm -rf /ocisg/metadata
     ```
   • Delete the LOGSTORAGE directory, for example:
     
     ```
     sudo rm -rf /ocisg/log
     ```
   • Delete the gateway_config file:
     
     ```
     sudo rm /etc/gateway_config
     ```
   • Delete the Storage Gateway installation directory ocisg:
     
     ```
     sudo rm -rf /opt/ocisg
     ```

**Getting Help with Storage Gateway**

This topic provides information about getting help with Oracle Cloud Infrastructure Storage Gateway.
Contacting Oracle Support

If you need technical support or help with Storage Gateway, you can go to My Oracle Support and create a service request. See Creating a Service Request Using the Console on page 126 for information.

Downloading the Support Bundle

If you contact Oracle Support about any issue with Storage Gateway, you might need to provide a support bundle to help the Oracle Support technicians diagnose the issue.

1. Log in to the management console.
2. Click System in the upper-right corner of the management console.
3. Click Help.
4. Click Download Support Bundle in System Logs.
   You can download and save the support bundle.

Contents of the Support Bundle

The support bundle contains the following information:

- All of the logs needed for diagnostics.
- Local storage usage information.
- Basic system information such as memory size, Docker version, and the Storage Gateway version.
- A list of file systems.
- Cloud Sync job details.
The Oracle Cloud Infrastructure Streaming service provides a fully managed, scalable, and durable solution for ingesting and consuming high-volume data streams in real-time.

Use Streaming for messaging, ingesting application logs, operational telemetry, web click-stream data, or any other use cases in which data is produced and processed continually and sequentially in a publish-subscribe messaging model.

About Streaming

Here's how Streaming works: a producer publishes messages to a stream, which is an append-only log. These messages are distributed among Oracle-managed partitions using the message's key for scalability.

Partitions allow you to distribute a stream by splitting messages across multiple nodes (or brokers). Each partition can be placed on a separate machine to allow multiple consumers to read a stream in parallel. Consumers can read from any partition regardless of where the partition is hosted. All partitions associated with a stream are deleted when the stream is deleted.

A consumer reads messages from one or more partitions. Each message within a stream is marked with an offset value, so a consumer can pick up where it left off if it is interrupted. Consumers can read messages individually, or as a member of a consumer group.

You can use Streaming for:

**Messaging**

Use Streaming to decouple the components of large systems. Producers and consumers can use Streaming as an asynchronous message bus and act independently and at their own pace.

**Metric and log ingestion**

Use Streaming as an alternative for traditional file-scraping approaches to help make critical operational data more quickly available for indexing, analysis, and visualization.

**Web or mobile activity data ingestion**

Use Streaming for capturing activity from websites or mobile apps, such as page views, searches, or other user actions. You can use this information for real-time monitoring and analytics, and in data warehousing systems for offline processing and reporting.
Infrastructure and apps event processing

Use Streaming as a unified entry point for cloud components to report their lifecycle events for audit, accounting, and related activities.

Benefits of Streams

Streams have several advantages over traditional messaging queues. Such as:

Configurable message persistence

You control how long your data is retained. Messages in a stream are available for the entirety of the stream's configured retention time.

Replay

Because a stream's messages are not removed immediately when processed by consumers, you can replay any and all messages in the stream at any time within the configured retention limit.

Message guarantees

Each message is guaranteed to be delivered at least once. In some cases, such as a consumer's failure to commit messages before going offline, messages may be delivered multiple times.

Order guarantees

Messages within a stream, per partition, are always delivered in the same order that they were produced.

Client-side cursors

Your client applications control and track which messages are read and can move the cursor as needed for maximum flexibility.

Horizontal scale

Partitions provide an opportunity to scale up throughput to meet the needs of multiple consumers, resulting in increased flexibility.

Consumer groups

Consumer groups handle all of the coordination that is required to deliver messages to multiple consumers in a balanced manner. Because this management is handled by a consumer group on behalf of all of its members, you can enjoy reduced overhead and operational ease.

Streaming Concepts

The following concepts are essential to understanding and working with Streaming.

stream

A partitioned, append-only log of messages.

stream pool

A grouping that you can use to organize and manage streams, including any shared Kafka or security settings.

partition

A section of a stream. Partitions allow you to distribute a stream by splitting messages across multiple nodes. Each partition is typically placed on a separate virtual machine in order to provide durability of data. This also allows multiple consumers to read from a stream in parallel.

cursor

A pointer to a location in a stream. This location could be a pointer to a specific offset or time in a partition, or to a groups' current location.
**message**
A Base64-encoded message that is published to a stream.

**producer**
An entity that publishes messages to a stream.

**consumer**
An entity that reads messages from one or more streams.

**consumer group**
A set of instances which coordinates messages from all of the partitions in a stream. At any given time, the messages from a specific partition can only be consumed by a single consumer in the group.

**instance**
A member of a consumer group. Instances are defined when a group cursor is created. Group membership is maintained through interaction; lack of interaction results in a timeout, removing the instance from the consumer group.

**topic/key**
An identifier used to group related messages.

**offset**
The location of a message within a partition. Each message within the partition is identified by its offset. Consumers can read messages starting from any chosen offset. You can use the offset to restart reading from a stream if interrupted.

**permissions**
You can use IAM to set permissions on the following operations: list, get, update, create, and delete streams.

### Streaming Features
Streaming provides the following features:

**Fully managed**
Streaming is fully managed, from the underlying infrastructure to its provisioning, deployment, maintenance, security patching, and replication. Integration with Monitoring and default metrics make operations easy.

Oracle manages stream partitions and consumer groups can handle your message offsets.

**Durability and Availability**
Messages published to the Streaming service are synchronously replicated across three availability domains when available. In regions with a single availability domain, the data is replicated across multiple fault domains. This ensures that even the failure of an availability domain or fault domain does not result in data loss. The result is highly durable data.

Oracle Cloud Infrastructure provides a service-level agreement (SLA) for Streaming. Refer to the Oracle Cloud Infrastructure Service Level Agreement page for details.

**Security**
Streaming data is encrypted both at rest and in transit, ensuring message integrity. You can let Oracle manage encryption, or use the Oracle Cloud Infrastructure Vault service to securely store and manage your own encryption keys if you need to meet specific compliance or security standards.

Integration with Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who and what services can access which keys and what they can do with those resources.

Private endpoints restrict access to a specified virtual cloud network (VCN) within your tenancy so that its streams cannot be accessed through the internet.
For more information, see Stream Security on page 3858.

Kafka compatibility

Streaming makes it possible to offload the setup, maintenance, and management of the infrastructure that hosting your own Apache Kafka cluster requires.

Streaming is compatible with most Kafka APIs, allowing you to use applications written for Kafka to send messages to and receive messages from the Streaming service without having to rewrite your code. See Using Kafka APIs on page 3881 for more information.

Streaming also takes advantage of the Kafka Connect ecosystem to interface directly with first-party and third-party products by using out-of-the-box Kafka source and sink connectors. See Using Kafka Connect on page 3883 for more information.

Ways to Access Streaming

You can access Streaming using any of the following options, based on your preference and use case.

- Oracle Cloud Infrastructure REST APIs provide the most functionality, but require programming expertise. API Reference and Endpoints provides endpoint details and links to the available API reference documents. For general information about using the API, see REST APIs on page 4368. The Streaming service is accessible with the Streaming API.

  Tip:

  Because Streaming is compatible with the Apache Kafka API, applications written for Kafka can also access Streaming.

- Oracle Cloud Infrastructure provides SDKs so that you can interact with Streaming without having to create a framework. Basic Streaming usage examples are included with our SDKs. For more information about using the SDKs, see the SDK Guides.

- The command line interface (CLI) provides both quick access and full functionality without the need for programming. For more information, see Using the CLI on page 4207.

- The Console is an easy-to-use, browser-based interface. You can use the Console to create and manage streams, stream pools, and Kafka Connect configurations, but you cannot publish or consume messages using the Console.

  To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Using Streaming

To get started with Streaming, see the following topics:

- For instructions on how to create and manage streams, see Managing Streams on page 3856 and Managing Stream Pools on page 3864.
- For information about publishing messages to a stream, see Publishing Messages on page 3870.
- For information on how to consume messages, see Consuming Messages on page 3873.
- For information on Apache Kafka compatibility, see Using Streaming with Apache Kafka on page 3880.
- For API reference documentation, see Streaming API.
- For SDK and CLI information, see Software Development Kits and Command Line Interface on page 4225.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).
An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For common policies used to authorize Streaming users, see Common Policies on page 2142.

For in-depth information on granting users permissions for the Streaming service, see Details for the Streaming Service in the IAM policy reference.

Limits on Streaming Resources

The Streaming service has the following limits:

- The maximum retention period for messages in a stream is seven days. The minimum retention period is 24 hours. All messages in a stream are deleted after the retention period passes, whether or not they have been read.
- The retention period for a stream cannot be changed after creation of the stream.
- A tenancy has a default limit of five partitions (Monthly Universal Credits) or zero partitions (Pay-as-You-Go or Promo). If your throughput requires additional partitions, you can request more.
- The number of partitions for a stream cannot be changed after creation of the stream.
- A single stream can support up to 50 consumer groups reading from the stream.
- Each partition can support:
  - A total data write rate of 1 MB per second. There is no limit on the number of PUT requests, provided the limit of 1 MB per second per partition is not exceeded.
  - 5 GET requests per second per consumer group. Since a single stream can support up to 50 consumer groups, and a single partition in a stream can be read by at-most one consumer in a consumer group, a partition can support up to 250 GET requests per second (5 GET requests per second per consumer in all 50 consumer groups).
- The maximum size of a unique message that producers can publish to a stream is 1 MB.

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Managing Streams

Before publishing messages to a stream, or consuming messages from a stream, you must first create a stream. You can use the Oracle Cloud Infrastructure Console or the Streaming API to create your stream.

When creating a stream, consider the expected stream throughput, message retention period, partition key strategy, and how your stream will be consumed. Most configuration values cannot be changed after the stream has been created. For example, after a stream is created, you can't change the message retention time or number of partitions.

Partitioning a Stream

To take full advantage of the Streaming service's ability to operate at scale, configure the number of partitions in the stream based on the following considerations.

Partitions and Throughput

When you create a stream, you must specify how many partitions the stream has. The expected throughput of your application can help you determine the number of partitions for your stream.

Multiply the average message size by the maximum number of messages written per second to estimate your expected throughput. Since a single partition is limited to a 1 MB per second data write rate, and 5 GET requests per second per consumer group, a higher throughput requires additional partitions to avoid throttling. Keep additional Streaming limits in mind when making your design decisions.
Streaming Service Overview

Tip:
To help you manage application spikes, we recommend allocating partitions slightly higher than your maximum throughput.

Publishing to Partitions
The content of the messages you intend to publish to a stream can also help you determine how many partitions your stream should have.

A message is published to a partition in the stream. If there is more than one partition, the partition where the message is published is calculated using the message's key.

For more information, see Publishing Messages on page 3870.

Key to partition mapping
Messages with the same key go to the same partition. Messages with different keys might go to different partitions or to the same partition. If you do not specify a key, Streaming recognizes the null key and generates a random key on the behalf of the user. If a user publishes the same message twice, it could go to different partitions, since a completely new key is generated. Do not expect all messages with a null key to go to the same partition.

By default, Streaming provides uniform and predictable distribution of messages to a stream's partitions. Streaming APIs do not let you specify exactly which partition data is published to, since this can introduce a risk of hotspotting a single partition if a user is not aware of the nuances of Streaming. However, if you use Kafka APIs to interact with Streaming, you may choose to do custom partitioning and explicitly map messages to partitions, although we do not recommend it.

Effective partitioning keys
To ensure uniform distribution of messages, you need effective values for your message keys. To create an effective value, consider the selectivity and cardinality of your Streaming data.

Cardinality: Consider the total number of unique keys that could potentially be generated based on the specific use case. Higher key cardinality generally means better distribution.

Selectivity: Consider the number of messages with each key. Higher selectivity means more messages per key, which can lead to hotspots.

Always aim for high cardinality and low selectivity.

Ordering
Messages with the same key are guaranteed to be stored in the order they are published, and delivered to consumers in the same order they were produced. Because messages with the same key go to the same partition, this guarantee only applies at the partition level.

Partitions and Consumer Groups
If your stream will be consumed by one or more consumer groups, you should factor that into your decision on how many partitions it should have. Partition reads are balanced among the instances in a consumer group.

Consumer groups can only utilize a single instance at a time if the stream has only one partition. If your stream has multiple partitions, you can scale the number of instances up to the number of the partitions and have one instance in the group reading from one partition in the stream.

For more information, see Using Consumer Groups on page 3876.

Stream Pooling
When you create your stream, you need to specify whether it should become a member of an existing stream pool, or a member of a new, automatically created stream pool. See Managing Stream Pools on page 3864 for more information.
Stream Security

Streaming data is encrypted both at rest and in transit. Private endpoints within your virtual cloud network (VCN) can be used to restrict access to your streams so they cannot be accessed through the internet.

Both encryption and private access are configured at the stream pool level to make managing groups of streams easier.

Encryption

By default, all encryption-related matters are handled by Oracle, but you can manage your own encryption keys using Oracle Cloud Infrastructure Vault. Vault allows you to bring your own Advanced Encryption Standard (AES) symmetric keys and manage, rotate, disable, and delete them as needed.

Because encryption keys are managed at the stream pool level, you can use a different encryption key for each logical stream grouping or virtual Kafka cluster.

To use your own encryption key:

• Ensure that you have the required IAM policies.
• Import your key.
• Change the master encryption key assigned to the stream pool.

For more information, see Overview of Vault on page 3952 and Managing Keys on page 3962.

Private Endpoints

Private endpoints associate a private IP address within a VCN to the stream pool, allowing Streaming traffic to avoid traversing the internet.

To create a private endpoint for Streaming, you need access to a VCN with a private subnet when you create the stream pool. See About Private Endpoints on page 3254 and VCNs and Subnets on page 2821 for more information.

To use private endpoints:

• Ensure you have the required IAM policies.
• Select Private Endpoint and provide the required information when you create your stream pool.

Because streams using private endpoints are not accessible from the internet, you cannot use the Console to show their latest messages.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let streaming users manage streams on page 2154 lets the specified group do everything with streaming and related Streaming service resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for the Streaming service, see Details for the Streaming Service in the IAM policy reference and Accessing Streaming Resources Across Tenancies on page 3895.

Using the Console

To create a stream

1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.

   A list of existing streams is displayed.

2. Click Create Stream at the top of the list.

3. **Stream Name**: Required. Specify a friendly name for the stream. It does not have to be unique within the compartment, but it must be unique to the stream pool. The stream name cannot be changed. Avoid entering confidential information.
4. **Compartment**: Choose the compartment in which the stream will be created. To change the compartment, select a different compartment from the drop-down list.

5. **Stream Pool**: Choose the stream pool that will contain your stream.
   a. If your chosen compartment has an existing stream pool, you can select it from the drop-down list or click Create new stream pool and configure the stream pool manually.
   b. If no stream pool exists in the chosen compartment, select Auto-create a default stream pool or click Create a new stream pool and configure the stream pool manually.

6. In the Define Stream Settings panel:
   a. **Retention (in Hours)**: Enter the number of hours (from 24 to 168) to retain messages. The default value is 24.
   b. **Number of Partitions**: Enter the number of partitions for the stream. The maximum number is based on the limits for your tenancy.

   **Tip:**
   The maximum **Total Write Rate** and **Total Read Rate** of your stream are displayed as you adjust the number of partitions.

7. Click **Show Advanced Options** to optionally define Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

8. Click **Create**.

**To delete a stream**
1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. You can delete a stream in two ways:
   a. Click the the Actions icon (three dots) on the right side of the stream you want to delete and select **Delete Stream**.
   b. Click the stream you want to delete. The stream details screen displays. Click **Delete**.
3. Confirm when prompted.

**To produce a test message**
1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Click a stream to display the stream details page.
3. Click **Produce Test Message**.
4. On the Test Stream dialog, enter the text-only message to produce in the **Data** text box.
5. Click **Produce**.

**To show recent messages on a stream**
1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Click a stream to display the stream details page.
3. In the **Recent Messages** panel, click **Load messages**.

Streams using private endpoints are not accessible from the internet, so their messages do not display in the Console.

**To move a stream to a different compartment**
1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Click a stream to display the stream details page.
3. Find the stream you want to move in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.
Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**Note:**

The examples in this section use the full syntax for all parameters, for example `--compartment-id`. For some parameters, there are shortened versions that you can use instead, like `-c`. See the CLI online help for instances of a shortened parameter associated with a command.

To get a list of streams in a compartment

`oci streaming admin stream list --compartment-id <compartment_OCID>`

For example:

```
oci streaming admin stream list --compartment-id ocid1.tenancy.oc1..exampleuniqueID

{
  "data": [
    {
      "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
      "defined-tags": {},
      "freeform-tags": {},
      "id": "ocid1.stream.oc1.phx.exampleuniqueID",
      "lifecycle-state": "ACTIVE",
      "messages-endpoint": "https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com",
      "name": "example_stream_2",
      "partitions": 1,
      "stream-pool-id": "ocid1.streampool.oc1.phx.exampleuniqueID",
      "time-created": "2020-08-21T21:19:35.707000+00:00"
    },
    {
      "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
      "defined-tags": {},
      "freeform-tags": {},
      "id": "ocid1.stream.oc1.phx.exampleuniqueID",
      "lifecycle-state": "DELETED",
      "messages-endpoint": "https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com",
      "name": "example_stream_1",
      "partitions": 5,
      "stream-pool-id": "ocid1.streampool.oc1.phx.exampleuniqueID",
      "time-created": "2020-07-16T20:59:32.904000+00:00"
    }
  ]
}
```

By default, getting a list of streams returns up to the first 10 streams in the compartment.

To get a list of streams in a stream pool

`oci streaming admin stream list --stream-pool-id <stream_pool_OCID>`

For example:

```
oci streaming admin stream list --stream-pool-id ocid1.streampool.oc1.phx.exampleuniqueID
```

Oracle Cloud Infrastructure User Guide 3860
By default, getting a list of streams returns up to the first 10 streams in the stream pool.

To create a stream

You can create a stream in a compartment or a stream pool. The --compartment-id and --stream-pool-id parameters cannot be specified at the same time.

```
oci streaming admin stream create --name <stream_name> --
partitions <number_of_partitions> --compartment-id <compartment_OCID>
```

```
oci streaming admin stream create --name <stream_name> --
partitions <number_of_partitions> --stream-pool-id <stream_pool_OCID>
```

For example:

```
oci streaming admin stream create --name MyStream --partitions 5 --
compartment-id ocid1.tenancy.oc1..exampleuniqueID
```

```
oci streaming admin stream create --name MyStream --partitions 5 --
compartment-id ocid1.tenancy.oc1..exampleuniqueID
```

```json
{
    "data": [
        {
            "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
            "defined-tags": {},
            "freeform-tags": {},
            "id": "ocid1.stream.oc1.phx.exampleuniqueID",
            "lifecycle-state": "ACTIVE",
            "messages-endpoint": "https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com",
            "name": "example_stream_2",
            "partitions": 1,
            "stream-pool-id": "ocid1.streampool.oc1.phx.exampleuniqueID",
            "time-created": "2020-08-21T21:19:35.707000+00:00"
        },
        {
            "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
            "defined-tags": {},
            "freeform-tags": {},
            "id": "ocid1.stream.oc1.phx.exampleuniqueID",
            "lifecycle-state": "DELETED",
            "messages-endpoint": "https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com",
            "name": "example_stream_1",
            "partitions": 5,
            "stream-pool-id": "ocid1.streampool.oc1.phx.exampleuniqueID",
            "time-created": "2020-07-16T20:59:32.904000+00:00"
        }
    ]
}
```
To view stream details

oci streaming admin stream get --stream-id <stream_OCID>

For example:

oci streaming admin stream get --stream-id
ocid1.stream.oc1.phx.exampleuniqueID
{}

"data": {
  "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
  "defined-tags": {},
  "freeform-tags": {},
  "id": "ocid1.stream.oc1.phx.exampleuniqueID",
  "lifecycle-state": "ACTIVE",
  "lifecycle-state-details": null,
  "messages-endpoint": "https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com",
  "name": "MyStream",
  "partitions": 5,
  "retention-in-hours": 24,
  "stream-pool-id": "ocid1.streampool.oc1.phx.exampleuniqueID",
  "time-created": "2020-11-02T19:12:22.385000+00:00"
},
"etag": "0613d634-86ab-4446-973f-268d175313d4-12e9725e-5574-4f6b-995b-7dcc80271666"
}

To delete a stream

Caution:
Stream contents are deleted immediately. You cannot recover a deleted stream.

oci streaming admin stream delete --stream-id <stream_OCID>

For example:

oci streaming admin stream --delete --stream-id
ocid1.stream.oc1.phx.exampleuniqueID
Are you sure you want to delete this resource? [y/N]:

Select y and press Enter. The stream is deleted with no further prompting.

To move a stream to a different stream pool

oci streaming admin stream update --stream-id <stream_OCID> --stream-pool-id <stream_pool_OCID>

For example:

oci streaming admin stream update --stream-id
ocid1.stream.oc1.phx.exampleuniqueID --stream-pool-id
ocid1.streampool.oc1.phx.exampleuniqueID
To move a stream to a different compartment

oci streaming admin stream change-compartment --stream-id <stream_OCID> --compartment-id <compartment_OCID>

For example:

oci streaming admin stream change-compartment --stream-id ocid1.stream.oc1.phx.exampleuniqueID --compartment-id ocid1.tenancy.oc1..exampleuniqueID

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following API operations to manage streams:

- CreateStream
- ListStreams
- GetStream
- UpdateStream
Managing Stream Pools

Stream pools are logical groupings for streams. Every stream needs to be a member of a stream pool. If you don't create a stream pool, the Streaming service uses a default pool to contain your streams.

You can use stream pools to:

- Organize streams into groups matching your organizational structure or a specific solution
- Restrict access to a specified virtual cloud network (VCN) inside your tenancy so that streams in the pool are not accessible through the internet
- Specify whether the data in the pool's streams should be encrypted using your own Vault encryption key or an Oracle-managed key

There is no limit to the number of stream pools you can create.

**Note:**
Stream names must be unique within a stream pool.

Stream Pools and Apache Kafka

Stream pools serve as the root of a virtual Apache Kafka cluster when you use Kafka with Streaming. All streams within the pool share the same Kafka configuration, encryption, and access control settings. Every action on that virtual cluster is scoped to that stream pool.

You can configure the stream pool to automatically create streams, or Kafka topics, and call `KafkaAdminClient::createTopic` to create a stream or topic in that stream pool.

For more information, see Using Streaming with Apache Kafka on page 3880.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let streaming users manage streams on page 2154 lets the specified group do everything with streaming and related Streaming service resources.

To set up a private endpoint, you must have access to a VCN with a private subnet where DNS resolution is enabled. For general information about policies and permissions to do this, see IAM Policies for Networking on page 2832. Specifically, you need use permissions for a VNIC, a network security group, if you specify one, and a subnet. For example:

```plaintext
allow user group ServiceWriters to use vnics in compartment ABC
allow user group ServiceWriters to use network-security-groups in compartment ABC
allow user group ServiceWriters to use subnets in compartment XYZ
```

To use your own encryption key, you must let the Streaming service use a Vault key to encrypt data in streams in this stream pool. For example:

```plaintext
allow service streaming to use keys in compartment ABC where target.key.id = 'key OCID>'
```
Streaming Service Overview

The preceding policy also requires a companion policy to let Streaming use a key on behalf of a user group to create a stream pool that uses the key for cryptographic purposes. For example:

```
allow user group StreamWriters to use key-delegate in compartment ABC where target.key.id = '<key_OCID>'
```

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for the Streaming service, see Details for the Streaming service in the IAM policy reference and Accessing Streaming Resources Across Tenancies on page 3895.

Using the Console

To create a stream pool

1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Stream Pools on the left side of the screen.

A list of existing stream pools is displayed.
3. Click Create Stream Pool to display the Create Stream Pool page.
4. Enter a name for the stream pool in the Stream Pool Name text box. Avoid entering confidential information.
5. Select a compartment from the Resource Compartment drop-down list.
6. In the Configure Stream Pool panel:
   a. Select Endpoint Type: Click Public Endpoint or Private Endpoint, depending on whether you want to restrict traffic to streams in this stream pool to a private endpoint that does not require traffic to traverse the internet. To create a private endpoint, you need access to a virtual cloud network (VCN) with a private subnet. Select a VCN with a private subnet where DNS resolution is also enabled, and then select the subnet. Optionally, if you want to assign a specific private IP address, you must choose one that belongs to the subnet's CIDR. By default, the Networking service assigns a random private IP address on your behalf and applies no security rules to the stream pool. For more information about VCNs and subnets, see VCNs and Subnets on page 2821.
   b. Configure Encryption Settings: By default, Encrypt using Oracle-managed keys is selected. If you want to encrypt the data in the streams in this stream pool using your own Vault encryption key, click Encrypt using customer-managed keys. To use the Vault service for your encryption needs, you need access to a vault and key and you need to allow the Streaming service to use the key.
      1. Vault: Choose the vault that contains the master encryption key you want to use from the drop-down list.
      2. Master Encryption Key: Choose the master encryption key you want to use from the drop-down list.

   For more information, see Stream Security on page 3858. For more information about encryption with a Vault key that you manage, see Overview of Vault on page 3952 and Managing Keys on page 3962.
7. If you would like to add tags or intend to use Kafka with this stream pool, click Show Advanced Options.
8. Add Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
9. To use the stream pool with Kafka, select the Auto Create Topics checkbox and configure your stream settings:
   a. Add a number of hours for the stream's retention period in Default Retention Period (hours) text box.
   b. Specify the Default Number of Partitions for the stream.
   c. Select the View Kafka settings after the stream pool is created checkbox to display the Kafka Connection settings for the stream pool when it is created.
10. Click Create.

To edit a stream pool

1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Stream Pools on the left side of the screen.

A list of existing stream pools is displayed.
3. Click the stream pool you want to edit to bring up the stream pool details page.
4. Click Edit Settings.
5. Click Edit Settings or Cancel when finished.

**To delete a stream pool**
1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Stream Pools on the left side of the screen.
   A list of existing stream pools is displayed.
3. You can delete a stream pool in two ways:
   a. Click the the Actions icon (three dots) on the right side of the stream pool you want to delete and select Delete Stream Pool.
   b. Click the stream pool you want to delete. The stream pool details screen displays. Click Delete.
4. Confirm when prompted.

**To change or remove the master encryption key assigned to an existing stream pool**
1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click Stream Pools.
3. Click a stream pool to display the stream details page.
4. In Stream Pool Information, next to Encryption Key, do one of the following:
   • To stop using an Oracle-managed key in favor of a Vault master encryption key that you manage, click Assign, select a vault and encryption key you have access to, and then click Assign.
   • To select a different Vault master encryption key that you manage, click Update, select a vault and encryption key you have access to, and then click Update.
   • Click Unassign to remove the assigned Vault master encryption key and let Oracle manage the encryption key, and then click Unassign again to confirm the removal of the existing key assignment.

**To move a stream pool to a different compartment**
1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Stream Pools on the left side of the screen.
   A list of existing stream pools is displayed.
3. You can move a stream pool in two ways:
   a. Click the the Actions icon (three dots) on the right side of the stream pool you want to move and select Move Resource.
   b. Click the stream pool you want to move. The stream pool details screen displays. Click Move Resource.
4. In the Move Resource to a Different Compartment dialog box, choose the destination compartment from the drop-down list.
5. Click Move Resource.

**Using the Command Line Interface (CLI)**
For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**Note:**
The examples in this section use the full syntax for all parameters, for example --compartment-id. For some parameters, there are shortened versions that you can use instead, like -c. See the CLI online help for instances of a shortened parameter associated with a command.
To get a list of stream pools

oci streaming admin stream-pool list --compartment-id <compartment_OCID>

For example:

oci streaming admin stream-pool list --compartment-id ocid1.tenancy.oc1..exampleuniqueID
{
  "data": [
    {
      "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
      "defined-tags": {},
      "freeform-tags": {},
      "id": "ocid1.streampool.oc1.phx.exampleuniqueID",
      "is-private": false,
      "lifecycle-state": "ACTIVE",
      "name": "MyStreamPool",
      "time-created": "2020-10-09T22:21:16.931000+00:00"
    },
    {
      "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
      "defined-tags": {},
      "freeform-tags": {},
      "id": "ocid1.streampool.oc1.phx.exampleuniqueID",
      "is-private": true,
      "lifecycle-state": "ACTIVE",
      "name": "example-stream-pool-02",
      "time-created": "2020-04-03T07:00:56.196000+00:00"
    },
    {
      "compartment-id": "ocid1.tenancy.oc1..exampleCompartmentOCID",
      "defined-tags": {},
      "freeform-tags": {},
      "id": "ocid1.streampool.oc1.phx.exampleStreamPoolOCID",
      "is-private": false,
      "lifecycle-state": "ACTIVE",
      "name": "example-stream-pool-01",
      "time-created": "2020-04-03T05:28:26.025000+00:00"
    }
  ]
}

By default, getting a list of streams returns up to the first 10 streams in the compartment.

To create a stream pool

oci streaming admin stream-pool create --name <stream_pool_name> --compartment-id <compartment_OCID>

For example:

oci streaming admin stream-pool create --name MyStreamPool --compartment-id ocid1.tenancy.oc1..exampleuniqueID
{
  "data": {
    "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
    "custom-encryption-key": {
      "key-state": "NONE",
      "kms-key-id": null
    }
  }
}
Tip:

Provide input for --custom-encryption-key-details, --private-endpoint-details, and --kafka-settings as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

To view stream pool details

oci streaming admin stream-pool get --stream-pool-id <stream_pool_OCID>

For example:

oci streaming admin stream-pool get --stream-pool-id ocid1.streampool.oc1.phx.exampleuniqueID

{
  "data": {
    "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
    "custom-encryption-key": {
      "key-state": "NONE",
      "kms-key-id": null
    },
    "defined-tags": {},
    "endpoint-fqdn": "cell-1.streaming.us-phoenix-1.oci.oraclecloud.com",
    "freeform-tags": {},
    "id": "ocid1.streampool.oc1.phx.exampleuniqueID",
    "is-private": false,
    "kafka-settings": {
      "auto-create-topics-enable": false,
      "bootstrap-servers": "cell-1.streaming.us-phoenix-1.oci.oraclecloud.com:9092",
      "log-retention-hours": 24,
      "num-partitions": 1
    },
    "lifecycle-state": "ACTIVE",
    "lifecycle-state-details": null,
    "name": "MyStreamPool",
    "private-endpoint-settings": {
      "nsg-ids": null,
      "private-endpoint-ip": null,
      "subnet-id": null
    },
    "time-created": "2020-11-02T23:01:59.429000+00:00"
  },
  "etag": "\"b0066564-4bf4-4e27-9255-9055e69a7808-03668273-b0d5-4b8b-9370-74522c29eb56\""
}
To update a stream pool

```bash
oci streaming admin stream-pool update --stream-pool-id <stream_pool_OCID>
```

For example:

```bash
oci streaming admin stream-pool update --stream-pool-id ocid1.streampool.oc1.phx.exampleuniqueID --name MyUpdatedStreamPool
```

Tip:

Provide input for `--custom-encryption-key-details`, `--private-endpoint-details`, and `--kafka-settings` as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.
To delete a stream pool

Caution:
The stream pool and all streams within the pool are deleted immediately. You cannot recover a deleted stream pool.

`oci streaming admin stream-pool delete --stream-pool-id <stream_pool_OCID>`

For example:

`oci streaming admin stream-pool delete --stream-pool-id ocid1.streampool.oc1.phx.exampleuniqueID
Are you sure you want to delete this resource? [y/N]:`

Select y and press Enter. The stream pool is deleted with no further prompting.

To move a stream pool to a different compartment

`oci streaming admin stream-pool change-compartment --stream-pool-id <stream_pool_OCID> --compartment-id <target_compartment_OCID>`

For example:

`oci streaming admin stream-pool change-compartment --stream-pool-id ocid1.streampool.oc1.phx.exampleuniqueID --compartment-id ocid1.compartment.oc1..exampleuniqueID
{
  "etag": "\"b9abe5ea-d473-4451-8cf4-9b058fa9b435-a670293bd0d9-4fff-9c54-4a862418e353\""
}

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following API operations to manage stream pools:

- CreateStreamPool
- ListStreamPools
- GetStreamPool
- UpdateStreamPool
- DeleteStreamPool
- ChangeStreamPoolCompartment

Publishing Messages

Once a stream is created and active, you can publish messages.

While you can use the Console to publish test messages to a stream after you create it, you need to use PutMessages to populate your stream, or, if you take advantage of the Streaming service's compatibility with Apache Kafka, your Kafka producer can handle message creation.

Messages

Messages are published to a single partition in a stream. If there is more than one partition in the stream, the decision of which partition to publish the message to depends on whether your producers are using the Streaming API and PutMessages, or taking advantage of Streaming's Kafka compatibility and using the Kafka API.
If your producers are using the Streaming API, partitioning is handled server-side by the Streaming service. If your producers are using the Kafka API, partitioning is handled client-side by Kafka.

**Server-side partitioning**
The partition where a message is published is calculated using the message's key. If the key is null, the partition is calculated using a random 16-byte value. You cannot specify which partition a key uses.

Passing a null key puts the message in a random partition. If a user publishes the same message twice, it could go to different partitions, since a completely new key is generated. Do not expect all messages with a null key to go to the same partition. If you want to ensure that messages with the same value go to the same partition, you should use the same key for those messages.

**Handling large messages**
If your messages are larger than the 1 MB limit, you can either use chunking or send the message by using Oracle Cloud Infrastructure Object Storage.

- **Chunking**: You can split large payloads into multiple, smaller chunks that the Streaming service can accept. The chunks are stored in the service in the same way that ordinary (non-chunked) messages are stored. The only difference is that the consumer must keep the chunks and combine them into the message when all the chunks have been collected. The chunks in the partition can be interwoven with ordinary messages.

- **Object Storage**: A large payload is placed in Object Storage and only the pointer to that data is transferred. The receiver recognizes this type of pointer payload, transparently reads the data from Object Storage, and provides it to the end user.

**Batching and Throttling**
We recommend batching messages to avoid throttling and enable better throughput.

The size of a batch of messages shouldn't exceed 1 MB. If this limit is exceeded, the throttling mechanism is triggered. The throttling mechanism for PutMessages is activated when data write rates exceed 1 MB per second per partition. There is no limitation on the number of writes to a stream, as long as you are under the 1 MB per second per partition throughput.

See [Limits on Streaming Resources](#) on page 3856 for more information.

**Required IAM Policy**
To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in [Let streaming users manage streams](#) on page 2154 lets the specified group do everything with streaming and related Streaming service resources.

If you're new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142. If you want to dig deeper into writing policies for the Streaming service, see [Details for the Streaming Service](#) in the IAM policy reference and [Accessing Streaming Resources Across Tenancies](#) on page 3895.

**Using the Console**

**To publish a message**
1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. In the list of available streams, click on the stream that you want to publish to.
3. Click **Produce Test Message**.
4. Type the message in the **Data** text box.
5. Click **Produce**.
Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

To publish a message

```shell
oci streaming stream message put --stream-id <stream_id> --messages <JSON_messages> --endpoint <messages_endpoint>
```

**Tip:**

Provide input for `--messages` as valid formatted JSON. See Passing Complex Input and Using a JSON File for Complex Input for information about JSON formatting.

For example, `file.txt` contains the properly formatted JSON. Its values are Base64-encoded:

```json
[
  {
    "key": "a2V5MjQ==",
    "value": "dmFsdWUx"
  },
  {
    "key": "a2V5Mjg==",
    "value": "dmFsdWUy"
  }
]
```

The `--messages` parameter takes the file as its value:

```shell
```

```json
{
  "data": {
    "entries": [
      {
        "error": null,
        "error-message": null,
        "offset": 0,
        "partition": "0",
        "timestamp": "2020-11-03T21:35:03.837000+00:00"
      },
      {
        "error": null,
        "error-message": null,
        "offset": 1,
        "partition": "0",
        "timestamp": "2020-11-03T21:35:03.837000+00:00"
      }
    ],
    "failures": 0
  }
}
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use the following API operations to produce messages:

- PutMessages

Consuming Messages

Consuming messages from a stream requires you to:

- Create a cursor.
- Use the cursor to read messages.
- Use the returned cursor to continue reading messages.

You can use an individual consumer to read messages from one or more streams, or use consumer groups to read messages from a stream.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let streaming users manage streams on page 2154 lets the specified group do everything with streaming and related Streaming service resources.

You can create a policy that gives a tenant stream-pull access to consume data from a stream in another tenant. See Accessing Streaming Resources Across Tenancies on page 3895 and Details for the Streaming Service if you want to dig deeper into writing policies for the Streaming service.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Using Individual Consumers

If you choose to use individual consumers to consume messages from your streams instead of using consumer groups, you can't take advantage of many of the benefits of Streaming, such as service-managed coordination, horizontal scaling, and offset management. Your applications will need to handle these scenarios, and many more, programmatically.

For these reasons, we recommend using consumer groups in a production environment, but it may be useful to use individual consumers for testing or proof-of-concept applications.

Using Cursors

A cursor is a pointer to a location in a stream. The location could be a specific offset or time in a partition.

Before you start to consume messages, you need to indicate the point from which you want to start consumption. You can do this by creating a cursor using the CreateCursor API.

There are five supported cursor types:

- TRIM_HORIZON - Start consuming from the oldest available message in the stream. Create a cursor at the TRIM_HORIZON to consume all messages in a stream.
- AT_OFFSET - Start consuming at a specified offset. The offset must be greater than or equal to the offset of the oldest message and less than or equal to the latest published offset.
- AFTER_OFFSET - Start consuming after the given offset. This cursor has the same restrictions as the AT_OFFSET cursor.
- AT_TIME - Start consuming from a given time. The timestamp of the returned message will be on or after the supplied time.
- LATEST - Start consuming messages that were published after you created the cursor.

When you create a cursor for an individual consumer, you need to specify the partition in the stream that the cursor should use. If your stream has more than one partition with messages, you need to create multiple cursors to read them.
Once you've created a cursor, you can start to consume messages using GetMessages.

As long as you keep consuming messages, there is no need to re-create a cursor, so cursors should be created outside of your loops to get messages.

**Getting Messages**

Once you've created a cursor, call GetMessages and specify that cursor to start consuming messages. The service responds with your messages and the opc-next-cursor header value that you should use in your next GetMessages call. The returned cursor is never null, but it expires in five minutes. If you stop consuming messages for longer than five minutes, you will need to re-create a cursor.

If you have more than one consumer reading from the same partition, they will receive the same messages. Your application should decide how to process messages.

If there are no more unread messages in the partition, Streaming returns a list of empty messages.

GetMessages batch sizes are based on the average message size published to the stream. By default, the service returns as many messages as possible. You can use the limit parameter to specify any value up to 10,000, but consider your average message size to avoid exceeding throughput on the stream.

**Falling behind**

To determine if your consumer is falling behind (you're producing faster than you're consuming), you can use the timestamp of the message. If the consumer is falling behind, consider spawning additional consumers to take over some of the partitions from the first consumer. There's no way to recover if you're falling behind on a single partition.

Consider the following options:

- Create a new stream with more partitions.
- Use consumer groups.
- If the issue is caused by a hotspot, change the message key strategy.
- Reduce message processing time, or handle requests in parallel.

If you want to know how many messages are left to consume in a given partition, use a cursor of type LATEST, get the offset of the next published message, and make the delta with the offset that you are currently consuming.

**Managing Offsets**

Offsets indicate the location of a message within a partition. If your consumer restarts or you need to recover from a failure, you can use the offset to restart reading from the stream.

**Tip:**

Consumer groups can manage offset commits automatically.

When you use individual consumers, your consumer application must manage processed offsets. The consumer is responsible for storing which offsets it reached or stopped at, for each partition. When your consumer restarts, read the offset of the last message that you processed, and then create a cursor of type AFTER_OFFSET and specify the offset that you just got. We don't provide any guidance for storing the offset of the last message that you processed. You may use any method, such as another stream, a file on your machine, or Object Storage.

**Note:**

Message offsets aren't dense. Offsets are monotonically increasing numbers. They do not decrease, and sometimes they increase by more than one. For example, if you publish two messages to the same partition, the first message could have an offset of 42 and the second message could have an offset of 45 (offsets 43 and 44 being non-existent).

**Using the Console**

You cannot use the console to consume messages, but you can use it to show recent messages on a stream.
Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

To create a cursor

```shell
oci streaming stream cursor create-cursor --stream-id <stream_OCID> --partition <partition> --type <cursor_type> --endpoint <messages_endpoint>
```

For example:

```shell
oci streaming stream cursor create-cursor --stream-id ocid1.stream.oc1.phx.exampleuniqueID --partition 0 --type TRIM_HORIZON --endpoint https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com
{
    "data": {
        "value": "examplecursorvalue"
    }
}
```

To get messages

```shell
oci streaming stream message get --stream-id <stream_OCID> --cursor <cursor> --endpoint <messages_endpoint>
```

Your first request to get messages should use the value returned when you created a cursor. Each subsequent request should use the opc-next-cursor value returned in the previous response.

For example:

```shell
{
    "data": [
        {
            "key": "a2V5MQ==",
            "offset": 0,
            "partition": "0",
            "stream": "MyStream",
            "timestamp": "2020-11-03T21:52:58.470000+00:00",
            "value": "dmFsdWUx"
        },
        {
            "key": "a2V5Mg==",
            "offset": 1,
            "partition": "0",
            "stream": "MyStream",
            "timestamp": "2020-11-03T21:52:58.470000+00:00",
            "value": "dmFsdWUy"
        },
        {
            "key": "a2V5MQ==",
            "offset": 2,
            "partition": "0",
            "stream": "MyStream",
            "timestamp": "2020-11-03T22:00:48.305000+00:00",
            "value": "dmFsdWUx"
        },
        {
            "key": "a2V5Mg==",
```
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following API operations to consume messages when using a single consumer:

- CreateCursor
- GetMessages

Using Consumer Groups

Consumers can be configured to consume messages as part of a group. In a production environment with multiple partitions, using a consumer group is our recommended method of consuming Streaming messages.

Each stream partition is assigned to a member of a consumer group. An individual member of a consumer group is called an instance. Each instance in a consumer group receives messages from one or more partitions, unless there are more instances than partitions. Instances in excess of the partition count for the stream do not receive messages.

Consumer groups handle the coordination that is required for multiple consumers to share the consumption of a stream. A consumer group automatically:

- Assigns one or more partitions to an instance
- Tracks the messages received by the group and manages commits
- Requests the proper partition(s) and offset(s) on behalf of each instance
- Balances the group as instances join or leave

Up to 50 consumer groups can read from a single stream. Each consumer group receives all of the messages in the stream at least once.

Consumer groups are ephemeral. They disappear when they're not used for the retention period of the stream.

Creating a Consumer Group

A consumer group is created on the first CreateGroupCursor request. Group cursors define a group name/instance name pair. When you create your group cursor, you should provide the ID of the stream, a group name, an instance name, and one of the following supported cursor types:

- TRIM_HORIZON - The group will start consuming from the oldest available message in the stream.
- AT_TIME - The group will start consuming from a given time. The timestamp of the returned message will be on or after the supplied time.
- LATEST - The group will start consuming messages that were published after you created the cursor.

Group cursor types are ignored on CreateGroupCursor calls that include the name of an existing group. That group's committed offsets are used instead of the provided cursor type.

Streaming uses the instance name to identify members of the group when managing offsets. Use unique instance names for each instance of the consumer group.

If you want the Streaming service to handle committing offsets, you should leave the group cursor's commitOnGet value set to true. We recommend using this method to reduce application complexity since your application does not have to handle commits.
**Consuming as a Group**

After your instances join the consumer group, they can read messages from the stream using `GetMessages`. Each call to `GetMessages` returns the cursor to use in the next `GetMessages` call as the `opc-next-cursor` header value. The returned cursor is never null, but it expires in five minutes. As long as you keep consuming, you should never have to re-create a cursor.

When Streaming receives a request for messages from an instance, the service:

- Checks to see whether a group rebalance is necessary
- **Commits the offset(s)** from that instance's previous request, if any
- Responds with the messages defined by the request's cursor

`GetMessages` batch sizes are based on the average message size published to that stream. By default, the service returns as many messages as possible. You can use the `limit` parameter to specify any value up to 10,000, but consider your average message size to avoid exceeding throughput on the stream or timeouts.

If there are no more unread messages in the partition, Streaming returns a list of empty messages.

Because consumer groups remove instances that have stopped consuming messages for more than 30 seconds, you should request fewer messages to avoid timeouts, or extend the timeout using `ConsumerHeartbeat`.

A partition cannot be assigned to multiple instances within the same consumer group. If you have more instances than partitions, the unassigned instances can send `GetMessages` requests, but they won't receive any messages. They remain otherwise idle until the consumer group needs to replace an instance, such as when an existing member of the group does not act within the timeout period.

If you need to manually update the group's position, you can use `UpdateGroup` to reset the location of all consumers in the group to the specified location in the stream.

**Offsets and Commits**

Offsets indicate the location of a message within a partition. If a consumer restarts or you need to recover from a failure, you can use the offset to restart reading from the stream.

When you use a consumer group, Streaming handles offsets automatically. The default behavior of `commitOnGet=true` means that offsets from the previous request are committed. For example:

**For consumer A:**

- A calls `GetMessages` and receives messages from an arbitrary partition, with offsets of 1–100.
- A processes all 100 messages successfully.
- A processes 15 messages, and then goes offline unexpectedly (for more than 30 seconds).

A new consumer **B**:

- B calls `GetMessages`, and the Streaming service uses the latest committed offset and returns messages with offsets 101–200.
- B continues the message loop.

In this example, a portion (15) of the messages were processed at least once, which means that they could have been processed more than once, but no data is lost.

Streaming provides "at-least-once" semantics for consumer groups. Consider when offsets are committed in a message loop. If a consumer goes offline before committing a batch of messages, that batch might be given to another consumer. When a partition is given to another consumer, the consumer uses the latest committed offset to start consumption. The consumer doesn't get messages before the committed offset. We recommend that consumer applications take care of duplicates.

**Note:**

Message offsets aren't dense. Offsets are monotonically increasing numbers. They do not decrease, and sometimes they increase by more than one. For
Streaming Service Overview

If you want to override the default offset behavior and implement a custom offset commit mechanism, set `commitOnGet` to `false` when creating the group cursor. You can use `ConsumerCommit` to commit messages without reading more messages. ConsumerCommit returns a cursor for you to use in your next request.

Caution:
Writing custom commit logic is complicated and full of race conditions and considerations. Many cases exist in which some internal state is changed, and the client is required to handle the situation.

Balancing and Rebalancing
Streaming considers the number of partitions in the stream and the number of instances in the consumer group when assessing balance. Group balancing is automatic. Each consumer is assigned to one or more partitions based on the following calculation:

\[
\left( \frac{n_{\text{Partitions}}}{n_{\text{Consumers}}} \right) \pm 1
\]

For example, if there are eight partitions in the stream and four consumers in the group, each consumer is assigned to two partitions. If there are 10 partitions in the stream and four consumers in the group, two consumers are assigned to two partitions, and two consumers are assigned to three partitions.

As instances join or leave a consumer group and requests are made for messages, partition assignments are reassessed. If the stream has at least one partition more than the number of current instances in the group, and a new instance joins, partitions are reassigned to all instances, including the new one. If an instance in the group stops consuming messages for more than 30 seconds, or fails to send a `ConsumerHeartbeat` within 30 seconds, that instance is removed from the consumer group and its partition is reassigned, if possible, to another instance.

These events are called `rebalancing`. The instances in the group are not aware of the rebalancing process, but the group has coordinated to own a mutually exclusive set of partitions in the stream.

At the end of a successful rebalance operation for a consumer group, every partition within the stream is owned by an instance within the group.

In this way, you can `scale the number of instances up to the number of the partitions` until each instance is consuming messages from only one partition. This configuration maximizes your stream's available throughput. After that point, any new instance joining the group remains in an idle state without being assigned to any partition.

Using the Console
You cannot use the console to consume messages, but you can use it to show recent messages on a stream.

Using the Command Line Interface (CLI)
For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

To create a group cursor

```
oci streaming stream cursor create-group-cursor --stream-id <stream_OCID> --group-name <consumer_group_name> --type <cursor_type> --endpoint <messages_endpoint>
```

For example:

```
oci streaming stream cursor create-group-cursor --stream-id ocid1.stream.oc1.phx.exampleuniqueID --group-name MyConsumerGroup --type TRIM_HORIZON --endpoint https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com
```
**Streaming Service Overview**

```json
{
  "data": {
    "value": "examplegroupcursorvalue"
  }
}
```

**To get messages**

```bash
oci streaming stream message get --stream-id <stream_OCID> --cursor <cursor> --endpoint <messages_endpoint>
```

Your first request to get messages should use the value returned when you created a cursor. Each subsequent request should use the `opc-next-cursor` value returned in the previous response.

For example:

```bash
{
  "data": [
    {
      "key": "a2V5MQ==",
      "offset": 0,
      "partition": "0",
      "stream": "MyStream",
      "timestamp": "2020-11-03T21:52:58.470000+00:00",
      "value": "dmFsdWUx"
    },
    {
      "key": "a2V5Mg==",
      "offset": 1,
      "partition": "0",
      "stream": "MyStream",
      "timestamp": "2020-11-03T21:52:58.470000+00:00",
      "value": "dmFsdWUy"
    },
    {
      "key": "a2V5MQ==",
      "offset": 2,
      "partition": "0",
      "stream": "MyStream",
      "timestamp": "2020-11-03T22:00:48.305000+00:00",
      "value": "dmFsdWUx"
    },
    {
      "key": "a2V5Mg==",
      "offset": 3,
      "partition": "0",
      "stream": "MyStream",
      "timestamp": "2020-11-03T22:00:48.305000+00:00",
      "value": "dmFsdWUy"
    }
  ],
  "opc-next-cursor": "examplenextcursorvalue"
}
```

**To send a heartbeat**

```bash
oci streaming stream group heartbeat --stream-id <stream_OCID> --cursor <cursor> --endpoint <messages_endpoint>
```

Oracle Cloud Infrastructure User Guide 3879
Your first heartbeat request should use the value returned when you created a group cursor. Each subsequent request should use the value returned in the previous response.

For example:

```
oci streaming stream group heartbeat --stream-id ocid1.stream.oc1.phx.exampleuniqueID --cursor examplecursorvalue --endpoint https://cell-1.streaming.us-phoenix-1.oci.oraclecloud.com
{
  "data": {
    "value": "examplenextcursorvalue"
  }
}
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following API operations to consume messages with consumer groups:

- CreateGroupCursor
- GetMessages
- ConsumerHeartbeat
- UpdateGroup

Using Streaming with Apache Kafka

Oracle Cloud Infrastructure Streaming lets users of Apache Kafka offload the setup, maintenance, and infrastructure management that hosting your own Zookeeper and Kafka cluster requires.

Streaming is compatible with most Kafka APIs, allowing you to use applications written for Kafka to send messages to and receive messages from the Streaming service without having to rewrite your code. See Using Kafka APIs on page 3881 for more information.

Streaming can also utilize the Kafka Connect ecosystem to interface directly with external sources like databases, object stores, or any microservice on the Oracle Cloud. Kafka connectors can easily and automatically create, publish to, and deliver topics while taking advantage of the Streaming service’s high throughput and durability. See Using Kafka Connect on page 3883 for more information.

Use cases for Streaming and Kafka include:

- Move data from Streaming to Autonomous Data Warehouse via the JDBC Connector to perform advanced analytics and visualization.
- Use the Oracle GoldenGate connector for Big Data to build an event-driven application.
- Move data from Streaming to Oracle Object Storage via the HDFS/S3 Connector for long term storage, or to run Hadoop/Spark jobs.

Kafka API Support

Streaming is fully upstream compatible with the latest versions of Kafka APIs. Streaming supports the following Kafka APIs:

- Producer (v0.7.0 and later)
- Consumer (v0.7.0 and later)
- Connect (v0.9.0.0 and later)
- Admin (v0.10.1.0 and later)
- Group Management (v0.7.0 and later)

The following Kafka APIs and features are not yet implemented in the Streaming service:

- Kafka Streams
Streaming Service Overview

- Compaction
- Transactions
- Dynamic Partition Addition
- Idempotent production

Kafka Clients
While many Kafka clients are available, we recommend the those that have been fully tested and certified to work with the Streaming service.

Streaming supports all versions of these Kafka clients:
- librdkafka
- apache-kafka-java
- confluent-kafka-python

Requirements and Limitations

Unique Stream Names
If you have streams with the same names in a compartment, you can't use Kafka with Streaming until you delete the duplicated streams, unless the streams are in different stream pools. Two streams with the same name can exist in the same compartment only if the streams are in different stream pools.

Duplicate stream names otherwise manifest through an "authentication failed" error. If you do not want to delete your streams, contact the Streaming team so we can rename your streams without data loss.

Load Balancing Connection Recycling
Because the Kafka protocol uses long-lived TCP connections, the Streaming Kafka compatibility layer implements a load balancing mechanism to periodically balance connections between front-end nodes. This mechanism periodically closes connections to force new ones. Most Kafka SDKs handle these disconnections automatically when consuming, but producing to Streaming using the Kafka API might raise disconnection errors. Disconnections can be mitigated by adding retries to your requests. Retries are part of the Kafka SDK and are automatically enabled, and you can explicitly configure their behavior.

Using Kafka APIs
This topic describes how to configure Apache Kafka for API compatibility with Oracle Cloud Infrastructure Streaming. When your producers use Kafka APIs to interact with Streaming the decision of which partition to publish a unique message to is handled client-side by Kafka.

Please refer to Kafka API Support on page 3880 for additional information.

Endpoints
For bootstrap servers, use your region endpoint on port 9092. For example:

```
streaming.us-phoenix-1.oci.oraclecloud.com:9092
```

Authentication
Authentication with the Kafka protocol uses auth tokens and the SASL/PLAIN mechanism. You can generate tokens in the Console user details page. See Working with Auth Tokens on page 2456 for more information.

Tip:
Create a dedicated group/user and grant that group the permission to manage streams in the appropriate compartment or tenancy. The policy in Let streaming users manage streams on page 2154 lets the specified group do
everything with streaming and related Streaming service resources. You then can generate an auth token for the user you created and use it in your Kafka client configuration.

Your username must be in the following format:

```
tenancyName/username/streamPoolId
```

**Tip:**

If you are using the Java SDK, you can also use instance principal authorization.

## Kafka Configuration

Set the following properties for your Kafka client.

### For the Java SDK

**Recommended settings for Java SDK:**

```java
Properties properties = new Properties();
properties.put("bootstrap.servers", "streaming.{region}.oci.oraclecloud.com:9092");
properties.put("security.protocol", "SASL_SSL");
properties.put("sasl.mechanism", "PLAIN");
properties.put("sasl.jaas.config",
"org.apache.kafka.common.security.plain.PlainLoginModule required username="{tenancyName}/#{username}/#{streamPoolId}" password="{authToken}";"
);
```

**Recommended settings for Java SDK producers:**

```java
properties.put("retries", 5); // retries on transient errors and load balancing disconnection
properties.put("max.request.size", 1024 * 1024); // limit request size to 1MB
```

**Recommended settings for Java SDK consumers:**

```java
properties.put("max.partition.fetch.bytes", 1024 * 1024); // limit request size to 1MB per partition
```

### For the Librdkafka SDK

**Recommended settings for Librdkafka SDK:**

```python
'metadata.broker.list': 'streaming.{region}.oci.oraclecloud.com:9092',
'security.protocol': 'SASL_SSL',
'sasl.mechanisms': 'PLAIN',
'sasl.username': '{tenancyName}/#{username}/#{streamPoolId}',
'sasl.password': '{authToken}'
```

**Recommended settings for Librdkafka SDK producers:**

```python
'message.send.max.retries': 5 // retries on transient errors and load balancing disconnection
'max.request.size': 1024 * 1024 // limit request size to 1 MB
```
Recommended settings for Librdkafka SDK consumers:

```java
'max.partition.fetch.bytes': 1024 * 1024 // limit request size to 1 MB per partition
```

**Instance Principal Authorization for the Java SDK**

If you are using the Java SDK, you can authorize an instance to interact with Streaming instead of using auth tokens.

To configure the Java SDK for instance principal authorization:

1. Verify that you have a valid Oracle Cloud Infrastructure (OCI) SDK and CLI configuration file.
2. Import the Oracle Cloud Infrastructure SDK for Java into your project. See [Getting Started with the SDK for Java](#) for more information.
3. Add the following Oracle Cloud Infrastructure SDK for Java dependency:

   ```xml
   <dependency>
     <groupId>com.oracle.oci.sdk</groupId>
     <artifactId>oci-java-sdk-addons-sasl</artifactId>
     <optional>false</optional>
     <version>1.13.1</version> <!-- that's the minimum version to use -->
   </dependency>
   ```

4. Modify the `sasl.mechanism` property of your Kafka client configuration:

   ```java
   properties.put("sasl.mechanism",
   OciMechanism.OCI_RSA_SHA256.mechanismName());
   ```

5. Modify the `sasl.jaas.config` property of your Kafka client configuration using one of the following options:

   ```java
   properties.put("sasl.jaas.config",
   "com.oracle.bmc.auth.sasl.InstancePrincipalsLoginModule required intent=
   \"streamPoolId:<streamPoolId>\";");
   ```

   ```java
   properties.put("sasl.jaas.config",
   "com.oracle.bmc.auth.sasl.UserPrincipalsLoginModule required
   config="<pathToConfig>" profile="<profile>" intent=
   \"streamPoolId:<streamPoolId>\";");
   ```

   - If `config` is not specified, the default config path is used (`~/.oci/config`).
   - If `profile` is not specified, the default profile is used (DEFAULT).

**For More Information**

- Apache Kafka documentation
- Blog post: Oracle Streaming Service Producer and Consumer

**Using Kafka Connect**

To use your Kafka connectors with Oracle Cloud Infrastructure Streaming, create a [Kafka Connect configuration](#) using the Console or the command line interface (CLI). The [Streaming API](#) calls these configurations **harnesses**.

**Note:**

Kafka Connect configurations created in a given compartment work only for streams in the same compartment.

You can use multiple Kafka connectors with the same Kafka Connect configuration. In cases that require producing or consuming streams in separate compartments, or where more capacity is required to avoid hitting throttle limits on
the Kafka Connect configuration (for example: too many connectors, or connectors with too many workers), you can create more Kafka Connector configurations.

For more information on managing Kafka Connect configurations using the Console and Streaming API, see Managing Kafka Connect Configurations on page 3885.

**Kafka Connectors**

Streaming's Kafka Connect compatibility means that you can take advantage of the many existing first- and third-party connectors to move data from your sources to your targets.

### Kafka connectors for Oracle products:

- Oracle Cloud Infrastructure Object Storage (Using Kafka Connect for S3)
  - Kafka Connect Amazon S3 source connector, for producers
  - Kafka Connect Amazon S3 sink connector, for consumers
- Oracle Integration Cloud
- Oracle Database (Using Kafka Connect JDBC)
- Oracle GoldenGate

For a complete list of third-party Kafka source and sink connectors, refer to the official Confluent Kafka hub.

**Kafka Connect Topics**

The Streaming service automatically creates the three topics (config, offset, and status) that are required to use Kafka Connect when you create the Kafka Connect configuration. These topics contain the OCID of the Kafka Connect configuration in their names.

Place these topic names in the `connect-distributed.properties` file of the Kafka connector that you want to use with Streaming.

For example:

```bash
# Relevant Kafka Connect setting
config.storage.topic:<connect_configuration_OCID>-config
offset.storage.topic:<connect_configuration_OCID>-offset
status.storage.topic:<connect_configuration_OCID>-status
```

**Note:**

These three compacted topics are meant to be used by Kafka Connect and Streaming to store configuration and state management data, and should not be used to store your data. To ensure that the Kafka Connect configuration topics are being used for their intended purpose by the connectors, there are hard throttle limits of 50 kb/s and 50 rps in place for these topics.

**Bootstrap Server**

Set the bootstrap server in your Kafka connector properties file to the endpoint for Streaming on port 9092. For example:

```bash
streaming.us-phoenix-1.oci.oraclecloud.com:9092
```

**Note:**

For a list of endpoints for Streaming, see the Streaming section in API Reference and Endpoints.
Authentication

Authentication with the Kafka protocol uses auth tokens and the SASL/PLAIN mechanism. You can generate tokens in the Console user details page. See Working with Auth Tokens on page 2456 for more information.

Tip:

It’s a good idea to create a dedicated group/user and grant that group the permission to manage streams in the appropriate compartment or tenancy. You then can generate an auth token for the user you created and use it in your Kafka client configuration.

Example Kafka Connector Properties File

The following shows an example Kafka connector `connect-distributed.properties` file:

```properties
bootstrap.servers=<streaming_endpoint>:9092
sasl.mechanism=PLAIN
security.protocol=SASL_PLAINTEXT
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
    required username="<userid>" password="<authToken>";
producer.sasl.mechanism=PLAIN
producer.security.protocol=SASL_PLAINTEXT
producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
    required username="<userid>" password="<authToken>";
consumer.sasl.mechanism=PLAIN
consumer.security.protocol=SASL_PLAINTEXT
consumer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
    required username="<userid>" password="<authToken>";
config.storage.topic:<connect_configuration_OCID>-config
offset.storage.topic:<connect_configuration_OCID>-offset
status.storage.topic:<connect_configuration_OCID>-status
```

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: The policy in Let streaming users manage streams on page 2154 lets the specified group do everything with streaming and related Streaming service resources.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for the Streaming service, see Details for the Streaming Service in the IAM policy reference.

For More Information

- Official Kafka Connect documentation
- Blog post: Oracle Streaming Service with Kafka Connect

Managing Kafka Connect Configurations

This topic describes how to work with Kafka Connect configurations. The Streaming API calls these configurations harnesses.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you’re using the Console or the REST API with an SDK, CLI, or other tool. If you get a message
that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

To allow a group to manage Kafka Connect configurations, you need to create the correct policy in your tenancy. For example:

```plaintext
allow group KafkaAdmins to manage connect-harnesses in tenancy
```

For administrators: The policy in Let streaming users manage streams on page 2154 lets the specified group do everything with streaming and related Streaming service resources.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for the Streaming service, see Details for the Streaming Service in the IAM policy reference and Accessing Streaming Resources Across Tenancies on page 3895.

**Using the Console**

To create a Kafka Connect Configuration

1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Kafka Connect Configurations on the left side of the screen.
   A list of existing Kafka Connect configurations is displayed.
3. Click Create Kafka Connect Configuration to display the Create Kafka Connect Configuration page.
4. Select a compartment in the Compartment drop-down list.
5. Enter a name for the configuration in the Kafka Connect Configuration Name text box. Avoid entering confidential information.
6. **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. Click Create Kafka Connect Configuration.
8. The details page for the new Kafka Connect configuration has a read-only text box labeled Kafka Connect Storage Topics.
   a. Click Copy to copy the connector configuration so you can paste it into the connect-distributed.properties file for your Kafka connector. For more information, see the official Kafka Connect documentation.

To delete a Kafka Connect Configuration

1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Kafka Connect Configurations on the left side of the screen.
   A list of existing Kafka Connect configurations is displayed.
3. You can delete a Kafka Connect configuration in two ways:
   a. Click the the Actions icon (three dots) on the right side of the configuration you want to delete and select Delete Kafka Connect Configuration.
   b. Click the configuration you want to delete. The Kafka Connect Configuration Details page displays. Click Delete.
4. Confirm when prompted.

To move a Kafka Connect Configuration to a different compartment

1. Open the navigation menu. Under Solutions and Platform, click Analytics, and then click Streaming.
2. Click on Kafka Connect Configurations on the left side of the screen.
   A list of existing Kafka Connect configurations is displayed.
3. You can move a Kafka Connect configuration in two ways:
   a. Click the the Actions icon (three dots) on the right side of the configuration you want to move and select **Move Resource**.
   b. Click the configuration you want to move. The Kafka Connect Configuration Details screen displays. Click **Move Resource**.
4. In the **Move Resource to a Different Compartment** dialog box, choose the destination compartment from the drop-down list.
5. Click **Move Resource**.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see Command Line Interface (CLI) on page 4192. For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**Note:**
The examples in this section use the full syntax for all parameters, for example `--compartment-id`. For some parameters, there are shortened versions that you can use instead, like `-c`. See the CLI online help for instances of a shortened parameter associated with a command.

To get a list of Kafka Connect configurations

```
oci streaming admin connect-harness list --compartment-id <compartment_OCID>
```

For example:

```
oci streaming admin connect-harness list --compartment-id exampleuniqueID
{
    "data": [
    {
        "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
        "defined-tags": {},
        "freeform-tags": {},
        "id": "ocid1.connectharness.oc1.phx.exampleuniqueID",
        "lifecycle-state": "ACTIVE",
        "name": "MyKafkaConnectConfig",
        "time-created": "2020-08-31T17:26:09.640000+00:00"
    }
    ]
}
```

By default, getting a list of Kafka Connect configurations returns up to the first 10 configurations in the compartment.

To create a Kafka Connect configuration

```
oci streaming admin connect-harness create --name <kafka_connect_configuration_name> --compartment-id <compartment_OCID>
```

For example:

```
oci streaming admin connect-harness create --name MyKafkaConnectConfig --compartment-id exampleuniqueID
{
    "data": {
        "compartment-id": "ocid1.tenancy.oc1..exampleuniqueID",
        "defined-tags": {},
        "freeform-tags": {},
        "id": "ocid1.connectharness.oc1.phx.exampleuniqueID",
        "lifecycle-state": "CREATING",
    }
}
```
Streaming Service Overview

To view Kafka Connect configuration details

oci streaming admin connect-harness get --connect-harness-id <kafka_connect_configuration_OCID>

For example:

oci streaming admin connect-harness get --connect-harness-id exampleuniqueID

To update a Kafka Connect configuration

oci streaming admin connect-harness update --connect-harness-id <kafka_connect_configuration_OCID> --defined-tags <JSON_tags>

For example:

oci streaming admin connect-harness update --connect-harness-id exampleuniqueid --defined-tags "{"tagNamespace": {"tagKey1": "tagValue1","tagKey2": "tagValue2"}}"

WARNING: Updates to freeform-tags and defined-tags will replace any existing values. Are you sure you want to continue? [y/N]: y

Select y and press Enter. The Kafka Connect configuration is updated:
To delete a Kafka Connect configuration

```plaintext
Caution:
Kafka Connect configurations are deleted immediately. You cannot recover a deleted configuration.
```

```plaintext
oci streaming admin connect-harness delete --connect-harness-id <kafka_connect_configuration_OCID>
```

For example:

```plaintext
oci streaming admin connect-harness delete --connect-harness-id ocid1.connectharness.oc1.phx.exampleuniqueID
Are you sure you want to delete this resource? [y/N]:
```

Select y and press Enter. The Kafka Connect configuration is deleted with no further prompting.

To move a Kafka Connect configuration to a different compartment

```plaintext
oci streaming admin connect-harness change-compartment --connect-harness-id <kafka_connect_configuration_OCID> --compartment-id <target_compartment_OCID>
```

For example:

```plaintext
oci streaming admin connect-harness change-compartment --connect-harness-id ocid1.connectharness.oc1.phx.exampleuniqueID --compartment-id ocid1.compartment.oc1..exampleuniqueID
```

### Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following API operations to manage Kafka Connector configurations:

- `CreateConnectHarness`
- `ListConnectHarnesses`
- `GetConnectHarness`
- `UpdateConnectHarness`
- `DeleteConnectHarness`
- `ChangeConnectHarnessCompartment`

### Using Oracle Cloud Infrastructure SDKs with Streaming

Oracle Cloud Infrastructure OCI provides SDKs so that you can interact with Streaming without having to create a framework. The OCI SDKs let you manage streams, stream pools, and Kafka Connect configurations, and publish and consume messages. Refer to the Streaming Service Overview on page 3852 for key concepts and additional information.
Streaming Service Overview

This topic includes examples that use the OCI SDK for Java on page 4225, but basic Streaming usage examples are included with all our SDKs:

- OCI SDK for Python examples
- OCI SDK for TypeScript and JavaScript examples
- OCI SDK for .NET examples
- OCI SDK for Go examples

For more information about using the OCI SDKs, see the SDK Guides.

Streaming Clients

The SDKs encapsulate the Streaming service in two clients: the StreamAdminClient and the StreamClient.

StreamAdminClient

The StreamAdminClient incorporates the control plane operations of Streaming. You can use it to create, delete, update, modify, and list streams.

To instantiate the StreamAdminClient object:

```java
StreamAdminClient adminClient = new StreamAdminClient([authProvider]);
adminClient.setEndpoint("<streaming_endpoint>"); // You cannot use the setRegion method
```

StreamClient

The StreamClient is used to publish and consume messages.

To instantiate a StreamClient object:

```java
// First you have to get the stream you want to consume from/publish to. You can either make a CreateStream, GetStream, or ListStream call. They all return a "messagesEndpoint" as part of a Stream object. That endpoint needs to be used when creating the StreamClient object.
GetStreamRequest getStreamRequest = GetStreamRequest.builder().streamId(streamId).build();
Stream stream = adminClient.getStream(getStreamRequest).getStream();
StreamClient streamClient = new StreamClient([authProvider]);
streamClient.setEndpoint(stream.getMessagesEndpoint());
```

Managing Streams

Creating streams

To create a stream, use the createStream method of StreamAdminClient.

Creating a stream is an asynchronous operation. You can check on the completion of the create operation by checking that the lifecycleStateDetails property of your new stream is either Active or Failed. See Managing Streams on page 3856 for more information.

The following is an example showing how to create a stream:

```java
// No error handling
CreateStreamDetails createStreamDetails = CreateStreamDetails.builder()
    .partitions(5) // number of partitions you want in your stream
    .name("myStream") // the name of the stream - only used in the console
    .compartmentId(tenancy) // the compartment id you want your stream to live in
    .build();
```
// You can also add tags to the createStreamDetails object.
CreateStreamRequest createStreamRequest =
    CreateStreamRequest.builder()
    .createStreamDetails(createStreamDetails)
    .build();

Stream stream = adminClient.createStream(createStreamRequest).getStream();
while (stream.getLifecycleState() != Stream.LifecycleState.Active &&
    stream.getLifecycleState() != Stream.LifecycleState.Failed) {
    GetStreamRequest getStreamRequest =
        GetStreamRequest.builder().streamId(stream.getId()).build();
    stream = adminClient.getStream(getStreamRequest).getStream();
}

// Handle stream Failure

Listing streams
Use the listStreams method to return a list of streams for a given compartment.
You can filter the returned list by OCID, life cycle state, and name.
The results can be sorted in ascending or descending order by name or creation time.
The results are passed back in a paginated list. A token is passed back with each page of results; pass this
token back to the getOpcNextPage method to retrieve the next page of results. A null token returned from
getOpcNextPage indicates that no more results are available.
For example:

// No error handling
ListStreamsRequest listStreamsRequest =
    ListStreamsRequest.builder()
    .compartmentId(tenancy)
    .build();
// You can filter by OCID (exact match only) [builder].id(streamId) -> This
// will return 0..1 item
// You can filter by name (exact match only) [builder].name(name) -> This
// will return 0..n items
// You can order the result per TimeCreated or Name [builder].sortBy(SortBy.
// [TimeCreated|Name])
// You can change the ordering [builder].sortOrder(SortOrder.[Asc|Desc])
// You can filter by lifecycleState [builder].lifecycleState(lifecycleState)
String page;
do {
    ListStreamsResponse listStreamsResponse =
        adminClient.listStreams(listStreamsRequest);
    List<StreamSummary> streams = listStreamsResponse.getItems();
    // Do something with the streams
    page = listStreamsResponse.getOpcNextPage();
} while (page != null);

Retrieving stream details
To get details about a stream, use the getStream method and then examine the properties of the stream. For
example:

// No error handling
GetStreamRequest getStreamRequest =
    GetStreamRequest.builder()
    .streamId(streamId)
Streaming Service Overview

```
.build();
Stream stream = adminClient.getStream(getStreamRequest).getStream();
```

### Deleting streams

To delete a stream, use the `deleteStream` method API of the `StreamAdminClient`. Deleting a stream is an asynchronous operation; the stream state changes to `Deleted` once the delete operation is finished. During the deletion process, the stream can't be used for consuming or producing messages.

The following example shows how to use the `deleteStream` method to delete a stream:

```
// No error handling
DeleteStreamRequest deleteStreamRequest =
    DeleteStreamRequest.builder()
    .streamId(stream.getId())
    .build();
adminClient.deleteStream(deleteStreamRequest);
```

### Managing Kafka Connect Configurations

In order to use Kafka Connect with Streaming, you need a Kafka Connect configuration, or Kafka Connect harness. You can retrieve the OCID for a harness when you create a new harness or use an existing one. For more information, see Using Kafka Connect on page 3883.

#### Creating a Kafka Connect harness

The following code example shows how to create a Kafka Connect harness:

```
CreateConnectHarnessDetails createConnectHarnessDetails =
    CreateConnectHarnessDetails.builder()
    .compartmentId(compartment) //compartment where you want to create connect harness
    .name("myConnectHarness") //connect harness name
    .build();
CreateConnectHarnessRequest connectHarnessRequest =
    CreateConnectHarnessRequest.builder()
    .createConnectHarnessDetails(createConnectHarnessDetails)
    .build();
CreateConnectHarnessResponse createConnectHarnessResponse =
    streamAdminClient.createConnectHarness(connectHarnessRequest);
ConnectHarness connectHarness =
    createConnectHarnessResponse.getConnectHarness();
while (connectHarness.getLifecycleState() !=
    ConnectHarness.LifecycleState.Active &&
    connectHarness.getLifecycleState() != ConnectHarness.LifecycleState.Failed) {
    GetConnectHarnessRequest getConnectHarnessRequest =
        GetConnectHarnessRequest.builder().connectHarnessId(connectHarness.getId()).build();
    connectHarness =
        streamAdminClient.getConnectHarness(getConnectHarnessRequest).getConnectHarness();
}
```
Streaming Service Overview

Listing Kafka Connect harnesses

The following code example shows how to list Kafka Connect harnesses:

```java
ListConnectHarnessesRequest listConnectHarnessesRequest =
    ListConnectHarnessesRequest.builder()
    .compartmentId(compartment) // compartment id to list all the connect harnesses.
    .lifecycleState(ConnectHarnessSummary.LifecycleState.Active)
    .build();

ListConnectHarnessesResponse listConnectHarnessesResponse =
    streamAdminClient.listConnectHarnesses(listConnectHarnessesRequest);
List<ConnectHarnessSummary> items = listConnectHarnessesResponse.getItems();
```

Publishing Messages

Once a stream is created and active, you can publish messages using the `streamClient.putMessages` method. See Publishing Messages on page 3870 for more information about publishing.

The following code example shows how to publish a message:

```java
// No error handling
List<PutMessagesDetailsEntry> messages = new ArrayList<>();

for (int i = 0; i < 40; i++) {
    byte[] key = "<myKey>".getBytes(Charsets.UTF_8); // In this case, all messages will go on the same partition since the key is the same.
    byte[] value = UUID.randomUUID().toString().getBytes(Charsets.UTF_8);
    messages.add(new PutMessagesDetailsEntry(key, value));
}

PutMessagesDetails putMessagesDetails =
    PutMessagesDetails.builder()
    .messages(messages)
    .build();

PutMessagesRequest putMessagesRequest =
    PutMessagesRequest.builder()
    .putMessagesDetails(putMessagesDetails)
    .build();

PutMessagesResult putMessagesResult =
    streamClient.putMessages(putMessagesRequest).getPutMessagesResult();
// It's not because the call didn't fail that the messages were successfully published!
int failures = putMessagesResult.getFailures();
// If failures is > 0, it means we have a partial-success call.
List<PutMessagesResultEntry> entries = putMessagesResult.getEntries();
// entries is a list of the same size as the list of messages you sent.
// It is guaranteed that the order of the messages is the same as when you sent them.
// Each entry contains either "offset/partition/timestamp" if the message was successfully published
// or "error/errorMessage" if it failed.
if (failures != 0) {
    entries.forEach(entry -> {
        if (StringUtils.isNotEmpty(entry.getError())) {
            // That particular message failed to get published.
            // It could be a throttle error and in that case the error would be "429" and errorMessage would contain a meaningful message.
            // Or it could be an internal error and the error would be "500".
```

Oracle Cloud Infrastructure User Guide 3893
Streaming Service Overview

Consuming Messages

Consuming messages requires the use of a cursor, which is a pointer to an offset into a partition. First you must create a cursor, then you must use the cursor to get messages. For more information, see Using Cursors on page 3873 and Getting Messages on page 3874.

Cursors

This example creates a TRIM_HORIZON cursor, which starts consuming starting from the oldest available message:

```java
// No error handling
CreateCursorDetails createCursorDetails =
    CreateCursorDetails.builder()
    .type(Type.TrimHorizon)
    .partition("0")
    .build();
// If using AT_OFFSET or AFTER_OFFSET you need to specify the offset
    [builder].offset(offset);
// If using AT_TIME you need to specify the time [builder].time(new Date(XXX))
CreateCursorRequest createCursorRequest =
    CreateCursorRequest.builder()
    .createCursorDetails(createCursorDetails)
    .build();
String cursor =
    streamClient.createCursor(createCursorRequest).getCursor().getValue();
// Cursor will then be used to get messages from the stream.
```

GetMessages

Once you’ve created a cursor, you can start to consume messages using the GetMessages method. Each call to GetMessages returns the cursor to use in the next GetMessages call.

Here’s an example of using a cursor to retrieve messages:

```java
// No error handling (there is a high chance of getting a throttling error using a tight loop)
while (true) { // or your own exit condition
    GetMessagesRequest getMessagesRequest =
        GetMessagesRequest.builder()
        .cursor(cursor)
        .build();

    GetMessagesResponse getMessagesResponse =
        streamClient.getMessages(getMessagesRequest);

    // This could be empty, but we will always return an updated cursor
    getMessagesResponse.getItems().forEach(message -> {
        // Process the message
    });

    cursor = getMessagesResponse.getOpcNextCursor();
```
Consuming Messages as a Group

Consumers can be configured to consume messages as part of a group. Stream partitions are distributed among members of a consumer group so that messages from any single partition are only sent to a single consumer. Group consumption is accomplished using the same cursor mechanism as with single consumers, but using a different kind of cursor.

For more information, see Using Consumer Groups on page 3876.

To create a consumer group, create a group cursor, providing a group, instance name, and cursor type. Group cursors support the following cursor types:

- **TRIM_HORIZON**: The group will start consuming from the oldest available message in the stream.
- **AT_TIME**: The group will start consuming from a given time. The timestamp of the returned message will be on or after the supplied time.
- **LATEST**: The group will start consuming messages that were published after you created the cursor.

Consumer groups are created on the first request to create a cursor. For example:

```java
CreateGroupCursorRequest groupRequest = CreateGroupCursorRequest.builder()
    .streamId(streamId)
    .createGroupCursorDetails(CreateGroupCursorDetails.builder()
        .groupName(groupName)
        .instanceName(instanceName)
        .type(CreateGroupCursorDetails.Type.TrimHorizon)
        .commitOnGet(true)
        .build())
    .build());

CreateGroupCursorResponse groupCursorResponse = streamClient.createGroupCursor(groupRequest);
String groupCursor = groupCursorResponse.getCursor().getValue();
// this groupCursor can be used in the same message loop a described above;
subsequent getMessages calls return an updated groupCursor.
```

Once you've created a group cursor, you can start to consume messages using GetMessages.

Accessing Streaming Resources Across Tenancies

This topic describes how to write policies that let your tenancy access Streaming resources in other tenancies.

If you're new to policies, see Getting Started with Policies on page 2135 and refer to Details for the Streaming Service on page 2343.

Cross-Tenancy Policies

Your organization might want to share Streaming resources with another organization that has its own tenancy. It could be another business unit in your company, a customer of your company, a company that provides services to your company, and so on. In cases like these, you need cross-tenancy policies in addition to the required user and service policies described previously.

**Endorse, Admit, and Define statements**

To access and share resources, the administrators of both tenancies need to create special policy statements that explicitly state the resources that can be accessed and shared. These special statements use the words Define, Endorse, and Admit.

Here's an overview of the special verbs used in cross-tenancy statements:

- **Endorse**: States the general set of abilities that a group in your own tenancy can perform in other tenancies. The Endorse statement always belongs in the tenancy with the group of users crossing the boundaries into the other tenancy to work with that tenancy's resources. In the examples, we refer to this tenancy as the source.

- **Admit**: States the kind of ability in your own tenancy that you want to grant a group from the other tenancy. The Admit statement belongs in the tenancy who is granting "admittance" to the tenancy.
Streaming Service Overview

identifies the group of users that requires resource access from the source tenancy and identified with a corresponding ENDORSE statement. In the examples, we refer to this tenancy as the destination.

- **Define**: Assigns an alias to a tenancy OCID for ENDORSE and ADMIT policy statements. A Define statement is also required in the destination tenancy to assign an alias to the source IAM group OCID for ADMIT statements.

Define statements must be included in the same policy entity as the endorse or the admit statement.

The ENDORSE and ADMIT statements work together, but they reside in separate policies, one in each tenancy. Without a corresponding statement that specifies access, a particular ENDORSE or ADMIT statement grants no access. **Agreement is required from both tenancies.**

**Source policies**
The source administrator creates policy statements that endorse a source IAM group allowed to manage resources in the destination tenancy.

Here is an example of a broad policy statement that endorses the IAM group StreamingAdmins group to do anything with all Streaming resources in any tenancy:

```plaintext
ENDORSE group StreamingAdmins to manage streams in any-tenancy
```

To write a policy that reduces the scope of tenancy access, the destination administrator must provide the destination tenancy OCID. Here is an example of policy statements that endorse the IAM group StreamingAdmins group to manage Streaming resources in the DestinationTenancy only:

```plaintext
Define tenancy DestinationTenancy as ocid1.tenancy.oc1..<unique_ID>
ENDORSE group StreamingAdmins to manage streams in tenancy DestinationTenancy
```

**Destination policies**
The destination administrator creates policy statements that:

- Define the source tenancy and IAM group that is allowed to access resources in your tenancy. The source administrator must provide this information.
- Admit those defined sources to access Streaming resources that you want to allow access to in your tenancy.

Here is an example of policy statements that endorse the IAM group StreamingAdmins in the source tenancy to do anything with all Streaming resources in your tenancy:

```plaintext
Define tenancy SourceTenancy as ocid1.tenancy.oc1..<unique_ID>
Define group StreamingAdmins as ocid1.group.oc1..<unique_ID>
ADMIT group StreamingAdmins of tenancy SourceTenancy to manage streams in tenancy
```

Here is an example of policy statements that endorse the IAM group StreamingAdmins in the source tenancy to manage Streaming resources only the SharedStreams compartment:

```plaintext
Define tenancy SourceTenancy as ocid1.tenancy.oc1..<unique_ID>
Define group StreamingAdmins as ocid1.group.oc1..<unique_ID>
ADMIT group StreamingAdmins of tenancy SourceTenancy to manage streams in compartment SharedStreams
```

**Streaming Metrics**

You can monitor the health and performance of your streams by using metrics and alarms. For more information, see Monitoring Overview on page 2660.

This topic describes the metrics emitted by the Streaming service using the metric namespace **oci_streaming**.
Overview of Streaming Metrics

The Streaming service provides metrics showing how the service is performing. These metrics are automatically available.

You can use these metrics to:

- Understand the produce/consume latency for a real-time application.
- Calculate and validate the price of service usage.
- Monitor changes in throughput over time.
- Check the time that the last message was consumed.
To view a default set of metrics charts in the Console, navigate to the Service Metrics page and then select the `oci_streaming` metric namespace.

**Available Metrics**

The following tables describe the available Streaming metrics.
You also can use the Monitoring service to create custom queries.

Each metric includes the following dimensions:

**REGION**
- The *REGION* where the stream resides.

**RESOURCEID**
- The *OCID* of the stream.

### Producers

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PutMessagesLatency</td>
<td>Put Messages Latency</td>
<td>time (ms)</td>
<td>Time taken for put messages operation measured over time range.</td>
<td>region,resourceId</td>
</tr>
<tr>
<td>PutMessagesThroughput</td>
<td>Put Messages Total Throughput</td>
<td>Bytes</td>
<td>Bytes pushed to the stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>PutMessagesThroughput</td>
<td>Put Messages Records/sec</td>
<td>count</td>
<td>Count of messages pushed to stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>PutMessagesThroughput</td>
<td>Put Messages Throttled Records/sec</td>
<td>count</td>
<td>Number of put messages throttled either due to volume or requests measured over time.</td>
<td></td>
</tr>
<tr>
<td>PutMessagesSuccess</td>
<td>Put Messages Success/sec</td>
<td>count</td>
<td>Successful requests for put messages per stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>PutMessagesFailure</td>
<td>Put Messages Failure/sec</td>
<td>count</td>
<td>Total failed putMessage requests per stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>PutMessagesRecords</td>
<td>Put Messages Requests/sec</td>
<td>count</td>
<td>Number of messages published to a stream measured over time.</td>
<td></td>
</tr>
</tbody>
</table>

### Consumers

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetMessagesLatency</td>
<td>Get Messages Latency</td>
<td>time (s)</td>
<td>Time taken for get messages operation measured over time range.</td>
<td>region,resourceId</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Display Name</td>
<td>Unit</td>
<td>Description</td>
<td>Dimensions</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>GetMessagesThroughput.Bytes</td>
<td>Get Messages Total Throughput</td>
<td>Bytes</td>
<td>Bytes retrieved from stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>GetMessagesThroughput.Count</td>
<td>Get Messages Requests/sec</td>
<td>count</td>
<td>Count of messages read from stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>GetMessagesThroughput.Count</td>
<td>Get Messages Throttled Requests/sec</td>
<td>count</td>
<td>Number of get messages throttled either due to volume or requests measured over time.</td>
<td></td>
</tr>
<tr>
<td>GetMessagesSuccess.Count</td>
<td>Get Messages Success/sec</td>
<td>count</td>
<td>Successful requests for get messages per stream measured over time.</td>
<td></td>
</tr>
<tr>
<td>GetMessagesFailure.Count</td>
<td>Get Messages Failure/sec</td>
<td>count</td>
<td>Total failed getMessage requests per stream measured over time.</td>
<td></td>
</tr>
</tbody>
</table>

**Stream Health**

A healthy stream is a stream that is active: messages are received and consumed successfully.

 Writes to the service are durable. If you can produce to your stream, and if you get a successful response, then the stream is healthy.

 After data is ingested, it is accessible to consumers for the configured retention period. If GetMessages API calls return elevated levels of internal server errors, the service isn't healthy.

 A healthy stream also has healthy metrics:

- **Put Messages Latency** is low.
- **Put Messages Total Throughput** is close to 1 MB per second per partition.
- **Put Messages Throttled Records** is close to 0.
- **Put Messages Failure** is close to 0.
- **Get Messages Latency** is low.
- **Get Messages Total Throughput** is close to 2 MB per second per partition.
- **Get Messages Throttled Requests** is close to 0.
- **Get Messages Failure** is close to 0.

**Suggested Alarms**

**Producers**

For producers, consider setting alarms on the following metrics:

- **Put Messages Latency**: An increase in latency means that the messages are taking longer to publish, which could indicate network issues.
Streaming Service Overview

- **Put Messages Total Throughput:**
  - An increase in total throughput could indicate that the 1 MB per second per partition limit will be reached, and that event will trigger the throttling mechanism.
  - A decrease could mean that the client producer is having an issue or is about to stop.
- **Put Messages Throttled Records:** It's important to get notified when messages are throttled.
- **Put Messages Failure:** It's important to get notified if put messages start failing.

**Consumers**

For consumers, consider setting similar alarms based on the following metrics:

- Get Messages Latency
- Get Messages Total Throughput
- Get Messages Throttled Requests
- Get Messages Failure

**Using the Console**

**To view default producer metrics**

1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Click a stream to view its details.
3. Under **Resources**, click **Produce Monitoring Charts**.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**To view default consumer metrics**

1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Click a stream to view its details.
3. Under **Resources**, click **Consume Monitoring Charts**.

For more information about monitoring metrics and using alarms, see **Monitoring Overview** on page 2660. For information about notifications for alarms, see **Notifications Overview** on page 3350.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use the following APIs for monitoring:

- **Monitoring API** for metrics and alarms
- **Notifications API** for notifications (used with alarms)

**Troubleshooting Streaming**

This topic covers various issues related to Oracle Cloud Infrastructure Streaming and how you can address them. Details about common API errors that all services return are detailed in **API Errors** on page 4372.

**Troubleshooting Access and Permissions**

**Request returns a "Processing exception while communicating" message and a -1 error**

When you use the Streaming client to send a request, you might see the following error message:

```
Caused by: com.oracle.bmc.model.BmcException: (-1, null, false) Processing exception while communicating to:
```
This error is related to the client. The Streaming service doesn't send it, which means that the request never made it to the service.

**Request returns a NotAuthorizedOrNotFound message and a 404 error**

When you send a request to Streaming, you might see an error message similar to the following:

```
com.oracle.bmc.model.BmcException: (404, NotAuthorizedOrNotFound,false)
Unknown stream ocid1.stream.oc1.phx.exampleuniqueID.
(opc-request-id: <opc_request_id>)
```

A 404 error usually means that the needed resource isn't found or that you don't have access to it. An example is when the stream-push policy is missing, or the stream has been deleted or is not accessible. Ensure that all the permissions are correctly set.

**Request returns a "Not Found" message and a 404 error**

When you send a request to Streaming, you might see an error message similar to the following:

```
redirected: false, status: 404, ok: false, statusText: "Not Found", headers: Headers, bodyUsed: false }
```

This error indicates a permission-related issue. Ensure that all the permissions are correctly set.

**Request returns a "The following tag namespaces/keys are not authorized or not found" message**

This error suggests that there is a tag on the stream that your user is not authorized to use. Remove the tag or authorize the user. See Resource Tags on page 211 for more information.

**Request returns a "bad handshake" message and a 104 error**

When you send a request to Streaming, you might see an error message similar to the following:

```
SSLLError(SSLError("bad handshake: SysCallError(104, 'ECONNRESET'.))
```

This error typically means that your system doesn't have the CA that the certificates were signed by. You may need to install the ca-certificates package on your host or pull the CA certificate from the target endpoint and import it into your system trust store by using `update-ca-trust` command.

**Troubleshooting Limits and Throttling**

Limits on Streaming Resources on page 3856 describes the service and resource limits that might result in the following scenarios.
Partial failures
Streaming supports partial failures caused by throttling, per partition. When a partial failure occurs, the service returns a \texttt{200} status code and indicates the failure in the response payload.

If an entire request is throttled, Streaming returns a \texttt{429} status code.

Request returns a "Too many requests message" and a 429 error
When you send a request to Streaming, you might see an error message that includes the following:

\begin{verbatim}
(429, Too many requests)
\end{verbatim}

This error is caused by the throttling mechanism in the service. It indicates that too many requests per second per partition are being received.

If this error occurs on the producer side, ensure that the total data write rate of 1 MB per second per partition is not exceeded by:

- Lowering the amount of requests per second.
- Decreasing message size by batching.

If this error occurs on the consumer side, ensure that:

- The cursor uses \texttt{commitOnGet(true)}.
- You reduce the number of requests, keeping in mind that the maximum data read rate is 5 GET requests per second per partition per consumer group.
- The \texttt{limit} is set for each GET request.

Request returns a "Request size is limited to 1 MiB" message and a 400 error
When you send a request to Streaming, you might see an error message similar to the following:

\begin{verbatim}
Exception in thread "main" com.oracle.bmc.model.BmcException: (400, InvalidParameter, false) Request size is limited to 1 MiB. (opc-request-id: \texttt{<opc_request_id>})
at com.oracle.bmc.http.internal.ResponseHelper.throwIfNotSuccessful(ResponseHelper.java:129)
at com.oracle.bmc.streaming.internal.http.PutMessagesConverter$1.apply(PutMessagesConverter.java:54)
at com.oracle.bmc.streaming.StreamClient.putMessages(StreamClient.java:466)
\end{verbatim}

This error occurs because the \texttt{PutMessages} call sent to the service is too large. The size must be less than or equal to 1 MB.

Stream creation fails with a "You exceed the number of allowed partitions" message
This error occurs when you try to create more partitions than your tenancy is allowed. You can request an increase.
Troubleshooting Production and Consumption

Messages do not appear in the Console after publishing them to a stream

You must click the Refresh button to show the first 100 messages. See Using the Console to show recent messages for more information.

Because streams using private endpoints are not accessible from the internet, their messages do not display in the Console.

Consumers receive a "The cursor is outside the retention period and is now invalid" message and a 400 error

When requesting messages from a stream, a consumer might see an error message like the following:

```
(400, InvalidParameter, false) The cursor is outside the retention period and is now invalid
```

This error means that the offsets stored for one or more of your partitions has fallen behind the trim horizon. Some data loss has occurred, and the data that was produced to the stream is no longer available for consumption. Data that is outside the retention period can't be recovered. At this point, the administrator must decide the best course of action, given the use case.

This error can happen if you are not committing offsets regularly, or if your consumer falls behind constantly. For more information, see Getting Messages on page 3874.

A manual call to the UpdateGroup method is required to reset the cursor for the instances within a consumer group.

Consumers receive a "Trying to commit unreserved partition" message and a 400 error

When requesting messages from a stream, a consumer that is part of a consumer group might see an error message like the following:

```
(400, InvalidParameter, false) Trying to commit unreserved partition
```

This error means that the consumer tried to commit an offset for a partition that was not reserved for that particular consumer. This error can happen when the consumer appears to have timed out, partitions are rebalanced to another consumer, and then the consumer tries to commit offsets. The default timeout is 30 seconds for a consumer. Timeouts for a consumer can be extended by sending a heartbeat. See Consuming as a Group on page 3877 for more information.

This error can also occur when pipelining (commitOnGet=false) and no commits occurred for a significant amount of time (more than 30 seconds).

Request fails with an "Unable to parse JSON body" message and a 400 error

When you send a request to Streaming, you might see an error message similar to the following:

```
(400, Unable to parse JSON body)
```

This error generally means that the JSON body contains an entry in an invalid format.

Ruby SDK requests fail with an "Unable to parse JSON body" message and a 400 error

When you send a request to Streaming using the Ruby SDK, you might see an error message similar to the following:

```
Unable to parse JSON body, 'status': 400, 'code': 'InvalidParameter'
```
The Ruby SDK doesn't do any encoding. You must use `Base64` to encode the strings that are sent in the key and value fields. For example:

```ruby
msgs << OCI::Streaming::Models::PutMessagesDetailsEntry.new(key: Base64.strict_encode64(k), value: Base64.strict_encode64(record.to_json))
if msgs.length > 0
  res = @oss_client.put_messages(@stream_ocid,
    OCI::Streaming::Models::PutMessagesDetails.new(messages: msgs))
end
```

### Troubleshooting Streaming and Kafka

**Kafka Connect configuration creation fails**

When you try to create a Kafka Connect configuration, you might see an error message like the following:

```
You are not authorized to create Kafka Connect Configurations
```

To create a Kafka Connect configuration, you need to create the correct IAM policy in your tenancy. For example:

```
Allow group xyz to manage connect-harnesses in tenancy
```

See [Managing Kafka Connect Configurations](#) on page 3885 for more information.
Tagging

This chapter explains how to use tags to add metadata to your resources.

Tagging Overview

Oracle Cloud Infrastructure Tagging allows you to add metadata to resources, which enables you to define keys and values and associate them with resources. You can use the tags to organize and list resources based on your business needs.

Caution:

Avoid entering confidential information when assigning descriptions, tags, or friendly names to your cloud resources through the Oracle Cloud Infrastructure Console, API, or CLI.

How Tagging Works

The Tagging service provides two ways for you to add tags to resources. Each approach offers a different type of tag for you to work with:

- Defined tags - tag administrators manage resource metadata.
- Free-form tags - unmanaged metadata applied to resources by users.

One approach involves a tag administrator creating and managing all the tags that users apply to resources. Use IAM policy to select tag administrators, who can create tags. Grant all others in the tenancy only the ability to apply tags. The benefit to this approach is that you can create and manage the keys and values used to tag resources. You can then avoid typos that weaken automation based on tags and provide better reporting based on tags.

The other approach is to allow users to add tags to resources. Each tag is edited or applied at the resource by you or a user creating or modifying a resource. You can use both types of tags throughout your tenancy.

Most of the Tagging features require defined tags. "Tag" is used generically to refer to defined tags. To create metadata that you can trust to manage resources and collect data, use defined tags. With defined tags, the following scenarios become possible:

- Create default tags that are applied to all resources in compartments. See Managing Tag Defaults on page 3927.
- Specify that users must apply tags to resources to successfully create resources in compartments.
- If you make a typo using defined tags, correct it by editing or even deleting the tag. When you delete a defined tag, Oracle removes the key and any value for that tag from all resources. See Deleting Tag Key Definitions and Namespaces on page 3917.
- Associate a list of predefined values for a defined tag. See Using Predefined Values on page 3924.
- Use system variables to generate values for defined tags or tag defaults automatically. See Using Tag Variables on page 3926.
- Track costs based on tags. Use of defined tags is recommended for this use case.
- Set budgets using cost-tracking tags to be alerted when your spending reaches specified levels. See Using Cost-Tracking Tags on page 3923.
Tagging Concepts

Here's a list of the basic tagging concepts:

**TAG NAMESPACE**

You can think of a tag namespace as a container for your tag keys. It consists of a name and zero or more tag key definitions. Tag namespaces are not case sensitive and must be unique across the tenancy. The namespace is also a natural grouping to which administrators can apply policy. One policy on the tag namespace applies to all the tag definitions contained within that namespace.

**TAG KEY**

The name you use to refer to the tag. Tag keys are case insensitive. For example, "mytagkey" duplicates "MyTagKey". You must create tag keys for defined tags in a namespace. Each tag key must be unique within a namespace.

**TAG VALUE TYPE**

The tag value type specifies the data type allowed for the value. Currently two data types are supported: string and a list of strings.

**KEY DEFINITION**

A key definition defines the schema of a tag and includes a namespace, tag key, and tag value type.

**TAG VALUE**

The tag value is the value that the user applying the tag adds to the tag key. Tag values support two data types: strings and lists of strings. You can define a list of values for the user to select from when you define the tag key, or you can allow the user to enter any value when the tag is applied to the resource. If you select a string tag value when you create the key, the user can leave the value blank when they apply the key.

In the example:

```
Operations.CostCenter="42"
```

Operations is the namespace, CostCenter is the tag key, and 42 is the tag value.

**TAG (OR DEFINED TAG)**

A tag is the instance of a key definition that is applied to a resource. It consists of a namespace, a key, and a value. "Tag" is used generically to refer to defined tags.

**FREE-FORM TAG**

A basic metadata association that consists of a key and a value only. Free-form tags have limited functionality. See Understanding Free-form Tags on page 3922.

**COST TRACKING**

Cost tracking is a feature available with defined tags. This feature is being deprecated and is currently only relevant for use with Budgets. To understand when you need to designate a tag as a cost-tracking Tag, see Using Cost-Tracking Tags on page 3923.

**TAG DEFAULT**

Tag defaults let you specify tags that are applied automatically to all resources in a specific compartment at the time of creation, regardless of the permissions of the user who creates the resource. See Managing Tag Defaults on page 3927.

**RETIRE**

You can retire a tag key definition or a tag namespace. Retired tag namespaces and key definitions can no longer be applied to resources. However, retired tags are not removed from the resources to which they have already been applied. You can still specify retired tags when searching, filtering, reporting, and so on.
Tagging

REACTIVATE

You can reactivate a tag namespace or tag key definition that has been retired to reinstate its usage in your tenancy.

TAG VARIABLE

You can use a variable to set the value of a tag. When you add or update a tag on a resource, the variable resolves to the data it represents. See Using Tag Variables on page 3926.

PREDEFINED VALUES

You can use a variable to set the value of a tag. When you add or update a tag on a resource, the variable resolves to the data it represents. See Using Predefined Values on page 3924.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

For administrators: Use the following topics to find example of IAM policy for Tagging:

- Required Permissions for Working with Defined Tags on page 3915
- Required Permissions for Working with Tag Defaults on page 3928
- Required Permissions for Working with Free-form Tags on page 3922

Region Availability

Tagging is currently available in all regions.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser.

Oracle Cloud Infrastructure supports the following browsers and versions:

- Google Chrome 69 or later
- Safari 12.1 or later
- Firefox 62 or later

Limits on Tags

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase.

- Tags per tenancy: unlimited
- Tags per resource: 10 free-form tags and 64 defined tags
- Tags enabled for cost-tracking: 10 per tenancy (includes both active and retired tags)
- Total tag data size: 5 K (JSON). The total tag data size includes all tag data for a single resource (all applied tags and tag values). Sizing is per UTF-8.
Tagging

- Number of pre-defined values for a tag key: 100 per list

<table>
<thead>
<tr>
<th>Resource</th>
<th>Supported Characters</th>
<th>Max Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag namespace</td>
<td>Printable ASCII, excluding periods (.) and spaces</td>
<td>100 characters</td>
</tr>
<tr>
<td>Tag key name (free-form and defined)</td>
<td>Printable ASCII, excluding periods (.) and spaces</td>
<td>100 characters</td>
</tr>
<tr>
<td>Tag value (free-form and defined)</td>
<td>Unicode characters</td>
<td>256 characters</td>
</tr>
</tbody>
</table>

**Resources That Can Be Tagged**

The following table lists resources that support tagging. This table will be updated as tagging support is added for more resources.

<table>
<thead>
<tr>
<th>Service</th>
<th>Taggable Resource Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics Cloud</td>
<td>analytics-instances</td>
</tr>
<tr>
<td>API Gateway</td>
<td>api-deployments</td>
</tr>
<tr>
<td></td>
<td>api-gateways</td>
</tr>
<tr>
<td>Application Migration</td>
<td>ams-migration</td>
</tr>
<tr>
<td></td>
<td>ams-source</td>
</tr>
<tr>
<td></td>
<td>ams-work-request</td>
</tr>
<tr>
<td>Audit</td>
<td>audit-events</td>
</tr>
<tr>
<td>Big Data</td>
<td>bds-instances</td>
</tr>
<tr>
<td>Block Volume</td>
<td>volumes</td>
</tr>
<tr>
<td></td>
<td>volume-backups</td>
</tr>
<tr>
<td></td>
<td>backup-policies</td>
</tr>
<tr>
<td></td>
<td>boot-volume-backups</td>
</tr>
<tr>
<td>Blockchain Platform</td>
<td>blockchain-platforms</td>
</tr>
<tr>
<td>Budgets</td>
<td>usage-budgets</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>managed-lists</td>
</tr>
<tr>
<td></td>
<td>targets</td>
</tr>
<tr>
<td>Service</td>
<td>Taggable Resource Types</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------</td>
</tr>
</tbody>
</table>
| **Compute**               | auto-scaling-configurations  
<p>|                           | cluster-networks         |
|                           | instance                 |
|                           | instance-configurations   |
|                           | instance-image            |
|                           | instance-pools            |
|                           | instanceconsoleconnections |
| <strong>Content and Experience</strong>| oce-instances             |
| <strong>Data Catalog</strong>          | data-catalogs            |
|                           | data-catalog-data-assets  |
|                           | data-catalog-glossaries   |
| <strong>Data Flow</strong>             | dataflow-applications     |
|                           | dataflow-runs             |
| <strong>Data Integration</strong>      | workspaces                |
| <strong>Data Safe</strong>             | data-safe                 |
| <strong>Data Science</strong>          | data-science-models       |
|                           | data-science-notebook-sessions |
|                           | data-science-projects     |
| <strong>Database</strong>              | autonomous-databases      |
|                           | db-systems                |
|                           | databases                 |
| <strong>Digital Assistant</strong>     | oda-instances             |
| <strong>DNS</strong>                   | dns-steering-policies     |
|                           | dns-tsig-keys             |
|                           | dns-zones                 |
| <strong>Email Delivery</strong>        | approved-senders          |
| <strong>Events</strong>                | cloudevents-rules         |
| <strong>File Storage</strong>          | file-systems              |
|                           | mount-targets             |
|                           | snapshots                 |
| <strong>Functions</strong>             | fn-app                    |
|                           | fn-function               |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Taggable Resource Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Checks</td>
<td>health-check-monitor</td>
</tr>
<tr>
<td>IAM</td>
<td>compartments, dynamic-groups, groups, identity-providers, network-sources, policies, tenancy (root compartment), users</td>
</tr>
<tr>
<td>Integration</td>
<td>integration-instances</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>load-balancers</td>
</tr>
<tr>
<td>Logging Analytics</td>
<td>loganalytics-entity, loganalytics-log-group</td>
</tr>
<tr>
<td>Management Agent</td>
<td>management-agents</td>
</tr>
<tr>
<td>Monitoring</td>
<td>alarms</td>
</tr>
<tr>
<td>MySQL Database</td>
<td>mysql-configurations, mysql-instances, mysql-backups</td>
</tr>
<tr>
<td>Service</td>
<td>Taggable Resource Types</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Networking, FastConnect</td>
<td>cpes</td>
</tr>
<tr>
<td></td>
<td>cross-connects</td>
</tr>
<tr>
<td></td>
<td>cross-connect-groups</td>
</tr>
<tr>
<td></td>
<td>dhcp-options</td>
</tr>
<tr>
<td></td>
<td>drgs</td>
</tr>
<tr>
<td></td>
<td>internet-gateways</td>
</tr>
<tr>
<td></td>
<td>ipsec-connections</td>
</tr>
<tr>
<td></td>
<td>ipv6s</td>
</tr>
<tr>
<td></td>
<td>ipsec-connections</td>
</tr>
<tr>
<td></td>
<td>local-peering-gateways</td>
</tr>
<tr>
<td></td>
<td>nat-gateways</td>
</tr>
<tr>
<td></td>
<td>network-security-groups</td>
</tr>
<tr>
<td></td>
<td>private-ips</td>
</tr>
<tr>
<td></td>
<td>public-ips</td>
</tr>
<tr>
<td></td>
<td>remote-peering-connections</td>
</tr>
<tr>
<td></td>
<td>route-tables</td>
</tr>
<tr>
<td></td>
<td>security-lists</td>
</tr>
<tr>
<td></td>
<td>service-gateways</td>
</tr>
<tr>
<td></td>
<td>subnets</td>
</tr>
<tr>
<td></td>
<td>vcns</td>
</tr>
<tr>
<td></td>
<td>virtual-circuits</td>
</tr>
<tr>
<td></td>
<td>vnics</td>
</tr>
<tr>
<td></td>
<td>vnic-attachments</td>
</tr>
<tr>
<td>Notifications</td>
<td>ons-subscriptions</td>
</tr>
<tr>
<td></td>
<td>ons-topics</td>
</tr>
<tr>
<td>Object Storage, Data Transfer, and Archive Storage</td>
<td>buckets</td>
</tr>
<tr>
<td></td>
<td>data-transfer-jobs</td>
</tr>
<tr>
<td>OS Management</td>
<td>osms-managed-instances</td>
</tr>
<tr>
<td></td>
<td>osms-managed-instance-groups</td>
</tr>
<tr>
<td></td>
<td>osms-software-sources</td>
</tr>
<tr>
<td></td>
<td>osms-scheduled-jobs</td>
</tr>
<tr>
<td>Quotas Service</td>
<td>quota</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>orm-jobs</td>
</tr>
<tr>
<td></td>
<td>orm-stacks</td>
</tr>
</tbody>
</table>
Managing Tags and Tag Namespaces

Oracle Cloud Infrastructure supports two kinds of tags: free-form tags and defined tags.

<table>
<thead>
<tr>
<th>Service</th>
<th>Taggable Resource Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>resourcesummary</td>
</tr>
<tr>
<td>Service Connector Hub</td>
<td>service-connectors</td>
</tr>
<tr>
<td>Streaming</td>
<td>connect-harnesses</td>
</tr>
<tr>
<td></td>
<td>streams</td>
</tr>
<tr>
<td></td>
<td>streampools</td>
</tr>
<tr>
<td>Tagging</td>
<td>tag-namespaces</td>
</tr>
<tr>
<td></td>
<td>tag-definitions (API only)</td>
</tr>
<tr>
<td>Vault</td>
<td>keys</td>
</tr>
<tr>
<td></td>
<td>vaults</td>
</tr>
<tr>
<td></td>
<td>key-delegate</td>
</tr>
<tr>
<td>WAF</td>
<td>http-redirects</td>
</tr>
<tr>
<td></td>
<td>waas-address-list</td>
</tr>
<tr>
<td></td>
<td>waas-certificate</td>
</tr>
<tr>
<td></td>
<td>waas-custom-protection-rule</td>
</tr>
<tr>
<td></td>
<td>waas-policy</td>
</tr>
</tbody>
</table>

Tip:
Watch a video to introduce you to the concepts and features of tagging: Introduction to Tagging.

Required IAM Policy

If you're in the Administrators group, then you have the required access for managing tag namespaces and tags. For more policy samples specific to working with tags and tag namespaces, see Required Permissions for Working with Defined Tags on page 3915.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.

Overview of Tags and Tag Namespaces

Defined tags provide more features and control than free-form tags. Before you create a defined tag key, you first set up a tag namespace for it. You can think of the tag namespace as a container for a set of tag keys. When you create the tag key definition, you must choose the type of value (which also determines how the user applying the tag adds the value):

- You can leave it empty so that a user can fill in the value.
- You can create a list of values so that the user must choose from those values.

To apply a defined tag to a resource, a user first selects the tag namespace, then the tag key within the namespace, and then they can assign the value. If the tag key contains a blank value, the user can type in a value or leave it blank. If the tag key contains a list, the user must select a value from the list.
Defined tags support policy to allow you to control who can apply your defined tags. The tag namespace is the entity to which you can apply policy. Administrators can control which groups of users are allowed to use each namespace.

The following diagrams illustrate defined tags. Two tag namespaces are set up: Operations and HumanResources. The tag keys are defined in the namespaces. Within each namespace, the tag keys must be unique, but a tag key name can be repeated across namespaces. In the example, both namespaces include a key named "Environment."

The first instance is tagged with two tags from the Operations tag namespace, indicating that it belongs to the Operations production environment and the Operations project "Alpha". The second instance is tagged with tags from both the HumanResources tag namespace and the Operations tag namespace, indicating that it belongs to the HumanResources "Production" environment, the HumanResources cost center "42", and also the Operations project "Beta".

**Working with Defined Tags**

You must set up the tag namespace and tag keys in your tenancy before users can apply a defined tag to a resource. As part of the set up process, you must also grant permissions to the user groups that needs to use the namespace.

**Note:**

Tag namespaces and tag key definitions beginning with "oci" and "orcl" are reserved for internal use.

Features of defined tags include:

- Consist of a tag namespace, a key, and a value.
• The tag namespace and tag key definition must be set up in your tenancy before users can apply a defined tag to a resource.
• You can create the tag key with either a tag value type of string (for the user to add a value or leave blank) or a list of values (from which the user must choose).
• When applying a defined tag, users select from the list of tag keys.
• Users can apply a defined tag during resource creation or to an existing resource.
• Defined tag keys are case insensitive.
• Defined tag values are case sensitive. For example, "alpha" and "Alpha" are distinct values.
• You can use tag variables.
• You can create a list of predefined variables to associate with a tag key. Users that apply the tag to a resource must select a value from the list you create.

**Required Permissions for Working with Defined Tags**

To apply, update, or remove defined tags for a resource, a user must be granted permissions on the resource and permissions to use the tag namespace.

Users must be granted `use` access on the `tag namespace` to apply, update, or remove a defined tag for a resource.

Some example policies for tag namespaces:

To allow a group to simply view the tag namespaces in the tenancy (or in a compartment) requires `inspect` access:

```
Allow group GroupA to inspect tag-namespaces in tenancy
```

**Important:**

To apply tags to a resource when using the Console, a user must have permissions to `inspect tag-namespaces in tenancy`. If the user does not have this permission, the list of tag namespaces cannot be presented to the user in the dialog menu.

To allow a group to read the tag definitions contained in tag namespaces requires `read` access:

```
Allow group GroupA to read tag-namespaces in tenancy
```

To allow a group to apply, update, or remove a defined tag for a resource requires the `use` access on the tag namespace:

```
Allow group GroupA to use tag-namespaces in tenancy
```

To allow usage of a specific tag namespace or namespaces, use a `where` clause with the `target.tag-namespace.name` variable. For example:

```
Allow group GroupA to use tag-namespaces in tenancy where target.tag-namespace.name='Operations'
```

or to specify multiple tag namespaces:

```
Allow group GroupA to use tag-namespaces in tenancy where any {target.tag-namespace.name='Operations', target.tag-namespace.name='HumanResources'}
```

To manage tag namespaces and the tag definitions in them, requires `manage` access:

```
Allow group GroupA to manage tag-namespaces in tenancy
```

In addition to the permissions to work with the tag namespace, to apply or remove defined tags on a resource you must have the update permission for the resource. For many resources, the update permission is granted with the `use`
Tagging

verb. For example, users who can use instances in CompartmentA can also apply, update, or remove defined tags for instances in CompartmentA.

Some resources don't include the update permission with the use verb. To allow a group to apply, update, or remove defined tags for these resources without granting the full permissions of manage, you can add a policy statement to grant only the `<RESOURCE>_UPDATE` permission from the manage verb. For example, to allow a group NetworkUsers to work with defined tags with VCNs in CompartmentA, you could write a policy like:

```
Allow group NetworkUsers to use vcns in compartment CompartmentA
Allow group NetworkUsers to manage vcns in compartment CompartmentA where request.permission='VCN_UPDATE'
```

The inspect permission for a resource grants permissions to view defined tags for that resource. For example, users who can inspect instances can also view any defined tags applied to the instance.

For information about resource permissions, see Policy Reference on page 2167.

**Example Scenario**

Your company has an Operations department. Within the Operations department are several cost centers. You want to be able to tag resources that belong to the Operations department with the appropriate cost center.

1. Create a tag namespace definition called Operations.
2. In the Operations namespace, create a tag key definition called CostCenter.

Alice already belongs to the group InstanceLaunchers. Alice can manage instances in CompartmentA. You want Alice and other members of the InstanceLaunchers group to be able to apply the Operations.CostCenter tag to instances in CompartmentA.

To grant the InstanceLaunchers group access to the Operations tag namespace (and only the Operations tag namespace), add the following statements to the InstanceLaunchers policy:

```
Allow group InstanceLaunchers to use tag-namespaces in compartment CompartmentA where target.tag-namespace.name='Operations'
```

Alice can now apply the Operations.CostCenter tag to resources in CompartmentA.

**Retiring Key Definitions and Namespace Definitions**

You can retire a tag key definition or a tag namespace definition.

When you retire a tag key definition, you can no longer apply it to resources. However, the tag is not removed from the resources that it was applied to. The tag still exists as metadata on those resources and you can still call the retired tag in operations (such as listing, sorting, or reporting).

**Important:**

Retiring a tag stops cost tracking for the tag, but if you do not disable the cost-tracking option on the tag key definition, the retired tag continues to count against your maximum of 10 cost-tracking tags for your tenancy. Disable cost tracking before you retire the tag key definition. To disable cost-tracking after a tag is retired, you must reactivate the tag key definition. You can't update tag key definitions that are in the retired state.

**Reactivating Tag Key Definitions and Namespace Definitions**

You can reactivate retired tag key definitions and tag namespace definitions.

- When you reactivate a tag key, it is again available for you to apply to resources.
• When you reactivate a tag namespace, you can create new tag key definitions in that namespace. However, if you want to use any of the tag key definitions that were retired with the namespace, you must explicitly reactivate each tag key definition.

Moving Tag Namespaces to a Different Compartment

You can move a tag namespace to a different compartment. The tag namespace can be active or retired when you move it. When you move the tag namespace, all its tag key definitions are moved along with it.

This functionality is useful if you need to reorganize your compartment hierarchy, or if you need to delete a compartment that contains a retired tag namespace. Remember that you can't delete a compartment that contains resources. A retired tag namespace, even though it is retired, is still an existing resource. Moving the retired tag namespace to a different compartment can enable you to delete its original containing compartment.

To move a tag namespace, you must be allowed to manage tag-namespaces in both compartments.

See the procedure To move a tag namespace to a different compartment on page 3918.

Deleting Tag Key Definitions and Namespaces

You can delete tag key definitions and tag namespaces.

When you delete a tag key definition, you begin a process that removes the tag from all resources in your tenancy. These things happen immediately:

• If the tag was a cost-tracking tag, it no longer counts against your 10 cost-tracking tags limit, whether you first disabled it or not.
• If the tag was used with dynamic groups, none of the rules that contain the tag will be evaluated against the tag.

The delete action is asynchronous and initiates a work request. Once you start the delete operation, the state of the tag changes to deleting, and tag removal from resources begins. This process can take up to 48 hours depending on the number of resources that were tagged as well as the regions in which those resources reside. When all tags are removed, the state changes to deleted. You cannot restore a deleted tag. After the tag state changes to Deleted, you can use the same tag name again.

To delete a tag key definition, you must first retire it. To delete a tag namespace, you must first retire the tag namespace. When you retire a tag namespace that contains tag key definitions, all the tag keys in the namespace are retired, allowing you to delete the tag namespace.

Using the Console

Managing Tag Namespaces

To create a tag namespace

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.

   A list of the tag namespaces in your current compartment is displayed.

2. Click Create Namespace Definition.

3. Enter the following:

   • **Create in Compartment**: The compartment in which you want to create the namespace definition.
   • **Namespace Definition Name**: A unique name for this set of tags. The name must be unique within your tenancy. Tag namespace is case insensitive. You cannot change this value later. Avoid entering confidential information.
   • **Description**: A friendly description. You can change this value later if you want to.

4. Click Create Namespace Definition.
To update a tag namespace's description

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.
   A list of the tag namespaces in your tenancy is displayed.
2. Click the tag namespace you want to update.
   The namespace's details are displayed. The description is displayed under the namespace's name.
3. Click the pencil next to the description.
4. Edit the description and save it. Avoid entering confidential information.

To retire a tag namespace

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.
   A list of the tag namespaces in your current compartment is displayed.
2. Click the tag namespace you want to retire.
   The namespace's details are displayed.
3. Click Retire Tag Namespace.
4. Confirm when prompted.

To reactivate a tag namespace

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.
   A list of the tag namespaces in your current compartment is displayed.
2. Click the tag namespace you want to reactivate.
   The namespace's details are displayed.
3. Click Reactivate Tag Namespace.
4. Confirm when prompted.

To move a tag namespace to a different compartment

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.
   A list of the tag namespaces in your current compartment is displayed.
2. Click the tag namespace you want to move.
   The namespace's details are displayed.
3. Click Move Tag Namespace.
4. Select the Target Compartment that you want to move the tag namespace to.
5. Click Move Tag Namespace.

To delete a tag namespace

To delete a tag namespace, you must first retire it.

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.
   A list of the tag namespaces in your current compartment is displayed.
2. Click the tag namespace that you want to delete.
   The namespace's details are displayed.
3. Click **Delete Tag Namespace**.

   **Tip:**

   If the **Delete Tag Namespace** option is unavailable, first retire your tag namespace.

4. Confirm when prompted.

### Managing Key Definitions

#### To create a key definition

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tag Namespaces**.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace you want to add the tag key definition to.

   A list of the tag key definitions that belong to the namespace is displayed.

3. Click **Create Tag Key Definition**.

4. Enter the following:

   - **Tag Key:** Enter the key. The key can be up to 100 characters in length. Tag keys are case insensitive and must be unique within the tag namespace. Avoid entering confidential information.
   - **Description:** Enter a friendly description.
   - **Cost-tracking:** Select the check box to enable this tag for cost tracking. You have a limit of 10 Using Cost-Tracking Tags on page 3923 in your tenancy.

5. Under **Tag Value Type**, choose one of the following:

   - **Static Value:** Specifies that the user applying the tag can specify any value for this key.
   - **A List of Values:** Specifies that the user must apply a value from a list you create. When you select this option, the **Values** box appears. Type the values from which the user can select. Separate multiple values with new lines. You must have at least one value. You can't have blank lines or duplicate values.

6. Click **Create Tag Key Definition**.

#### To update a tag key definition

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tag Namespaces**.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace that includes the tag key definition you want to update.

   A list of the tag key definitions is displayed.

3. Click the tag key definition you want to update.

   The key definition's details are displayed.

4. Click **Edit Tag Key Definition**.

   The edit dialog appears.

   You can change the description, the tag value type, and enable or disable cost tracking. Avoid entering confidential information.

   If you chose a list of values, the **Values** box appears, and you must add at least one value. You can't have blank lines or duplicate values in the **Values** box.

   You have a limit of 10 Using Cost-Tracking Tags on page 3923 in your tenancy.

5. Make your changes and save it.
To retire a tag key definition

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace that includes the tag key definition you want to retire.

   A list of the tag key definitions is displayed.

3. Select the tag key definition you want to retire. To retire multiple tag key definitions at the same time, select all of the tag key definitions that you want to retire.

   **Important:**

   If the tag is a cost-tracking tag, disable the cost-tracking flag. If you don't disable cost-tracking, this tag will still count against your tenancy maximum of 10 cost-tracking tags, even after it is retired. For more information, see Using Cost-Tracking Tags on page 3923.

4. Click Retire.

5. Confirm when prompted.

To reactivate a tag key definition

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace that includes the tag key definition you want to reactivate.

   A list of the tag key definitions is displayed.

3. Select the tag key definition you want to reactivate. To reactivate multiple tag key definitions at the same time, select all of the tag key definitions that you want to reactivate.

4. Click Reactivate.

5. Confirm when prompted.

To delete a tag key definition

To delete a tag key definition, you must first retire it.

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace that includes the tag key definition you want to delete.

   A list of the tag key definitions is displayed.

3. Select the retired tag key definition you want to delete. To delete multiple tag key definitions at the same time, select all of the tag key definitions that you want to delete. You can delete up to five tag key definitions at the same time.

4. Click Delete.

   **Tip:**

   If the Delete option is unavailable, first retire your tag key definition.
5. Confirm when prompted.
   After you confirm, the state changes to Deleting. Track the progress of the operation using the work request.

**To track the progress of the delete operation**

a. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tag Namespaces**.
   A list of the tag namespaces in your current compartment is displayed.

b. Click the tag namespace that includes the tag key definition you deleted.
   A list of the tag key definitions is displayed.

c. Click **Work Requests**.
   The work requests for deleted tag definitions are displayed.

**To monitor a work request for a deleted tag**

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tag Namespaces**.
   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace that includes the tag key definition you deleted.
   A list of the tag key definitions is displayed.

3. Click **Work Requests**.
   The work requests for deleted tag definitions are displayed.

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage tag namespaces:

- **GetTagNamespace**
- **ListTagNamespaces**
- **CreateTagNamespace**
- **UpdateTagNamespace** - Use to retire or reactivate a tag namespace.
- **CascadeDeleteTagNamespace** - Use to delete a tag namespace and all of its tag key definitions. You must first retire the tag namespace.
- **DeleteTagNamespace** - Use to delete the tag namespace. You must first delete all of the tag key definitions contained in the tag namespace.
- **ChangeTagNamespaceCompartment**

Use these API operations to manage tag key definitions:

- **GetTag** - gets the tag key definition
- **ListTags** - lists tag key definitions
- **ListCostTrackingTags** - lists the tags that have been enabled for cost-tracking (can be performed in the root compartment only)
- **CreateTag** - creates a tag key definition
- **UpdateTag** - updates the tag key definition (use this operation to retire or reactivate a tag key)
- **DeleteTag** - deletes the tag key definition
- **BulkDeleteTags** - deletes multiple tag key definitions within a tag namespace

Use these API operations to manage work requests spawned by the DeleteTag operation:

- **ListTaggingWorkRequests**
- **ListTaggingWorkRequestErrors**
- **ListTaggingWorkRequestLogs**
Tagging

- GetTaggingWorkRequest

**Understanding Free-form Tags**

Oracle Cloud Infrastructure supports two kinds of tags: free-form tags and defined tags. This topic describes free-form tags.

Because free-form tags are limited in functionality, Oracle recommends that you only use them to try out the tagging feature in your system when you are first getting started with tagging. For more information about the features and limitations of free-form tags, see Working with Free-form Tags on page 3922.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for free-form tags. For more policy samples specific to working with free-form tags, see Required Permissions for Working with Free-form Tags on page 3922.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.

**Overview of Free-form Tags**

Free-form tags consist of a key and a value, for example:

Environment: Production

where "Environment" is the key and "Production" is the value.

You can apply multiple free-form tags to a single resource, up to the limit.

**Working with Free-form Tags**

Free-form tags consist of a key-value pair and have limited features. To experience the full feature set of tagging, use defined tags.

Features of free-form tags include:

- Consist of a key and a value. Free-form tags do not belong to a namespace.
- You can apply free-form tags during resource creation or to an existing resource.
- Free-form tag keys are case sensitive. For example, "Project" and "project" are distinct keys.
- Free-form tag values are case sensitive. For example, "alpha" and "Alpha" are distinct values.

Limitations of free-form tags include:

- When applying a free-form tag, you can't see a list of existing free-form tags, so you don't know what tags and values have already been used.
- You can't see a list of existing free-form tags in your tenancy.
- You can't use free-form tags to control access to resources. That is, you can't include free-form tags in IAM policies.
- You can't use tag variables in free-form tags.
- You can't use predefined values in free-form tags.

**Required Permissions for Working with Free-form Tags**

To apply, update, or remove free-form tags for a resource, you must have the update permission on the resource. For many resources, the update permission is granted with the use verb. For example, users who can use instances in CompartmentA can also apply, update, or remove free-form tags for instances in CompartmentA.
Tagging

Some resources do not include the update permission with the use verb. To allow a group to apply, update, or remove free-form tags for these resources without granting the full permissions of manage, you can add a policy statement to grant only the `<RESOURCE>_UPDATE` permission from the manage verb. For example, to allow a group NetworkUsers to work with free-from tags with VCNs in CompartmentA, you could write a policy like:

```
Allow group NetworkUsers to use vcns in compartment CompartmentA
Allow group NetworkUsers to manage vcns in compartment CompartmentA where request.permission='VCN_UPDATE'
```

The inspect verb for a resource grants permissions to view free-form tags for that resource. Therefore, users who can inspect instances in CompartmentA can also view any free-form tags applied to the instance.

For information about resource permissions, see Policy Reference on page 2167.

Using Cost-Tracking Tags

Cost-tracking tags are only relevant when you set budgets.

- You can only use a cost-tracking tag with defined tags.
- You cannot specify free-form tags as cost-tracking tags.
- You do not have to designate a tag as cost-tracking, in order for it to be exposed in Cost Analysis or Cost and Usage Reports.

Required IAM Policy

Cost tracking is a feature of defined tags. To allow users to work with cost tracking, use the same IAM policy for working with tag namespaces and tags. For more information, see Required Permissions for Working with Defined Tags on page 3915.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.

Working with Cost-Tracking Tags

Suppose you have a defined tag key definition called Finance.CostCenter. You enable this tag key definition for cost tracking. You apply the tag with a value of "W1" (Finance.CostCenter="W1") to some resources, and you apply the tag with a value of "C2" (Finance.CostCenter="C2") to other resources. These tags enables the following scenario:

- Create one budget for resources tagged "Finance.CostCenter=W1" and a second budget for resources tagged "Finance.CostCenter=C2". If spending surpasses a certain amount or is forecast to exceed a particular threshold, you can set up alerts that notify you.

Limits on Cost-Tracking Tags

- You can have a maximum of 10 tag key definitions enabled for cost-tracking in your tenancy at a time. For example, you could enable the Project tag key as a cost-tracking tag and have 75 different departments, but it only takes up 1 tag.

Using the Console

You can enable cost-tracking when you create a tag key definition, or you can update an existing tag key definition to enable cost tracking.

To create a key definition

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.
   A list of the tag namespaces in your current compartment is displayed.
2. Click the tag namespace you want to add the tag key definition to.
   A list of the tag key definitions that belong to the namespace is displayed.
3. Click **Create Tag Key Definition**.
4. Enter the following:
   - **Tag Key**: Enter the key. The key can be up to 100 characters in length. Tag keys are case insensitive and must be unique within the tag namespace. Avoid entering confidential information.
   - **Description**: Enter a friendly description.
   - **Cost-tracking**: Select the check box to enable this tag for cost tracking. You have a limit of 10 **Using Cost-Tracking Tags** on page 3923 in your tenancy.
5. Under **Tag Value Type**, choose one of the following:
   - **Static Value**: Specifies that the user applying the tag can specify any value for this key.
   - **A List of Values**: Specifies that the user must apply a value from a list you create. When you select this option, the **Values** box appears. Type the values from which the user can select. Separate multiple values with new lines. You must have at least one value. You can't have blank lines or duplicate values.
6. Click **Create Tag Key Definition**.

**To update a tag key definition**

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tag Namespaces**.
   A list of the tag namespaces in your current compartment is displayed.
2. Click the tag namespace that includes the tag key definition you want to update.
   A list of the tag key definitions is displayed.
3. Click the tag key definition you want to update.
   The key definition's details are displayed.
4. Click **Edit Tag Key Definition**.
   The edit dialog appears.
   You can change the description, the tag value type, and enable or disable cost tracking. Avoid entering confidential information.
   If you chose a list of values, the **Values** box appears, and you must add at least one value. You can't have blank lines or duplicate values in the **Values** box.
   You have a limit of 10 **Using Cost-Tracking Tags** on page 3923 in your tenancy.
5. Make your changes and save it.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.
- **ListCostTrackingTags** - lists the tags that have been enabled for cost-tracking (can be performed in the root compartment only)

**Using Predefined Values**

You can create a list of values and associate that list with a tag key definition. When users then apply the tag to a resource, they must select a value from the list of predefined values. Use lists of predefined values to impose limits on the values that users can apply to tags.
You can use predefined values with defined tags and default tags. You cannot create lists of predefined values for free-form tags.
**Tagging**

**Required IAM Policy**

Predefined values are a feature of defined tags. To allow users to work with predefined values, use the same IAM policy for working with tag namespaces and tags. For more information, see Required Permissions for Working with Defined Tags on page 3915.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.

**Working with Predefined Values**

You can update existing tags to use predefined values.

Every list of predefined values that you create must contain at least one value. Lists can't contain duplicate values or blank entries. With predefined values, users applying tags can't set the value of a tag to `null`. For more information, see Using the Console on page 3925.

**Predefined Values and Default Tags**

You can use predefined values and default tags to impose limits on the values that users can apply to tags.

Here's how it works:

1. You define a list of predefined values for a tag key.
2. You create a default tag that uses the key with the list of predefined values and requires that users who create resources in the compartment add the value to the tag.
3. Oracle prompts all users creating resources in the compartment to enter a tag value. Because the tag key contains a predefined list that you created, the value the user applies is a value that you trust.

These features help to ensure that new resources contain the values you expect. For more information, see Managing Tag Defaults on page 3927.

**Using the Console**

**To create a key definition**

1. Open the navigation menu. Under Governance and Administration, go to Governance and click Tag Namespaces.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace you want to add the tag key definition to.

   A list of the tag key definitions that belong to the namespace is displayed.

3. Click Create Tag Key Definition.

4. Enter the following:
   - **Tag Key**: Enter the key. The key can be up to 100 characters in length. Tag keys are case insensitive and must be unique within the tag namespace. Avoid entering confidential information.
   - **Description**: Enter a friendly description.
   - **Cost-tracking**: Select the check box to enable this tag for cost tracking. You have a limit of 10 Using Cost-Tracking Tags on page 3923 in your tenancy.

5. Under Tag Value Type, choose one of the following:
   - **Static Value**: Specifies that the user applying the tag can specify any value for this key.
   - **A List of Values**: Specifies that the user must apply a value from a list you create. When you select this option, the Values box appears. Type the values from which the user can select. Separate multiple values with new lines. You must have at least one value. You can't have blank lines or duplicate values.

6. Click Create Tag Key Definition.
To update a tag key definition

1. Open the navigation menu. Under **Governance and Administration**, go to **Governance** and click **Tag Namespaces**.

   A list of the tag namespaces in your current compartment is displayed.

2. Click the tag namespace that includes the tag key definition you want to update.

   A list of the tag key definitions is displayed.

3. Click the tag key definition you want to update.

   The key definition's details are displayed.

4. Click **Edit Tag Key Definition**.

   The edit dialog appears.

   You can change the description, the tag value type, and enable or disable cost tracking. Avoid entering confidential information.

   If you chose a list of values, the **Values** box appears, and you must add at least one value. You can't have blank lines or duplicate values in the **Values** box.

   You have a limit of 10 **Using Cost-Tracking Tags** on page 3923 in your tenancy.

5. Make your changes and save it.

Using the API

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

- **CreateTag** - creates a tag key definition
- **UpdateTag** - updates the tag key definition (use this operation to retire or reactivate a tag key)

Using Tag Variables

You can use a variable to set the value of a defined tag. When you add the tag to a resource, the variable resolves to the data it represents. You can use tag variables in defined tags and default tags. You cannot use tag variables in free-form tags.

Required IAM Policy

Tag variables are a feature of defined tags. To allow users to work with tag variables, use the same IAM policy for working with tag namespaces and tags. For more information, see **Required Permissions for Working with Defined Tags** on page 3915.

If you're new to policies, see **Getting Started with Policies** on page 2135 and **Common Policies** on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see **Details for IAM** on page 2280.

Working with Tag Variables

Consider the following example:

```plaintext
Operations.CostCenter="${iam.principal.name} at ${oci.datetime}"
```

Operations is the namespace, CostCenter is the tag key, and the tag value contains two tag variables `${iam.principal.name}` and `${oci.datetime}`. When you add this tag to a resource, the variables resolve to your user name (the name of the principal that applied the tag) and a time date stamp for when you added the tag.

```
user_name at 2019-06-18T18:00:57.604Z
```

The variable is replaced with data at the time that you apply the tag. If you later edit the tag, the variable is gone and only the data remains. You can edit the tag value in all the ways you would edit any other tag value.
To create a tag variable, you must use a specific format.

```
${<variable>}
```

Type a dollar sign followed by open and close curly brackets. The tag variable goes between the curly brackets. You can use tag variables with other tag variables and with string values.

**Supported Tag Variables**

The following tag variables are supported.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${iam.principal.name}</code></td>
<td>The name of the principal that tagged the resource.</td>
</tr>
<tr>
<td><code>${iam.principal.type}</code></td>
<td>The type of principal that tagged the resource.</td>
</tr>
<tr>
<td><code>${oci.datetime}</code></td>
<td>The date and time that the tag was created.</td>
</tr>
</tbody>
</table>

**Managing Tag Defaults**

This topic describes how to you can specify tags to be automatically applied to resources at creation time.

**Required IAM Policy**

If you're in the Administrators group, then you have the required access for managing tag defaults and tag namespaces. For specific policy information for this feature, see [Required Permissions for Working with Tag Defaults](#) on page 3928.

If you're new to policies, see [Getting Started with Policies](#) on page 2135 and [Common Policies](#) on page 2142. If you want to dig deeper into writing policies for tagging or other IAM components, see [Details for IAM](#) on page 2280.

**Overview of Tag Defaults**

Tag defaults let you specify tags that are applied automatically to all resources at the time of creation in a specific compartment. This feature allows you to ensure that appropriate tags are applied at resource creation without requiring the user creating the resource to have access to the tag namespaces. Consider the following example:

Alice is a finance administrator and has access to the restricted tag namespace Finance. Alice can set up a tag default to apply the Finance.CostCenter tag with a value of W1234 to all resources. Eli can create resources but does not have access to the Finance tag namespace. When Eli creates a resource, the Finance.CostCenter tag is automatically applied with a value of W1234. Eli cannot change this tag, and Alice is confident that it is always applied correctly and not changed by the users who create or edit resources.

Tag defaults allow tenancy administrators to create secure permissions boundaries between users concerned with governance and users who need to create and administer resources.

**Where to Manage Tag Defaults**

Tag defaults are defined for a specific compartment. In the Console, you manage tag defaults on the Compartment Details page.
Required Permissions for Working with Tag Defaults

To create or edit a tag default for a compartment, you must be granted the following combination of permissions:

- manage tag-defaults access on the compartment where you are adding the tag default
- use tag-namespaces access on the compartment where the tag namespace resides
- inspect tag-namespaces access on the tenancy

For the full mapping of permissions to API operations, see Details for IAM on page 2280.

For example, assume you created a set of tag namespaces in CompartmentA. To give a group named TagAdmins access to add tag defaults to CompartmentA, write a policy with the following statements:

```
Allow group TagAdmins to manage tag-defaults in compartment CompartmentA
Allow group TagAdmins to use tag-namespaces in compartment CompartmentA
Allow group TagAdmins to inspect tag-namespaces in tenancy
```

Now assume you also want to allow TagAdmins to create tag defaults in CompartmentA using tag namespaces that reside in CompartmentZ. Add a statement to allow TagAdmins to use tag namespaces in CompartmentZ:

```
Allow group TagAdmins to use tag-namespaces in compartment CompartmentZ
```

Now when TagAdmins create tag defaults in CompartmentC, they can use tag namespaces that reside in either CompartmentA or CompartmentZ.

Working with Tag Defaults

You can only use tag defaults with defined tags. Free-form tags are not supported for tag defaults.

You can define up to 5 tag defaults per compartment.

After a tag default is created in a compartment:

- The default tag is applied to any new resources created in that compartment.
- Previously existing resources in the compartment are not tagged retro-actively.
- If you change the default value of the tag default, existing occurrences are not updated.

Deleting Tag Defaults

- If you delete the tag default from the compartment, existing occurrences of the tag are not removed from resources.
Tagging

- When you delete a tag key definition, existing tag defaults based on that tag key definition are not removed from the compartment. Until you delete the tag default in the compartment, the tag default continues to count against your limit of 5 tag defaults per compartment.

**Required Tag Values**

For tag defaults, you must include a tag value, but you have a choice about how the value is applied.

- Default value
- User-applied value

If you use a default value, then you must create it. This value is applied to all resources.

If you specify that a user-applied value is required, then the user creating the resource must enter the value for the tag at the time of resource creation. Users cannot create resources without entering a value for the tag.

| Tip: |
| You can use predefined values and user-applied values to ensure that users only apply a value that you trust. See Using Predefined Values on page 3924. |

**Tag Inheritance**

The default tag is applied to all resources created in the compartment, including child compartments and the resources created in the child compartments.

Example:

- In CompartmentA, you create a tag default, TagA.
  
  Resources (and compartments) created in CompartmentA are automatically tagged with TagA.
  
  - In the subcompartment, CompartmentB, you create tag default, TagB.
    
    Resources and compartments created in CompartmentB are automatically tagged with TagA and TagB.
    
    - In the sub-subcompartment, CompartmentC, you create tag default TagC.
      
      Resources created in CompartmentC are automatically tagged with TagA, TagB, and TagC.

This example is illustrated in the following graphic:
Overriding Tag Defaults

Tag defaults can be overridden at the time of resource creation by users who have the appropriate permissions to both create the resource and to use the tag namespace.

Example: CompartmentA has a tag default defined to apply CostCenter.Operations="42". Pradeep belongs to a group that grants him permissions to create instances in CompartmentA and also to use tag namespaces in CompartmentA. He creates an instance in CompartmentA, and in the Create Instance dialog, he applies the tag CostCenter.Operations="50". Because he has the appropriate permissions, when the instance is created, the tag default is overridden, and the instance is tagged with CostCenter.Operations="50".

After a resource is created and tagged, users with the appropriate permissions to both update the resource and to use the tag namespace can modify the default tags that were applied at resource creation.

Tag Defaults and Retired Tags

Retired tags can't be applied to new resources. Therefore, if the tag namespace or tag key specified in a tag default is retired, when new resources are created, the retired tag is not applied. As a best practice, you should delete the tag default that specifies the retired tag.

Tag Defaults and Tag Variables

You can use tag variables in tag defaults. Tag variables dynamically resolve at resource creation time. For example, you enter a tag variable for principal name as the tag default in a particular compartment.

Operations.CostCenter="${iam.principal.name}" 

Davis and Garcia each create buckets in that compartment. The buckets that Davis creates include default tags that contain his name as the value, while the buckets that Garcia creates have his name.

Operations.CostCenter="Davis"
Operations.CostCenter="Garcia"

Meanwhile, the tag default still contains the original variables. See Using Tag Variables on page 3926.
Limits on Tag Defaults

A maximum of 5 tag defaults can be defined per compartment.

Note:

When you delete a tag key definition, existing tag defaults based on that tag key definition are not removed from the compartment. Until you delete the tag default in the compartment, the tag default continues to count against your limit of 5 tag defaults per compartment.

See Limits on Tags on page 3908 for more limits on tags.

Using the Console

To create a tag default

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
   
   A list of the compartments that you have access to displays.
2. In the list, click the name of the compartment to which you want to add a tag default.
3. On the compartment details page, click Tag Defaults.
   
   The list of existing tag defaults displays.
4. Click Create Tag Default.
5. Enter the following (all fields are required):
   
   • Tag Namespace: Select the tag namespace for the tag default.
   • Tag Key: Select the tag key.
6. Specify the type of value you want this tag to have:
   
   • Default Value: Enter the value you want this tag to have.
   • User-applied Value: Users that create resources must enter the value as resources are created.
7. Click Create Tag Default.

To update the default value of a tag default

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
   
   A list of the compartments that you have access to displays.
2. In this list, click the name of the compartment that has the tag default that you want to update.
3. On the compartment details page, click Tag Defaults.
   
   The list of existing tag defaults displays.
4. Find the tag default you want to update. Go to the the Actions icon (three dots) and click Edit.
5. Specify the type of value you want this tag to have:
   
   • Default Value: Enter the value you want this tag to have.
   • User-applied Value: Users that create resources must enter the value as resources are created.
6. Click Save Changes.

To delete a tag default

1. Open the navigation menu. Under Governance and Administration, go to Identity and click Compartments.
   
   A list of the compartments that you have access to displays.
2. In the list, click the name of the compartment that has the tag default that you want to delete.
3. On the compartment details page, click Tag Defaults.
   
   The list of existing tag defaults displays.
4. Find the tag default that you want to delete. Go to the the Actions icon (three dots) and click Delete.
5. Confirm when prompted.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use these API operations to manage tag defaults:

- GetTagDefault
- ListTagDefaults
- CreateTagDefault
- UpdateTagDefault
- DeleteTagDefault

Understanding Automatic Tag Defaults

Use tag defaults to manage resources in your tenancy, including tracking costs by principal name and the date resources are created. In tenancies created after December 17, 2019, two tag defaults are automatically added to the root compartment. These tag defaults apply tags to all resources with the following values:

- Name of the principal that created the resource
- Date the resource was created

Overview of Automatic Tag Defaults

The tag defaults Oracle automatically adds come from a tag namespace called Oracle-Tags, which includes two tag key definitions:

- CreatedBy (Cost-tracking tag)
- CreatedOn

Oracle uses these tags to define two tag defaults in the root compartment of your tenancy. When users create resources in your tenancy, each tag is added to the resource automatically. The values for these tags contain the name of the principal that created the resource and the date and time the resource was created. For more information, see Using Tag Variables on page 3926.

Required IAM Policy

Automatic tag defaults are two tag defaults, automatically created in the root compartment. To allow users to work with these tag defaults, use the same IAM policy for working with tag defaults. For more information, see Required Permissions for Working with Defined Tags on page 3915.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142. If you want to dig deeper into writing policies for groups or other IAM components, see Details for IAM on page 2280.

Working with Automatic Tag Defaults

You can use the cost-tracking tag feature to check usage and set budgets or to filter resources by date. You can remove and update tags automatically applied to resources as you would any other tag. For more information, see Using Cost-Tracking Tags on page 3923 and Resource Tags on page 211.

If you no longer want these tags applied to resources automatically, you can remove the tag defaults that Oracle created. Although Oracle created the tag defaults, they are ordinary tag defaults that you can manage as you would any other. For more information, see Managing Tag Defaults on page 3927.

Using Tags to Manage Access

This topic describes how you can use tags in policy to scope access based on tags applied to either the requestor or the target of an authorization call.

About Tag-Based Access Control

Using conditions and a set of tag variables, you can write policy to scope access based on the tags that have been applied to a resource. Access can be controlled based on a tag that exists on the requesting resource (group, dynamic
Tagging

group, or compartment) or on the target of the request (resource or compartment). Tag-based access control provides additional flexibility to your policies by allowing you to define access policies with tags that span compartments, groups, and resources.

**Caution:**

If your organization chooses to create policies that use tags to manage access, then ensure that you have appropriate controls in place to govern who can apply tags. Also, after policies are in place, keep in mind that applying tags to a group, user, or resource has the potential to confer access to resources.

**Before you create a policy** that specifies a tag on either a target or a requestor, ensure that you are aware of:

- all the potential requestors (users, groups, dynamic groups) that carry the tag
- all the resources that carry the tag

**Before you apply a tag to a resource,** ensure that you are aware of any policies in place that include the tag and could impact who has access to the resource.

**Managing Access Using Tags Applied to the Requesting Resource**

You can control access based on the value of a tag applied to:

- a group (of users) requesting access
- a dynamic group (of instances) requesting access
- a compartment that a resource in a dynamic group resides in

By using tags in your policy statements to scope access, you can define access for multiple groups through a single policy statement. You can also confer access and revoke access for groups by applying or removing tags, without changing the original policies.

The basic syntax for each variable is shown in the following table. Note that the syntax is the same for group and dynamic group, but each is presented in a different row. See Supported Operators on page 3936 for more usage examples.

<table>
<thead>
<tr>
<th>Tag Applied to Requestor</th>
<th>Variable Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>request.principal.group.tag.&lt;tagNamespace&gt;.&lt;tagKeyDefinition&gt;=&lt;value&gt;</td>
<td>The tags applied to the groups that the user belongs to are evaluated for a match.</td>
</tr>
</tbody>
</table>

Sample policy for user group:

```
allow any-user to manage instances in compartment HR where request.principal.group.tag.Operations.Project='Prod'
```

Any user who belongs to a group that has been tagged with Operations.Project='Prod' can manage instances in the HR compartment.
Tagging

<table>
<thead>
<tr>
<th>Tag Applied to Requestor</th>
<th>Variable Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic group</td>
<td>request.principal.group.tag.&lt;value&gt;'</td>
<td>The tags applied to the dynamic groups that the instance belongs to are evaluated for a match.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>compartment</td>
<td>request.principal.compartment.tag.&lt;value&gt;'</td>
<td>The tags applied to the compartment that the requesting resource belongs to are evaluated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**

Users reside in the root compartment of your tenancy, so tags must be applied to the root compartment for those policy statements to work.

**Managing Access Using Tags Applied to the Target Resource**

You can control access based on the value of a tag applied to:

- a resource
- a compartment that the target resource resides in

The basic syntax for these variables is shown in the following table. See Supported Operators on page 3936 for more usage examples.
Tagged

<table>
<thead>
<tr>
<th>Tag Applied to Target</th>
<th>Variable Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resource</td>
<td>target.resource.tag.{tagNamespace}.{tagKeyDefinition}='{tagKeyDefinition}='value'</td>
<td>The tag applied to the target resource of the request is evaluated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>There are limitations to the permissions that can be granted in this type of policy. See the following sections in this topic for details.</td>
</tr>
<tr>
<td>compartment</td>
<td>target.resource.compartment.tag.{tagNamespace}.{tagKeyDefinition}='{tagKeyDefinition}='value'</td>
<td>The tag applied to the target compartment of the request is evaluated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See <a href="#">Compartment Hierarchies</a> on page 3938 for details on how access is granted in nested compartments.</td>
</tr>
</tbody>
</table>

### Permissions to List a Resource Must Be Granted Separately

Policies that scope access based on the tag applied to the target resource can't allow the permissions that enable you to return a list of resources. Therefore, permissions to allow listing a resource must be granted through an additional policy statement. This means that if you have defined a policy like:

```
allow group GroupA to manage all-resources in compartment Operations where
target.resource.tag.Operations.Project= 'Prod'
```

GroupA will not be able to list any of the resources that they are otherwise allowed to manage. Members of GroupA would not be able to use the Console to interact with these resources and users would need to know the OCID of the resource they are attempting to manage, which makes using the SDK and CLI cumbersome, also.

To allow GroupA to list those resources, you need to add another policy statement like:

```
allow group GroupA to inspect all-resources in compartment Operations
```

This approach improves the tag-based policy because it allows users to use the Console more easily (by allowing them to see the resource they want to manage), but still limits the permissions to only inspect. The members of GroupA cannot take any action on those resources unless they are tagged appropriately. Keep in mind when using tag-based access control that the added flexibility requires this additional potential expansion of access.

Another approach you can use to avoid this limitation is to tag the compartments that contains the resources you want to grant access to. An example policy looks like this:

```
allow group GroupA to manage all-resources in tenancy where
target.resource.compartment.tag.Operations.Project= 'Prod'
```

This policy allows the members of GroupA to manage all resources in the tenancy that are in compartments that are tagged with the Operations.Project='Prod' tag.

### Policies that Require a Tag on the Target Resource Can't Grant Create Permissions

When you write a policy to scope access based on the value of a tag on the resource, keep in mind that the policy cannot grant create permissions. A request to create an instance would fail because the target resource has not been created yet and therefore does not have the appropriate tag to be evaluated. So a policy like:

```
allow group GroupA to manage all-resources in compartment Operations where
target.resource.tag.Operations.Project= 'Prod'
```

would fail because the target resource has not been created yet and therefore does not have the appropriate tag to be evaluated.
allow group GroupA to manage instances in compartment Operations where
target.resource.tag.Operations.Project='Prod'

allows the members of GroupA to use and delete instances that are tagged with Operations.Project='Prod', but they
cannot create instances.

Supported Operators

Your policy using these tag variables can include these operators and match types:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>String</td>
<td>request.principal.group.tag.MyTagNamespace.MyTag='sample'</td>
<td>Evaluates to true if any of the groups that the requestor belongs to is tagged with the matching value &quot;sample&quot; for MyTagNamespace.MyTag. (The value is case insensitive.)</td>
</tr>
<tr>
<td></td>
<td>Pattern</td>
<td>request.principal.group.tag.MyTagNamespace.MyTag=/*sample/</td>
<td>Evaluates to true if any of the values of MyTagNamespace.MyTag ends with &quot;sample&quot;. (Simple case insensitive pattern match.)</td>
</tr>
<tr>
<td></td>
<td>Policy variable</td>
<td>request.principal.group.tag.mytagnamespace.mytag = target.resource.tag.mytagnamespace.mytag</td>
<td>Evaluates to true when the specified resource mytagnamespace.mytag has a value that matches the specified target mytagnamespace.tag.</td>
</tr>
<tr>
<td>!=</td>
<td>String</td>
<td>request.principal.group.tag.MyTagNamespace.MyTag!='sample'</td>
<td>Evaluates to true if none of the string values of the policy variable equals &quot;sample&quot;. (Simple case insensitive string comparison.)</td>
</tr>
<tr>
<td></td>
<td>Pattern</td>
<td>request.principal.group.tag.MyTagNamespace.MyTag=/!*sample/</td>
<td>Evaluates to true if none of the values of MyTagNamespace.MyTag ends with &quot;sample&quot;. (Simple case insensitive pattern match.)</td>
</tr>
<tr>
<td></td>
<td>Policy variable</td>
<td>request.principal.group.tag.mytagnamespace.mytag != target.resource.tag.mytagnamespace.mytag</td>
<td>Evaluates to true if neither side is a subset of the other.</td>
</tr>
</tbody>
</table>
### In / Not In

<table>
<thead>
<tr>
<th>Operator</th>
<th>Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>String</td>
<td><code>request.principal.group.tag.MyTagNamespace.MyTag in ('sample', 'sample1')</code></td>
<td>The clause evaluates to true if any of the values of <code>MyTagNamespace.MyTag</code> for any group of the current requesting principal either equals to &quot;sample&quot; or &quot;sample1&quot;.</td>
</tr>
<tr>
<td></td>
<td>Pattern</td>
<td><code>request.principal.group.tag.MyTagNamespace.MyTag in (/*sample/, /sample1*/)</code></td>
<td>The clause evaluates to true if any of the values of <code>MyTagNamespace.MyTag</code> for any group of the current requesting principal either ends with &quot;sample&quot; or starts with &quot;sample1&quot;.</td>
</tr>
<tr>
<td></td>
<td>Policy variable</td>
<td><code>request.principal.group.tag.MyTagNamespace.MyTag in (target.resource.tag.mytagnamespace.mytag, 'sample')</code></td>
<td>The clause evaluates to true if any of the following conditions are met: 1. Either <code>request.principal.group.tag.MyTagNamespace.MyTag</code> or <code>target.resource.tag.mytagnamespace.mytag</code> is a subset of the other. 2. Any string values of <code>request.principal.group.tag.MyTagNamespace.MyTag</code> equals &quot;sample&quot;.</td>
</tr>
<tr>
<td>not in</td>
<td>String</td>
<td><code>request.principal.group.tag.MyTagNamespace.MyTag not in ('sample', 'sample1')</code></td>
<td>The clause evaluates to true if none of the values of <code>MyTagNamespace.MyTag</code> for any group of the current requesting principal equals to &quot;sample&quot; or &quot;sample1&quot;.</td>
</tr>
<tr>
<td></td>
<td>Pattern</td>
<td><code>request.principal.group.tag.MyTagNamespace.MyTag not in (/*sample/, /sample1*/)</code></td>
<td>The clause evaluates to true if none of the values of <code>MyTagNamespace.MyTag</code> for any group of the current requesting principal ends with &quot;sample&quot; or starts with &quot;sample1&quot;.</td>
</tr>
<tr>
<td>Operator</td>
<td>Type</td>
<td>Example</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Policy variable</td>
<td>request.principal.group.tag.MyTagNamespace.MyTag not in (target.resource.tag.mytagnamespace.mytag, 'sample')</td>
<td>The clause evaluates to true if all of the following conditions are met: 1. Neither request.principal.group.tag.MyTagNamespace.MyTag nor target.resource.tag.mytagnamespace.mytag is a subset of the other. 2. None of the string values of request.principal.group.tag.MyTagNamespace.MyTag equals &quot;sample&quot;.</td>
</tr>
</tbody>
</table>

**Support for Wildcards**

You can use the * character to match all occurrences of `{tagNamespace}.{tagKeyDefinition}` regardless of the value. In the policy, you can place * in single quotes '*' or between backslashes /*/. For example,

allow group GroupA to use all-resources in compartment HR where target.resource.tag.HR.Project= '*'

In this example, GroupA can use all resources in the compartment HR that are tagged with the tag namespace and tag key: HR.Project with any value.

**Limitations on Characters in Tag Namespaces and Tag Key Definitions Used in Policy Variables**

Tag namespaces and tag key definitions support a broader set of characters than are allowed in policy variables. Therefore, to use tag namespaces and tag key definitions in variables, ensure that they only include the characters also supported by policy variables. Supported characters are:

a-z, A-Z, 0-9, _, @, -, :

If your tag namespaces or tag keys have characters other than these, you cannot use them in policy variables. Tag namespaces and tag keys cannot be renamed, so you will have to create new tag namespaces and tag key definitions.

**Considerations for Case**

When working with tags in policies, be aware that tag values are case insensitive. For example:

request.principal.group.tag.MyTagNamespace.MyTag='sample'

is the same as

request.principal.group.tag.MyTagNamespace.MyTag='Sample'

**Compartment Hierarchies**

When you write a condition to allow access based on the tag applied to a target compartment, remember that this policy also allows access to all compartments nested inside the tagged compartment. All subcompartments in the tagged compartment are resources in the tagged compartment, and therefore the policy grants access.

For example, in this scenario:
Tagging

The policy:

```plaintext
allow group GroupA to use all-resources in tenancy where
    target.resource.compartment.Operations.Project='ProjectA'
```

allows GroupA to use all the resources in CompartmentA, CompartmentA1, and CompartmentA1.1, even though the tag is applied to CompartmentA only.

**Supported Services**

All Oracle Cloud Infrastructure services support the `request.principal.compartment`, `request.principal.group`, and `target.resource.compartment.tag` policy variables.

Not all services support the `target.resource.tag` policy variable. The following table lists the **supported services**. If the service is not listed in the table, it is not supported at this time.

Some services have limitations. See the appropriate link in the table.

<table>
<thead>
<tr>
<th>Services Supported</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Gateway</td>
<td>See <a href="#">API Gateway Service Limitations</a> on page 3940.</td>
</tr>
<tr>
<td>Application Migration</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Big Data</td>
<td>See <a href="#">Big Data Service Limitations</a> on page 3941.</td>
</tr>
<tr>
<td>Blockchain Platform</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Block Volume</td>
<td>See <a href="#">Block Volume Service Limitations</a> on page 3941.</td>
</tr>
<tr>
<td>Compute</td>
<td>See <a href="#">Compute Service Limitations</a> on page 3941.</td>
</tr>
<tr>
<td>Compute Management</td>
<td>See <a href="#">Compute Management Limitations</a> on page 3942.</td>
</tr>
<tr>
<td>Content and Experience</td>
<td>See <a href="#">Content and Experience Limitations</a> on page 3942.</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>See <a href="#">Data Catalog Service Limitations</a> on page 3944.</td>
</tr>
<tr>
<td>Data Flow</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Data Science</td>
<td>See <a href="#">Data Science Service Limitations</a> on page 3944.</td>
</tr>
<tr>
<td>Database</td>
<td>See <a href="#">Database Service Limitations</a> on page 3942.</td>
</tr>
<tr>
<td>Services Supported</td>
<td>More Information</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Digital Assistant</td>
<td>See Digital Assistant Limitations on page 3945.</td>
</tr>
<tr>
<td>DNS</td>
<td>See Public DNS Limitations on page 3947.</td>
</tr>
<tr>
<td>Email Delivery</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>FastConnect</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Functions</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Health Checks</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>IAM</td>
<td>Supported resources are: users, groups, policies, dynamic-groups, network-sources, and identity-providers</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>See Load Balancing Service Limitations on page 3945.</td>
</tr>
<tr>
<td>Networking</td>
<td>See Networking Service Limitations on page 3946.</td>
</tr>
<tr>
<td>NoSQL Database Cloud</td>
<td>See Networking Service Limitations on page 3946.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Object Storage</td>
<td>See Object Storage Service Limitations on page 3947.</td>
</tr>
<tr>
<td>Quotas Service</td>
<td>Fully supported, no limitations.</td>
</tr>
<tr>
<td>Tagging Namespace</td>
<td>See Tagging Namespace Limitations on page 3947.</td>
</tr>
<tr>
<td>Vault</td>
<td>Encryption not supported.</td>
</tr>
<tr>
<td>WAF</td>
<td>See WAF Limitations on page 3947.</td>
</tr>
</tbody>
</table>

**Limitations and Additional Policies Needed for Specific Target.Resource.Tag Scenarios**

For some services, not all permissions or resource types are supported. When a permission is not supported, that means that even if the resource is tagged and the permission is included in the verb granting access, that permission is not allowed and authorization fails for the operation governed by the permission. For example, the Block Volume service resource `volume-backups`, does not support tag-based access control for the `VOLUME_BACKUP_COPY` permission. Therefore, this policy:

```sql
allow group TestGroup to manage volume-backups in compartment Compartment1
where target.resource.tag.TagNS.TagKey = 'test'
```

does not allow members of the group TestGroup to perform the `CopyVolumeBackup` operation. To grant that permission to TestGroup, you would need to add another policy statement to cover it.

In addition, some operational scenarios require authorization to access multiple resources. When scoping access to tags that are applied to the target resource, you must include a separate policy for each resource involved in the operation. Also, because of the limitations for listing resources and other service-specific permissions, additional policies (not scoped by tag) are required.

**API Gateway Service Limitations**

In addition to the expected tag-based access control policy for API Gateway resources, you’ll need policy allowing manage permissions for `api-workrequests`.

Here is an example policy with the additional permissions:

```sql
allow group TestGroup to manage api-workrequests in compartment Compartment1
```
Tagging

**Big Data Service Limitations**

In addition to the expected tag-based access control policy for Big Data resources, you’ll need policy allowing manage permissions for `cluster-work-requests`.

Here is an example policy with the additional permissions:

```
allow group TestGroup to manage cluster-work-requests in compartment Compartment1
```

**Block Volume Service Limitations**

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type with Limitations</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Volume</td>
<td>backup-policy-assignments</td>
<td>BACKUP_POLICY_ASSIGNMENT_DELETE</td>
</tr>
<tr>
<td></td>
<td>volume-backups</td>
<td>VOLUME_BACKUP_COPY</td>
</tr>
</tbody>
</table>

Scenarios requiring additional policy:

**Attach a block volume to a compute instance:**

To attach a block volume to a compute instance, in addition to the tag-based access control policy to allow the `use` verb on volumes and instances, you’ll need some additional permissions.

For example:

```
allow group TestGroup to use volumes in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'
allow group TestGroup to use instances in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'
```

These two policies allow members of TestGroup to use volumes and instances in Compartment1, when the resources have the appropriate tag. To allow members to attach a block volume to an instance, you’ll also need policies that allow the permissions shown in the following statements:

```
allow group TestGroup to read instances in compartment Compartment1
allow group TestGroup to manage volume-attachments in compartment Compartment1 where any {request.permission='VOLUME_ATTACHMENT_CREATE', request.permission='VOLUME_ATTACHMENT_DELETE'}
```

**Compute Service Limitations**

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>instance-console-connection</td>
<td>INSTANCE_CONSOLE_CONNECTION_DELETE</td>
</tr>
<tr>
<td></td>
<td>instances</td>
<td>INSTANCE_POWER_ACTIONS</td>
</tr>
</tbody>
</table>

Scenarios requiring additional policy:

**Attach compute instance to subnet:**
To manage a compute instance’s subnet attachment, in addition to the expected tag-based access control policy for instances and subnets, shown here:

allow group TestGroup to use subnets in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'
allow group TestGroup to manage instances in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'

You’ll need additional permissions on vnics:

allow group TestGroup to use vnics in compartment Compartment1 where ANY{request.permission='VNIC_ATTACH', request.permission='VNIC_CREATE'}

Delete a VNIC from a compute instance:

To delete a VNIC from a compute instance, in addition to the expected tag-based access control policy for instances and subnets shown here:

allow group TestGroup to manage instances in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'
allow group TestGroup to use subnets in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'

You’ll need policy allowing you permissions on vnics:

allow group TestGroup to use vnics in compartment Compartment1 where ANY{request.permission='VNIC_DELETE', request.permission='VNIC_DETACH'}

### Compute Management Limitations

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute Management</td>
<td>instance-pools</td>
<td>All permissions</td>
<td>The instance-pools resource type is not supported.</td>
</tr>
<tr>
<td></td>
<td>auto-scaling-configurations</td>
<td>AUTO_SCALING_CONFIGURATION_UPDATE</td>
<td></td>
</tr>
</tbody>
</table>

### Content and Experience Limitations

In addition to the expected tag-based access control policy for Content and Experience resources, you’ll need policy allowing manage permissions for oce-work-requests.

Here is an example policy with the additional permissions:

allow group TestGroup to manage oce-requests in compartment Compartment1

### Database Service Limitations

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>all</td>
<td>DATABASE_DELETE</td>
<td></td>
</tr>
</tbody>
</table>

Update Tags for ExaData Infrastructure:
Tagging

Not supported at this time using tag-based access control policies.

Scenarios requiring additional policy:

**Delete a DB-System:**

To delete or update a DB-System, in addition to the expected tag-based access control policy for db-systems, shown here:

allow group TestGroup to manage db-systems in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'

You’ll need policy allowing you permissions for db-backups, db-homes, vnics, subnets and databases. Here is an example policy showing the additional permissions:

allow group TestGroup to manage db-backups in compartment Compartment1 where ANY {request.permission='DB_BACKUP_DELETE', request.permission='DB_BACKUP_INSPECT'}
allow group TestGroup to manage db-homes in compartment Compartment1 where request.permission='DB_HOME_DELETE'
allow group TestGroup to manage vnics in compartment Compartment1 where ANY {request.permission='VNIC_DELETE', request.permission='VNIC_DETACH'}
allow group TestGroup to manage subnets in compartment Compartment1 where request.permission='SUBNET_DETACH'
allow group TestGroup to manage databases in compartment compartment1

**Move a DB-system to another compartment:**

To move a DB-System to another compartment, in addition to the expected tag-based access control policy for db-systems shown here:

allow group TestGroup to manage db-systems in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'

You’ll need policy allowing you permissions for databases, db-homes, and db-backups. Here is an example policy with the additional permissions:

allow group TestGroup to use databases in compartment Compartment1 where request.permission='DATABASE_UPDATE'
allow group TestGroup to manage db-backups in compartment Compartment1 where request.permission='DB_BACKUP_INSPECT'
allow group TestGroup to manage db-homes in compartment Compartment1 where request.permission='DB_HOME_UPDATE'

**Database delete for Exadata DB-System:**

To delete a database resource for an Exadata DB-System, you’ll need the expected tag-based access control policy for db-systems and databases shown here:

allow group TestGroup to manage db-systems in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'
allow group TestGroup to manage databases in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'

You’ll also need permissions for db-homes and db-backups. Here is an example policy with the additional permissions:

allow group TestGroup to manage db-homes in compartment Compartment1 where request.permission='DB_HOME_UPDATE'
allow group TestGroup to manage db-backups in compartment Compartment1 where ANY {request.permission='DB_BACKUP_DELETE', request.permission='DB_BACKUP_INSPECT'}

Delete Database:
Deleting a database for a baremetal or virtual machine DB system is not supported using tag-based policies on the target resource.

Database backup create:
To create a database backup, you'll need the expected tag-based access control policy for databases:

```
allow group TestGroup to manage databases in compartment Compartment1 where target.resource.tag.TagNS.TagKey= 'test'
```

You'll also need permissions for db-backups. Here is an example policy with the additional permissions:

```
allow group TestGroup to manage db-backups in compartment Compartment1 where request.permission='DB_BACKUP_CREATE'
```

Database restore:
To restore a database backup, you'll need the expected tag-based access control policy for databases:

```
allow group TestGroup to manage databases in compartment Compartment1 where target.resource.tag.TagNS.TagKey= 'test'
```

You'll also need permissions for backups, like the one shown here:

```
allow group TestGroup to manage db-backups in compartment Compartment1 where ANY {request.permission='DB_BACKUP_INSPECT', request.permission='DB_BACKUP_CONTENT_READ'}
```

Create Data Guard association:
Creating a Data Guard association is not supported using tag-based policies on the target resource.

Data Catalog Service Limitations
In addition to the expected tag-based access control policy for Data Catalog resources, you'll need the following additional policies for data-catalog-family:

```
allow group resource_managers to read data-catalog-family in tenancy where request.operation = 'GetWorkRequest'
allow group resource_managers to read data-catalog-family in tenancy where request.operation = 'ListWorkRequestErrors'
allow group resource_managers to read data-catalog-family in tenancy where request.operation = 'listworkrequestlogs'
```

Data Science Service Limitations
In addition to the expected tag-based access control policy for Data Science resources, you’ll need policy allowing manage permissions for data-science-work-requests.

Here is an example policy with the additional permissions:

```
allow group TestGroup to manage data-science-work-requests in compartment Compartment1
```
### Digital Assistant Limitations

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Assistant</td>
<td>oda-design</td>
<td>All permissions</td>
</tr>
<tr>
<td></td>
<td>oda-insights</td>
<td>All permissions</td>
</tr>
</tbody>
</table>

In addition to the expected tag-based access control policy for the Oracle Digital Assistant resources, you'll need the following additional policies for `oda-instances`:

```plaintext
allow group TestGroup to inspect oda-instances in compartment Compartment1
allow group TestGroup to read oda-instances in compartment Compartment1
   request.operation = 'GetWorkRequest'
allow group TestGroup to read oda-instances in compartment Compartment1
   request.operation = 'ListWorkRequestErrors'
allow group TestGroup to read oda-instances in compartment Compartment1
   request.operation = 'listworkrequestlogs'
```

### Load Balancing Service Limitations

Scenarios requiring additional policy:

#### Update Load Balancer:

To perform any update to load balancers, in addition to the expected tag-based access control policy for `load-balancers`:

```plaintext
allow group TestGroup to manage load-balancers in compartment Compartment1
   where target.resource.tag.TagNS.TagKey= 'test'
```

You’ll need policy that allows the GetWorkRequest API operation. Here is an example policy with the additional permission:

```plaintext
allow group TestGroup to read load-balancers in compartment Compartment1
   where request.operation = 'GetWorkRequest'
   network-security-group
```

#### Delete Load Balancer:

To delete a load balancer, in addition to the expected tag-based access control policy for `load-balancers`, `subnets`, and `network-security-group`:

```plaintext
allow group TestGroup to manage load-balancers in compartment Compartment1
   where target.resource.tag.TagNS.TagKey= 'test'
allow group TestGroup to use subnets in compartment Compartment1 where
   target.resource.tag.TagNS.TagKey= 'test'
allow group TestGroup to use network-security-group in compartment
   Compartment1 where target.resource.tag.TagNS.TagKey= 'test'
```

You’ll need these additional permissions for `vnics`:

```plaintext
allow group TestGroup to use vnics in compartment Compartment1 where ANY
   {request.permission = 'VNIC_DETACH', request.permission = 'VNIC_DELETE',
    request.permission='VNIC_DISASSOCIATE_NETWORK_SECURITY_GROUP'}
```
Networking Service Limitations

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>private-ips</td>
<td>PRIVATE_IP_UPDATE, PRIVATE_IP_DELETE, VNIC_UNASSIGN, SUBNET_DETACH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>route-tables</td>
<td>UPDATE (INTERNET_GATEWAY_DETACH)</td>
<td>Removing a route rule is not supported.</td>
</tr>
<tr>
<td></td>
<td>vnics</td>
<td>VNIC_UPDATE, VNIC_DELETE</td>
<td></td>
</tr>
</tbody>
</table>

Attach service gateway or NAT gateway to a route table:

Attaching a service gateway or a NAT gateway to a route table is not supported using tag-based policies on the target resource.

Scenarios requiring additional policy:

**Attach DRG to VCN:**

To attach DRG to VCN, in addition to the following expected tag-based access control policy for `virtual-network-family` and `vcns`:

```plaintext
allow group TestGroup to use virtual-network-family in compartment Compartment1 where target.resource.tag.TagNS.TagKey = 'test'
```

You’ll need policy allowing you manage permissions for `drgs`. Here is an example policy with the additional permissions:

```plaintext
allow group TestGroup to manage drgs in compartment Compartment1
```

NoSQL Database Cloud Service Limitations

Supported resources are: `nosql-tables`, `nosql-rows`, and `nosql-indexes`.

In addition to the expected tag-based access control policy for the NoSQL Database Cloud resources, you’ll need these additional policies:

```plaintext
allow group TestGroup to read nosql-tables in compartment Compartment1 where request.operation='ListWorkRequests'
allow group TestGroup to read nosql-tables in compartment Compartment1 where request.operation='ListWorkRequestErrors'
allow group TestGroup to read nosql-tables in compartment Compartment1 where request.operation='ListWorkRequestLogs'
```

Note that the preceding policies are required to navigate the NoSQL Database Cloud resources in the Console.
### Tagging

#### Object Storage Service Limitations

<table>
<thead>
<tr>
<th>Service</th>
<th>Resource Type</th>
<th>Permissions Not Supported with the target.resource.tag Policy Variable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Storage</td>
<td>objects</td>
<td>All permissions related to accessing objects</td>
<td>Objects are not taggable.</td>
</tr>
</tbody>
</table>

#### Public DNS Limitations

In addition to the expected tag-based access control policy for dns resources, you’ll need policy allowing you manage permissions for dns-records. Here is an example policy with the additional permissions:

```
allow group TestGroup to manage dns-records in compartment Compartment1
```

#### Tagging Namespace Limitations

Policy that grants a user access to a tag namespace based on a tag on the namespace does not allow the user to create or delete tag key definitions in that tag namespace.

For example, the policy:

```
allow group TestGroup to manage tag-namespaces in compartment Compartment1 where target.resource.tag.TagNS.TagKey='test'
```

does not allow the users in TestGroup to create or delete tag key definitions in the tag namespaces tagged with TagNS.TagKey='test'.

#### WAF Limitations

In addition to the expected tag-based access control policy for the WAF resources, you’ll need policy allowing you manage permissions for waas-work-request. Here is an example policy with the additional permissions:

```
allow group TestGroup to manage waas-work-request in compartment Compartment1
```

#### Illustrated Examples

- Illustrated Examples on page 3947
- Example Using Tags Applied to a Target Resource on page 3949

#### Example Using Tags Applied to a Group

Following is an example that demonstrates how you can use tags applied to user groups to manage access to resources in a compartment.

Assume you have three compartments: ProjectA, ProjectB, and ProjectC

For each compartment, there is an admin group set up: A-Admins, B-Admins, and C-Admins.
Each admin group has full access over their compartment through the following policies:

- allow group A-Admins to manage all-resources in compartment ProjectA
- allow group B-Admins to manage all-resources in compartment ProjectB
- allow group C-Admins to manage all-resources in compartment ProjectC

Your organization has set up the following tag namespace and key to tag each group by its role:

- EmployeeGroup.Role

Some values for this tag are 'Admin', 'Developer', 'Test-Engineer'.

All your admin groups are tagged with EmployeeGroup.Role='Admin'

Now you want to set up a Test compartment for members of the three projects to share. You want to give Admin access to all three of your existing admin groups. To accomplish this, you can write a policy like:

allow any-group to manage all-resources in compartment Test where request.principal.group.tag.EmployeeGroup.Role='Admin'
Tagging

With this policy, all of your existing admin groups with the tag will have access to the Test compartment. Also, any new or existing groups that you tag with EmployeeGroup.Role='Admin' in the future will have access to the Test compartment without having to update the policy statements.

**Example Using Tags Applied to a Target Resource**

In this example, each of your organization's project compartments contains two child compartments: Test and Prod. You want to give your test engineers access to the test compartments across all three projects. To accomplish this, you create a tag:

`ResourceGroup.Role='Test'`

and apply this to the Test compartments in each of your project compartments.

You can then use a policy like:
allow group Testers to use all-resources in tenancy where
target.resource.compartment.tag.ResourceGroup.Role='Test'
to allow your group Testers to access the resources across all three test compartments.

Frequently Asked Questions About Tagging

This topic provides answers to frequently asked questions (FAQ) about Tagging.

What is the difference between free-form tags and defined tags?
Free-form tags are simple (string) key and (string) value pairs that can be set on a resource. Free-form tags cannot be used for applying policies or for authentication, and these tags are not included in metering data. Any user can create and apply free-form tags.

Tag administrators create defined tags for the tenancy, and users can apply these tags to resources. Most of the Tagging features require defined tags. For example, tag rules and policies only reference defined tags. For more information, see How Tagging Works.

How do I decide which kind of tag to use?
Most of the Tagging features require defined tags. Because free-form tags are limited in functionality, Oracle recommends that you only use them to try out the tagging feature in your system when you are first getting started with tagging. For more information, see Tagging Overview.

Are there any tools to help users migrate from free-form tags to defined tags?
Not currently.

Who creates defined tags?
Tag administrators create and manage defined tags, and users apply these tags to resources. Use IAM policy to select tag administrators who can create tags. Grant all other users in the tenancy only the ability to apply tags. For more information, see Working with Defined Tags.

What is the difference between a tag namespace, tag key, and key definition?
See Tagging Concepts.

Can I use Tagging with resources that do not have an OCID?
No. Tagging is only supported with resources that have OCIDs.

What are the allowed characters for tag namespaces and keys?
The allowed characters are printable ASCII, except U+0020 space (" "), and U+002E full stop ("."). Namespace and key names cannot be empty.
Avoid entering confidential information.

Can I use an OCID to name my tag namespace?
No. OCIDs do not follow the required format for tag namespaces.

Do I need to provide a value for compartmentId when making API requests?
No. Because namespaces are unique under tenants, you do not need to provide the compartmentId value. All API requests automatically come with tenancy information.
Can I change the name of my tag namespace?
No. You can retire your tag namespace, but you cannot change its name.

Can I change the name of my tag key definition?
No. You can retire your tag key definition, but you cannot change its name.

What is the base URL of the Tagging service?
Tagging is part of the Identity service. The Tagging service has two parts:

• Handling the creation and management of new tag namespaces and tag key definitions. For these operations, use the Identity Service base URL.
• Applying tags to specific resources by including the tag namespace, key, and value information in requests sent to each supporting service.

When I try to delete a tag key definition, why do I get the error "Can't enable definition <tag definition> in retired namespace <namespace name>"?
You cannot delete a tag key definition in a retired namespace. Reactivate the tag namespace and then retire the tag. For more information, see Managing Tags and Tag Namespaces.
Chapter 39

Vault

This chapter explains how to create vaults, encryption keys, and secrets, and how to manage and use them.

Overview of Vault

Oracle Cloud Infrastructure Vault is a managed service that lets you centrally manage the encryption keys that protect your data and the secret credentials that you use to securely access resources. Vaults securely store master encryption keys and secrets that you might otherwise store in configuration files or in code. Specifically, depending on the protection mode, keys are either stored on the server or they are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification.

The key encryption algorithms that the Vault service supports includes the Advanced Encryption Standard (AES), the Rivest-Shamir-Adleman (RSA) algorithm, and the elliptic curve digital signature algorithm (ECDSA). You can create and use AES symmetric keys and RSA asymmetric keys for encryption and decryption. You can also use RSA or ECDSA asymmetric keys for signing digital messages.

You can use the Vault service to create and manage the following resources:

- Vaults
- Keys
- Secrets

You can use the Vault service to exercise the following lifecycle management features for vaults, master encryption keys, and secrets, helping you to control these resources and access to them:

- Create vaults
- Create or import cryptographic material as master encryption keys
- Create secrets to store secret credentials
- Enable or disable master encryption keys for use in cryptographic operations
- Rotate keys to generate new cryptographic material
- Export key or vault metadata to a backup that you can restore and use again later
- Update secrets with new secret contents
- Specify which secret version is currently in use through promotion
- Configure rules to govern the management and use of secrets
- Tag vaults, master encryption keys, or secrets to add metadata to resources
- Delete vaults, keys, or secrets when they're no longer needed

Regarding the use of master encryption keys, you can do the following:

- Use keys for encryption and decryption of data while at rest or in transit
- Use keys to sign messages and verify signed messages
Assign keys to supported Oracle Cloud Infrastructure resources, including, but not limited to, buckets and file systems

Generate data encryption keys

The following services integrate with the Vault service to support the use of customer-managed keys to encrypt data in their respective, specified resources:

- Oracle Cloud Infrastructure Block Volume: block and boot volumes
- Oracle Cloud Infrastructure Container Engine for Kubernetes: Kubernetes secrets at rest in the etcd key-value store (when creating new clusters only)
- Oracle Cloud Infrastructure Database: Autonomous Container Databases on dedicated Autonomous Exadata Infrastructure and Exadata Databases (without Oracle Data Guard enabled)
- Oracle Cloud Infrastructure File Storage: file systems
- Oracle Cloud Infrastructure Object Storage: buckets
- Oracle Cloud Infrastructure Streaming: stream pools

In addition, integration with Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who and what services can access which keys and secrets and what they can do with those resources. Oracle Cloud Infrastructure Audit integration gives you a way to monitor key and secret usage. Audit tracks administrative actions on vaults, keys, and secrets.

Key and Secret Management Concepts

The following concepts are key to understanding the Vault service.

VAULTS

Vaults are logical entities where the Vault service creates and durably stores keys and secrets. The type of vault you have determines features and functionality such as degrees of storage isolation, access to management and encryption, scalability, and the ability to back up. The type of vault you have also affects pricing. You cannot change a vault's type after you create the vault.

The Vault service offers different vault types to accommodate your organization's needs and budget. All vault types ensure the security and integrity of the encryption keys and secrets that vaults store. A virtual private vault is an isolated partition on a hardware security module (HSM). Vaults otherwise share partitions on the HSM with other vaults.

Virtual private vaults include 1000 key versions by default. If you don't require the greater degree of isolation or the ability to back up the vault, you don't need a virtual private vault. Without a virtual private vault, you can manage costs by paying for key versions individually, as you need them. (Key versions count toward your key limit and costs. A key always contains at least one active key version. Similarly, a secret always has at least one secret version. However, limits on secrets apply to the tenancy, rather than a vault.)

The Vault service designates vaults as an Oracle Cloud Infrastructure resource.

KEYS

Keys are logical entities that represent one or more key versions, each of which contains cryptographic material. A key's cryptographic material is generated for a specific algorithm that lets you use the key for encryption or in digital signing. When used for encryption, a key or key pair encrypts and decrypts data, protecting the data where the data is stored or while the data is in transit. With an AES symmetric key, the same key encrypts and decrypts data. With an RSA asymmetric key, the public key encrypts data and the private key decrypts data.

You can use AES keys in encryption and decryption, but not in digital signing. RSA keys, however, can be used not only to encrypt and decrypt data, but also to digitally sign data and verify the authenticity of signed data. You can use ECDSA keys in digital signing, but not to encrypt or decrypt data.

When processed as part of an encryption algorithm, a key specifies how to transform plaintext into ciphertext during encryption and how to transform ciphertext into plaintext during decryption. When processed as part of a signing algorithm, together, the private key of an asymmetric key and a message produce a digital signature that accompanies the message in transit. When processed as part of a signature verifying algorithm
by the recipient of the signed message, the message, signature, and the public key of the same asymmetric key confirm or deny the authenticity and integrity of the message.

Conceptually, the Vault service recognizes three types of encryption keys: master encryption keys, wrapping keys, and data encryption keys.

The encryption algorithms that the Vault service supports for master encryption keys include AES, RSA, and ECDSA. You can create AES, RSA, or ECDSA master encryption keys by using the Console, CLI, or API. When you create a master encryption key, the Vault service can either generate the key material internally or you can import the key material from an external source. (Support for importing key material depends on the encryption algorithm of the key material.) When you create master encryption keys, you create them in a vault, but where a key is stored and processed depends on its protection mode.

Master encryption keys can have one of two protection modes: HSM or software. A master encryption key protected by an HSM is stored on an HSM and cannot be exported from the HSM. All cryptographic operations involving the key also happen on the HSM. Meanwhile, a master encryption key protected by software is stored on a server and, therefore, can be exported from the server to perform cryptographic operations on the client instead of on the server. While at rest, the software-protected key is encrypted by a root key on the HSM. For a software-protected key, any processing related to the key happens on the server. A key’s protection mode affects pricing and cannot be changed after you create the key.

After you create your first symmetric master encryption key, you can then use the API to generate data encryption keys that the Vault service returns to you. Some services can also use a symmetric master encryption key to generate their own data encryption keys.

A type of encryption key that comes included with each vault by default is a wrapping key. A wrapping key is a 4096-bit asymmetric encryption key based on the RSA algorithm. The public and private key pair do not count against your service limits. They also do not incur service costs. You use the public key as the key encryption key when you need to wrap key material for import into the Vault service. You cannot create, delete, or rotate wrapping keys.

The Vault service recognizes master encryption keys as an Oracle Cloud Infrastructure resource.

KEY VERSIONS

Each master encryption key is automatically assigned a key version. When you rotate a key, the Vault service generates a new key version. The Vault service can generate the key material for the new key version or you can import your own key material.

Periodically rotating keys limits the amount of data encrypted or signed by one key version. If a key is ever compromised, key rotation thus reduces the risk. A key’s unique, Oracle-assigned identifier, called an Oracle Cloud ID (OCID), remains the same across rotations, but the key version lets the Vault service seamlessly rotate keys to meet any compliance requirements you might have.

Although you can’t use an older key version for encryption after you rotate a key, the key version remains available to decrypt any data that it previously encrypted. If you rotate an asymmetric key, the public key can no longer be used to encrypt data, but the private key remains available to decrypt data previously encrypted by the public key. When you rotate an asymmetric key used in digital signing, you can no longer use the private key version to sign data, but the public key version remains available to verify the digital signature of data previously signed by the older private key version.

For symmetric keys, you do not need to track which key version was used to encrypt what data because the key’s ciphertext contains the information that the service needs for decryption purposes. Through rotations of asymmetric keys, however, you must track which key version was used to encrypt or sign what data. With asymmetric keys, the key’s ciphertext does not contain the information that the service requires for decryption or verification.

With AES symmetric keys, each key version counts as one key version when calculating service limits usage. However, with RSA and ECDSA asymmetric keys, each key version counts as two when calculating usage against service limits because an asymmetric key has both a public key and private key. (Asymmetric keys are also known as key pairs.)

HARDWARE SECURITY MODULES

When you create an AES symmetric master encryption key with the protection mode set to HSM, the Vault service stores the key version within a hardware security module (HSM) to provide a layer of
physical security. (When you create a secret, secret versions are base64-encoded and encrypted by a master encryption key, but are not stored within the HSM.) Any given key version or secret version, after it’s created, is replicated within the service infrastructure as a measure of protection against hardware failures. Key versions of HSM-protected keys are not otherwise stored anywhere else and cannot be exported from an HSM.

When you create an RSA or ECDSA asymmetric master encryption key with the protection mode set to HSM, the Vault service stores the private key within an HSM and does not allow its export from the HSM. However, you can download the public key.

The Vault service uses HSMs that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. This certification means that the HSM hardware is tamper-evident, has physical safeguards for tamper-resistance, requires identity-based authentication, and deletes keys from the device when it detects tampering.

ENVELOPE ENCRYPTION

The data encryption key used to encrypt your data is, itself, encrypted with a master encryption key. This concept is known as envelope encryption. Oracle Cloud Infrastructure services do not have access to the plaintext data without interacting with the Vault service and without access to the master encryption key that is protected by Oracle Cloud Infrastructure Identity and Access Management (IAM). For decryption purposes, integrated services like Object Storage, Block Volume, and File Storage store only the encrypted form of the data encryption key.

SECRETS

Secrets are credentials such as passwords, certificates, SSH keys, or authentication tokens that you use with Oracle Cloud Infrastructure services. Storing secrets in a vault provides greater security than you might achieve storing them elsewhere, such as in code or configuration files. You can retrieve secrets from the Vault service when you need them to access resources or other services.

You can create secrets by using the Console, CLI, or API. Secret contents for a secret are imported to the service from an external source. The Vault service stores secrets in vaults.

The Vault service supports secrets as an Oracle Cloud Infrastructure resource.

SECRET VERSIONS

Each secret is automatically assigned a secret version. When you rotate secret, you provide new secret contents to the Vault service to generate a new secret version. Periodically rotating secret contents reduces the impact in case a secret is exposed. A secret’s unique, Oracle-assigned identifier, called an Oracle Cloud ID (OCID), remains the same across rotations, but the secret version lets the Vault service rotate secret contents to meet any rules or compliance requirements you might have. Although you can’t use an older secret version’s contents after you rotate it if you have a rule configured preventing secret reuse, the secret version remains available and is marked with a rotation state other than "current". For more information about secret versions and their rotation states, see Secret Versions and Rotation States on page 4018.

SECRET BUNDLES

A secret bundle consists of the secret contents, properties of the secret and secret version (such as version number or rotation state), and user-provided contextual metadata for the secret. When you rotate a secret, you create a new secret version, which also includes a new secret bundle version.

Regions and Availability Domains

The Vault service is available in all Oracle Cloud Infrastructure commercial regions. See About Regions and Availability Domains on page 180 for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

Unlike some Oracle Cloud Infrastructure services, however, the Vault service does not have one regional endpoint for all API operations. The service has one regional endpoint for the provisioning service that handles create, update, and list operations for vaults. For create, update, and list operations for keys, service endpoints are distributed across multiple independent clusters. Service endpoints for secrets are distributed further still across different independent clusters.
Because the Vault service has public endpoints, you can directly use data encryption keys generated by the service for cryptographic operations in your applications. However, if you want to use master encryption keys with a service that has integrated with Vault, you can do so only when the service and the vault that holds the key both exist within the same region. Different endpoints exist for key management operations, key cryptographic operations, secret management operations, and secret retrieval operations. For more information, see Oracle Cloud Infrastructure API Documentation.

The Vault service maintains copies of encryption keys and secrets across all availability domains within a region. This replication makes it possible for the Vault service to produce keys or secrets upon request, even when an availability domain is unavailable.

Private Access to Vault

The Vault service supports private access from Oracle Cloud Infrastructure resources in a virtual cloud network (VCN) through a service gateway. Setting up and using a service gateway on a VCN lets resources (such as the instances that your encrypted volumes are attached to) access public Oracle Cloud Infrastructure services such as the Vault service without exposing them to the public internet. No internet gateway is required and resources can be in a private subnet and use only private IP addresses. For more information, see Access to Oracle Services: Service Gateway on page 3256.

Resource Identifiers

The Vault service supports vaults, keys, and secrets as Oracle Cloud Infrastructure resources. Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

Ways to Access Oracle Cloud Infrastructure

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface) or the REST API. Instructions for the Console and API are included in topics throughout this guide. For a list of available SDKs, see Software Development Kits and Command Line Interface on page 4225.

To access the Console, you must use a supported browser. You can use the Console link at the top of this page to go to the sign-in page. You will be prompted to enter your cloud tenant, your user name, and your password.

For general information about using the API, see REST APIs on page 4368.

Authentication and Authorization

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Limits on Vault Resources

See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

For instructions to view your usage level against the tenancy's resource limits, see Viewing Your Service Limits, Quotas, and Usage on page 216. You can also get each individual vault's usage against key limits by viewing key and key version counts in the vault details.
Managing Vaults

This topic describes how to create and manage vaults. For information specifically about backing up and restoring vaults, see Backing Up Vaults and Keys on page 4003. For information about what you can do with keys, see Managing Keys on page 3962. For information about what you can do with secrets, see Managing Secrets on page 4007.

The Vault service lets you create vaults in your tenancy as containers for encryption keys and secrets. If needed, a virtual private vault provides you with a dedicated partition in a hardware security module (HSM), offering a level of storage isolation for encryption keys that’s effectively equivalent to a virtual independent HSM.

Vault management tasks include the following:

• Creating a vault
• Viewing vault configuration details
• Updating the vault name
• Managing vault tags
• Deleting a vault
• Moving a vault to a new compartment

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see Let security admins manage vaults, keys, and secrets on page 2151. For more information about permissions or if you need to write more restrictive policies, see Details for the Vault Service on page 2347.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Moving Resources to a Different Compartment

You can move vaults from one compartment to another. After you move a vault to a new compartment, inherent policies apply immediately and affect access to the vault. Moving a vault doesn't affect access to any keys or secrets that the vault contains. You can move a key or secret from one compartment to another independently of moving the vault it's associated with. For more information, see Managing Compartments on page 2431.

Using the Console

To view vault configuration details

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault you want to view.
3. From the list of vaults in the compartment, click the name of the vault.
4. The console displays the following information:

- **Compartment**: The unique, Oracle-assigned ID of the compartment that contains the vault.
- **OCID**: The unique, Oracle-assigned ID of the vault.
- **Created**: The date and time when you initially created the vault.
- **HSM Key Version Usage**: The number of all key versions across all HSM-protected master encryption keys that the vault contains. A master encryption key comprises one or more key versions, up to the limit allowed by service limits.
- **Software Key Version Usage**: The number of all key versions across all software-protected master encryption keys that the vault contains. This can include one or more key versions for each master encryption key, up to the limit allowed by service limits.
- **Virtual Private**: Whether or not the vault is a virtual private vault.
- **Management Endpoint**: The service endpoint for CreateKey, CreateKeyVersion, EnableKey, DisableKey, UpdateKey, ListKeys, ListKeyVersions, GetKey, GetKeyVersion, ImportKey and ImportKeyVersion operations.
- **Cryptographic Endpoint**: The service endpoint for Encrypt, Decrypt, and GenerateDataEncryptionKey operations.
- **Wrapping Key**: The public RSA wrapping key for the vault.

To create a new vault

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment where you want to create the vault.
3. Click **Create Vault**.
4. In the **Create Vault** dialog box, click **Name**, and then enter a display name for the vault. Avoid entering confidential information.
5. Optionally, make the vault a virtual private vault by selecting the **Make it a virtual private vault** check box. For more information about vault types, see [Key and Secret Management Concepts](#) on page 3953.

   **Note:**
   You cannot change the vault type after the vault is created.

6. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see [Resource Tags](#) on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
7. When you are finished, click **Create**.

To change a vault name

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault you want to rename.
3. From the list of vaults in the compartment, click the name of the vault.
4. On the **Vault Details** page, click **Edit Name**.
5. In the **Edit Vault Name** dialog box, click **Name**, and then enter a new display name for the vault. Avoid entering confidential information.
6. When you are finished, click **Save**.

To manage a vault’s tags

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault for which you want to manage tags.
3. From the list of vaults in the compartment, click the name of the vault.
4. On the **Vault Details** page, click the **Tags** tab to view or editing existing tags. Or, click **Add Tag(s)** to add new ones.

**To delete a vault**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you delete a vault, the vault and all its associated keys go into a pending deletion state until the waiting period expires. By default, this is 30 days, but can be set from a minimum of 7 days up to a maximum of 30 days. When a vault is deleted, all its associated keys are also deleted.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault you want to delete.
3. From the list of vaults in the compartment, click the name of the vault.
4. On the **Vault Details** page, click **Delete**.
5. To confirm that you want to delete the vault, type the name of the vault, and then choose the date and time you want the vault to be deleted.
6. When you are finished, click **Delete Vault**.

**To cancel the deletion of a vault**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that’s in a pending deletion state.
3. From the list of vaults in the compartment, click the name of the vault.
4. On the **Vault Details** page, click **Cancel Deletion**.
5. To confirm that you want to cancel deletion of the vault, click **Cancel Deletion**.

**To move a vault to a different compartment**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **Table Scope**, in the **Compartment** list, choose the compartment that contains the vault that you want to move.
3. Find the vault in the list, click the the Actions icon (three dots), and then click **Move Resource**.
4. Choose the destination compartment from the list.
5. Click **Move Resource**.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see [Command Line Interface (CLI)](https://docs.oracle.com/en_us/oci/1.1.4.0.0/compute/plug_oci/index.html). For a complete list of flags and options available for CLI commands, see the [Command Line Reference](https://docs.oracle.com/en_us/oci/1.1.4.0.0/compute/plug_oci/index.html).

**To view vault configuration details**

Open a command prompt and run `oci kms management vault get` to view the configuration details for a vault:

```sh
oci kms management vault get --vault-id <target_vault_id>
```

For example:

```sh
oci kms management vault get --vault-id ocid1.vault.region1.sea.exampleaaacu2.examplesrcvbtqe5wgrxn2jua3olmeausn5fauxseubwu5my5tf3w3j33edq
```

**To create a new vault**

Open a command prompt and run `oci kms management vault create` to create a new vault:
Note:
You cannot change the vault type after the vault is created.

oci kms management vault create --compartment-id <target_compartment_id> --display-name <vault_name> --vault-type <vault_type>

For example:

oci kms management vault create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgqmgzm2zzum45ibploogtabk3zz --display-name vault-1 --vault-type VIRTUAL_PRIVATE

Avoid entering confidential information.

**To create a new vault with resource tags**

Open a command prompt and run `oci kms management vault create` with one or both of the `--defined-tags` and `--freeform-tags` options to create a new vault with resource tags:

Note:
You cannot change the vault type after the vault is created.

oci kms management vault create --compartment-id <target_compartment_id> --display-name <vault_name> --vault-type <vault_type> --defined-tags <JSON_formatted_defined_tag> --freeform-tags <JSON_formatted_freeform_tag>

For example, on a MacOS or Linux machine:

oci kms management vault create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgqmgzm2zzum45ibploogtabk3zz --display-name vault-1 --vault-type VIRTUAL_PRIVATE --defined-tags '{"Operations": {"CostCenter": "42"}}' --freeform-tags '{"Department": "Finance"}"

Or, for example, on a Windows machine:

oci kms management vault create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgqmgzm2zzum45ibploogtabk3zz --display-name vault-1 --vault-type VIRTUAL_PRIVATE --defined-tags '{"Operations": {"CostCenter": "42"}}' --freeform-tags '{"Department": "Finance"}"

Avoid entering confidential information.

**To change a vault name**

Open a command prompt and run `oci kms management vault update` to change a vault's name:

oci kms management vault update --vault-id <target_vault_id>

For example:

oci kms management vault update --vault-id ocid1.vault.region1.sea.exampleaaacu2.exampleexravte5wgrxn2jua3olmeausn5fauxsuebuwu5my5 --display-name new-vault-name
Avoid entering confidential information.

**To delete a vault**

Open a command prompt and run `oci kms management vault schedule-deletion` to delete a vault:

```
oci kms management vault schedule-deletion --vault-id <target_vault_id>
```

For example:

```
oci kms management vault schedule-deletion --vault-id ocid1.vault.region1.sea.exampleaaacu2.examplesrcvbtqe5wgrxn2jua3olmeausn5fauxseubwu5my5tf3w3
```

When you delete a vault, the vault and all its associated keys go into a pending deletion state until the waiting period expires. By default, this is 30 days, but can be set from a minimum of 7 days up to a maximum of 30 days. When a vault is deleted, all its associated keys are also deleted.

**To cancel the deletion of a vault**

Open a command prompt and run `oci kms management vault cancel-deletion` to cancel the pending deletion of a vault:

```
oci kms management vault cancel-deletion --vault-id <target_vault_id>
```

For example:

```
oci kms management vault cancel-deletion --vault-id ocid1.vault.region1.sea.exampleaaacu2.examplesrcvbtqe5wgrxn2jua3olmeausn5fauxseubwu5my5tf3w3
```

**To move a vault to a different compartment**

Open a command prompt and run `oci kms management vault change-compartment` to move a vault from one compartment to another within the same tenancy:

```
oci kms management vault change-compartment --vault-id <target_vault_id> --compartment-id <new_compartment_id>
```

For example:

```
oci kms management vault change-compartment --vault-id ocid1.vault.region1.sea.exampleaaacu2.examplesrcvbtqe5wgrxn2jua3olmeausn5fauxseubwu5my5tf3w3 --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqmgczzum45ibploogtqabw3zz
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage vaults:

- CancelVaultDeletion
- CreateVault
- GetVault
- ListVaults
- ScheduleVaultDeletion
- UpdateVault
Managing Keys

This topic describes what you can do with keys and key versions to manage their creation and usage. For information specifically about creating keys with your own key material, see Importing Keys and Key Versions on page 3986. For information about assigning keys to protect supported resources, see Assigning Keys on page 3971. For information about how you can use keys in cryptographic operations, see Using Keys on page 3971. For information about backing up and restoring keys, see Backing Up Vaults and Keys on page 4003. For information about what you can do with vaults where you store keys, see Managing Vaults on page 3957. For information about keys more generally, see Key and Secret Management Concepts on page 3953.

In the context of this topic, management of keys includes the ability to do the following:

- Create keys
- View key details
- View a list of keys
- View a list of key versions for a specific key
- Update a key name
- Manage a key's tags
- Enable keys for use in cryptographic operations
- Rotate keys to generate new cryptographic material
- Disable keys to prevent their usage in cryptographic operations
- Delete keys to permanently prevent their usage in cryptographic operations or assignment to resources
- Move a key to a new compartment

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see Let security admins manage vaults, keys, and secrets on page 2151. For more information about permissions or if you need to write more restrictive policies, see Details for the Vault Service on page 2347.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring the traffic associated with your master encryption keys, see Vault Metrics on page 4020.

Moving Resources to a Different Compartment

You can move keys from one compartment to another. After you move a key to a new compartment, inherent policies apply immediately and affect access to the key and key versions. Moving a key doesn't affect access to the vault that
a key is associated with. Similarly, you can move a vault from one compartment to another independently of moving any of its keys. For more information, see Managing Compartments on page 2431.

**Using the Console**

**To create a new master encryption key**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment where you want to create the key.
3. From the list of vaults in the compartment, do one of the following:
   - Click the name of the vault where you want to create the key.
   - Create a new vault for the key by following the instructions in **To create a new vault**, and then click the name of the vault.
4. Click **Master Encryption Keys**, and then click **Create Key**.
5. In the **Create Key** dialog box, choose a compartment from the **Create in Compartment** list. (Keys can exist outside the compartment the vault is in.)
6. Click **Protection Mode**, and then do one of the following:
   - To create a master encryption key that is stored and processed on a hardware security module (HSM), choose **HSM**.
   - To create a master encryption key that is stored and processed on a server, choose **Software**.
   
   You cannot change a key's protection mode after you create it. For more information about keys, including information about key protection modes, see Key and Secret Management Concepts on page 3953.
7. Click **Name**, and then enter a name to identify the key. Avoid entering confidential information.
8. Click **Key Shape: Algorithm**, and then choose from one of the following algorithms:
   - **AES**. Advanced Encryption Standard (AES) keys are symmetric keys that you can use to encrypt data at rest.
   - **RSA**. Rivest-Shamir-Adleman (RSA) keys are asymmetric keys, also known as key pairs consisting of a public key and a private key, that you can use to encrypt data in transit, to sign data, and to verify the integrity of signed data.
   - **ECDSA**. Elliptic curve cryptography digital signature algorithm (ECDSA) keys are asymmetric keys that you can use to sign data and to verify the integrity of signed data.
9. Depending on what you chose in the previous step, either click **Key Shape: Length** or **Key Shape: Curve ID**, and then choose the key length, in bits, for AES and RSA keys, or specify the curve ID for ECDSA keys. For AES keys, the Vault service supports keys that are exactly 128 bits, 192 bits, or 256 bits in length. For RSA keys, the service supports keys that are 2048 bits, 3072 bits, or 4096 bits. With ECDSA keys, you can create keys that have an elliptic curve ID of NIST_P256, NIST_P384, or NIST_P521.
10. Optionally, to apply tags, click **Show Advanced Options**.

   If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
11. When you are finished, click **Create Key**.

**To view key details**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault with the key you're interested in.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Master Encryption Keys**, and then click the name of the key for which you want to see configuration details. (If needed, first change the list scope to the compartment that contains the key, and then click the key name.)
5. The console displays the following information:
   • **OCID**: The unique, Oracle-assigned ID of the key.
   • **Created**: The date and time when you initially created the key.
   • **Compartment**: The unique, Oracle-assigned ID of the compartment that contains the key.
   • **Protection Mode**: Where the key is stored and processed, whether on a hardware security module (HSM) or on a server (software).
   • **Vault**: The unique, Oracle-assigned ID of the vault that contains the key.
   • **Key Version**: The unique, Oracle-assigned ID of the key version.
   • **Algorithm**: The encryption algorithm used by the key.
   • **Length**: The number of bits in the key length (for AES keys and RSA keys).
   • **Curve ID**: The curve ID of the key (for ECDSA keys).

**To view a list of keys**
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault with the keys you're interested in.
3. From the list of vaults in the compartment, click the vault name.
4. To see a list of keys in this vault, click Master Encryption Keys. You can see keys in other compartments by changing the list scope.

**To view a list of key versions**
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault with the key you're interested in.
3. From the list of vaults in the compartment, click the vault name.
4. Click Master Encryption Keys, click the name of the key for which you want to see a list of key versions, and then click Versions. (If needed, first change the list scope to the compartment that contains the key, and then click the key name.)

**To change the name of a key**
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault with the key you want to rename.
3. From the list of vaults in the compartment, click the vault name.
4. Click Master Encryption Keys, locate the key you want to rename, and then click the Actions icon (three dots) for that key. (If needed, first change the list scope to the compartment that contains the key.)
5. In the Actions menu, click Edit Name.
6. In the Edit Key Name dialog box, click Name, and then enter a new name. Avoid entering confidential information.
7. When you are finished, click Update.

**To manage a key's tags**
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault with the key for which you want to manage tags.
3. From the list of vaults in the compartment, click the vault name.
4. Click Master Encryption Keys, locate the key you want to manage, and then click the key name. (If needed, first change the list scope to the compartment that contains the key, and then click the key name.)
5. On the Key Details page, click the Tags tab to view or edit existing tags. Or, click Add Tags to add new ones.

**To enable a key**
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault with the key you want to enable.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Master Encryption Keys**, locate the key you want to enable, and then select the check box next to the key name. (If needed, first change the list scope to the compartment that contains the key.)
5. In the **Actions** menu, click **Enable**.

### To rotate a master encryption key

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault with the key you want to rotate.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Master Encryption Keys**, locate the key you want to rotate, and then select the check box next to the key name. (If needed, first change the list scope to the compartment that contains the key.)
5. In the **Actions** menu, click **Rotate Key**. (You can only rotate keys in an enabled state.)
6. In the **Confirm** dialog box, click **Rotate Key**.

Cryptographic operations involving objects that were encrypted with the previous version of this key will continue to use the older key version. You can re-encrypt those objects with the current key version if you prefer.

### To disable a key

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault with the key you want to disable.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Master Encryption Keys**, locate the key you want to disable, and then click the Actions icon (three dots) for that key. (If needed, first change the list scope to the compartment that contains the key.)
5. In the **Actions** menu, click **Disable**.

### To delete a key

**Caution:**

When you set a key to the Pending Deletion state, anything encrypted by that key immediately becomes inaccessible. This includes secrets. The key also cannot be assigned or unassigned to any resources or otherwise updated. When the key is deleted, all key material and metadata is irreversibly destroyed. Before you delete a key, either assign a new key to resources currently encrypted by the key or preserve your data another way. If you want to restore use of a key before it is permanently deleted, you can cancel its deletion.

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the key you want to delete.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Master Encryption Keys**, locate the key you want to delete, and then click the Actions icon (three dots) for that key. (If needed, first change the list scope to the compartment that contains the key.)
5. In the **Actions** menu, click **Delete Key**.
6. Confirm that you want to delete the key by clicking the box and then typing the key name.
7. Schedule when you want the Vault service to delete the key. By default, the service schedules keys for deletion 30 days from the current date and time. You can set a range between 7 days and 30 days.
8. When you're ready, click **Delete Key**. If needed, you can restore use of the key and access to encrypted resources and data by canceling the scheduled deletion.
To cancel the deletion of a key

Tip:
You can only cancel the deletion of a key that's in a Pending Deletion state.

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault that has the key you want to delete.
3. From the list of vaults in the compartment, click the vault name.
4. Click Master Encryption Keys. Locate the key you want to delete, and then click the Actions icon (three dots) for that key. (If needed, first change the list scope to the compartment that contains the key.)
5. In the Actions menu, click Cancel Deletion.
6. Confirm that you want to cancel the key's deletion by clicking Cancel Deletion. Access to the key and any resources or data encrypted by the key are restored when key returns to an enabled state.

To move a key to a different compartment

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under Scope, in the Compartment list, choose the compartment that contains the vault that has the master encryption key that you want to move.
3. From the list of vaults in the compartment, click the vault name.
4. Click Master Encryption Keys. Find the key in the list, click the the Actions icon (three dots), and then click Move Resource. (If needed, first change the list scope to the compartment that contains the key.)
5. Choose the destination compartment from the list.
6. Click Move Resource.
7. If there are alarms monitoring the key, update the alarms to reference the new compartment. See To update an alarm after moving a resource on page 2737 for more information.

Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

Tip:
Each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint. When using the CLI for key operations, you must provide the appropriate endpoint for the type of operation. To retrieve a vault's endpoints, see instructions in To view vault configuration details on page 3957.

To create a new key

Open a command prompt and run oci kms management key create to create a new key:

```
oci kms management key create --compartment-id <target_compartment_id> --display-name <key_name> --key-shape <key_encryption_information> --endpoint <control_plane_url>
```

For example, on a MacOS or Linux machine:

```
oci kms management key create --compartment-id ocidl.compartment.oc1...example1example25qrlpo4agcmothkbgmmuz2zzum45ibploogtabwk3zz --display-name key-1 --key-shape '{"algorithm":"AES","length":"16"}' --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```
Or, for example, on a Windows machine:

```bash
oci kms management key create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --display-name key-1 --key-shape '{"algorithm":"AES","length ":"16"}' --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

Avoid entering confidential information.

By default, the service creates a master encryption key protected by an HSM. If you prefer to create a master encryption key protected by software, specify the protection mode with `--protection-mode`. For example, on a Windows machine:

```bash
oci kms management key create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --display-name key-1 --key-shape '{"algorithm":"AES","length":"16"}' --protection-mode SOFTWARE --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

### To create a new key with resource tags

Open a command prompt and run `oci kms management key create` with one or both of the `--defined-tags` and `--freeform-tags` options to create a new key with resource tags:

```bash
oci kms management key create --compartment-id <target_compartment_id> --display-name <key_name> --key-shape <JSON_formatted_key_encryption_information> --defined-tags <JSON_formatted_defined_tag> --freeform-tags <JSON_formatted_freeform_tag> --endpoint <control_plane_url>
```

For example, on a MacOS or Linux machine:

```bash
oci kms management key create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --display-name key-1 --key-shape '{"algorithm":"AES","length":"16"}' --defined-tags '{"Operations": {"CostCenter":"42"}}' --freeform-tags '{"Department":"Finance"}' --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

Or, for example, on a Windows machine:

```bash
oci kms management key create --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --display-name key-1 --key-shape '{"algorithm":"AES","length":"16"}' --defined-tags '{"Operations": {"CostCenter": "42"}}' --freeform-tags '{"Department": "Finance"}' --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

Avoid entering confidential information.

### To view a key's details

Open a command prompt and run `oci kms management key get` to view a specific key's details:

```bash
oci kms management key get --key-id <key_OCID> --endpoint <control_plane_url>
```
For example:

```shell
to change the name of a key

oci kms management key update --key-id ocid1.key.region1.sea.exampleaaacu2.example.com --display-name key-A --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

Avoid entering confidential information.
To enable a key

Open a command prompt and run `oci kms management key enable` to enable a key:

```
oci kms management key enable --key-id <target_key_id> --
endpoint <control_plane_url>
```

For example:

```
oci kms management key enable --key-id
ocid1.key.region1.sea.exampleaaacu2.exampleexamplemtspuqmo45cvblugmizcoeu2nfc6b3zfaux21mqz2
--endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

To rotate a key

Open a command prompt and run `oci kms management key rotate` to rotate a key:

```
oci kms management key rotate --key-id <target_key_id> --
endpoint <control_plane_url>
```

For example:

```
oci kms management key rotate --key-id
ocid1.key.region1.sea.exampleaaacu2.exampleexamplemtspuqmo45cvblugmizcoeu2nfc6b3zfaux21mqz2
--endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

Cryptographic operations involving objects that were encrypted with the previous version of this key will continue to use the older key version. You can re-encrypt those objects with the current key version if you prefer.

To disable a key

Open a command prompt and run `oci kms management key disable` to disable a key:

```
oci kms management key disable --key-id <target_key_id> --
endpoint <control_plane_url>
```

For example:

```
oci kms management key disable --key-id
ocid1.key.region1.sea.exampleaaacu2.exampleexamplemtspuqmo45cvblugmizcoeu2nfc6b3zfaux21mqz2
--endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

To delete a key

**Caution:**
When you set a key to the Pending Deletion state, anything encrypted by that key immediately becomes inaccessible. This includes secrets. The key also cannot be assigned or unassigned to any resources or otherwise updated. When the key is deleted, all key material and metadata is irreversibly destroyed. Before you delete a key, either assign a new key to resources currently encrypted by the key or preserve your data another way. If you want to restore use of a key before it is permanently deleted, you can cancel its deletion.
Open a command prompt and run `oci kms management key schedule-deletion` to schedule a key's deletion:

```
oci kms management key schedule-deletion --key-id <target_key_id> --endpoint <control_plane_url>
```

For example:

```
oci kms management key schedule-deletion --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmg22mlvkq9 --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

By default, the service schedules keys for deletion 30 days from the current date and time. You can set a range between 7 days and 30 days. For example:

```
oci kms management key schedule-deletion --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmg22mlvkq9 --time-of-deletion 2019-06-30T10:00:00Z --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

**To cancel the deletion of a key**

**Tip:**

You can only cancel the deletion of a key that's in a Pending Deletion state.

Open a command prompt and run `oci kms management key cancel-deletion` to cancel a key's scheduled deletion:

```
oci kms management key cancel-deletion --key-id <target_key_id> --endpoint <control_plane_url>
```

For example:

```
oci kms management key cancel-deletion --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmg22mlvkq9 --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

**To move a key to a different compartment**

Open a command prompt and run `oci kms management key change-compartment` to move a master encryption key from one compartment to another within the same tenancy:

```
oci kms management key change-compartment --key-id <target_key_id> --compartment-id <new_compartment_id>
```

For example:

```
oci kms management key change-compartment --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmg22mlvkq9 --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbgqmmuz2zzum45ibploqtabwk3zz
```
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to manage keys:

- CreateKey
- DisableKey
- EnableKey
- GetKey
- UpdateKey
- CreateKeyVersion
- GetKeyVersion
- ListKeys
- ListKeyVersions
- CancelKeyDeletion
- ScheduleKeyDeletion
- ChangeKeyCompartment

Assigning Keys

This topic describes how to assign keys to supported resources and how to remove those key assignments when no longer needed.

Instead of using an encryption key that Oracle manages, you can assign master encryption keys that you manage to block or boot volumes, databases, file systems, buckets, and stream pools. Block Volume, Database, File Storage, Object Storage, and Streaming use the keys to decrypt the data encryption keys that protect the data that is stored by each respective service. By default, these services rely on Oracle-managed master encryption keys for cryptographic operations. When you remove a Vault master encryption key assignment from a resource, the service returns to using an Oracle-managed key for cryptography.

You can also assign master encryption keys to clusters that you create using Container Engine for Kubernetes to encrypt Kubernetes secrets at rest in the etcd key-value store.

For information about managing the creation and usage of master encryption keys and key versions, see Managing Keys on page 3962. For information specifically about creating keys with your own key material, see Importing Keys and Key Versions on page 3986. For information about how you can use keys in cryptographic operations, see Using Keys on page 3998. For information about what you can do with vaults where you store keys, see Managing Vaults on page 3957.

Required IAM Policy

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keys associated with volumes, buckets, file systems, clusters, and stream pools will not work unless you authorize Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming to use keys on your behalf. Additionally, you must also authorize users to delegate key usage to these services in the first place. For more information, see Let a user group delegate key usage in a compartment on page 2152 and Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools on page 2153 in Common Policies on page 2142. Keys associated with databases will not work unless you authorize a dynamic group that includes all nodes in the DB system to manage keys in the tenancy. For more information, see Required IAM Policy on page 1306 in Creating and Managing Exadata Databases on page 1306.</td>
</tr>
</tbody>
</table>
To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which **compartment** you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see *Let security admins manage vaults, keys, and secrets* on page 2151. For more information about permissions or if you need to write more restrictive policies, see *Details for the Vault Service* on page 2347.

If you're new to policies, see *Getting Started with Policies* on page 2135 and *Common Policies* on page 2142.

**Using the Console**

**To assign a key to a new Object Storage bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment where you want to create a bucket that's encrypted with a Vault service master encryption key.
3. Click **Create Bucket**, and then follow the instructions in To create a bucket on page 3401 in *Managing Buckets* on page 3398.

**To assign a key to an existing Object Storage bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the bucket that you want to encrypt with a Vault service master encryption key.
3. From the list of buckets, click the bucket name.
4. Do one of the following:
   - If the bucket already has a key assigned to it, next to **Encryption Key**, click **Edit** to assign a different key.
   - If the bucket does not already have a key assigned to it, next to **Encryption Key**, click **Assign**.
5. Choose the vault compartment, vault, key compartment, and key.
6. When you are finished, click **Assign** or **Update**, as appropriate.

**To assign a key to a new Block Volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment where you want to create a block volume that's encrypted with a Vault service master encryption key.
3. Click **Create Block Volume**, and then follow the instructions in *Creating a Volume*.

**To assign a key to an existing Block Volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the block volume that you want to encrypt with a Vault service master encryption key.
3. From the list of volumes, click the volume name.
4. If the volume is currently attached to an instance, click **Detach from Instance**. Follow the instructions in the **Detach Block Volume** dialog box as appropriate, click **Continue Detachment** and then click **OK**.
5. Then, do one of the following:
   - If the volume already has a key assigned to it, next to **Encryption Key**, click **Edit** to assign a different key.
   - If the volume does not already have a key assigned to it, next to **Encryption Key**, click **Assign**.
6. Choose the vault compartment, vault, key compartment, and key.
7. When you are finished, click **Assign** or **Update**, as appropriate.

**To assign a key to a new file system**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment where you want to create a file system that's encrypted with a Vault service master encryption key.
3. Click **Create File System**, and then follow the instructions in **Creating File Systems** on page 1948.

**To create a Compute instance with an encrypted boot volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment where you want to create an instance with a boot volume that's encrypted with a Vault service master encryption key.
3. Click **Create Instance**, and then follow the instructions in **Launching an Instance**.

**To assign a key to an existing boot volume**

**Note:**

To assign a key to an existing boot volume, you must first detach the boot volume from any instance. However, you can only detach a boot volume from an instance when the instance is stopped. For more information, see **Detaching a Boot Volume** on page 623 and **Stopping and Starting an Instance** on page 779.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the boot volume that you want to encrypt with a Vault service master encryption key.
3. From the list of volumes, click the volume name.
4. Do one of the following:
   - If the volume already has a key assigned to it, next to **Encryption Key**, click **Edit** to assign a different key.
   - If the volume does not already have a key assigned to it, next to **Encryption Key**, click **Assign**.
5. Choose the vault compartment, vault, key compartment, and key.
6. When you are finished, click **Assign** or **Update**, as appropriate.

**To create a Kubernetes cluster with encrypted secrets in the etcd key-value store**

**Note:**

These instructions assume you have already followed the steps in **Encrypting Kubernetes Secrets at Rest in Etcd** on page 900 and created:

- a dynamic group including all clusters in the compartment
- a suitable policy to give the dynamic group access to the master encryption key in Vault

1. Open the navigation menu. Under **Solutions and Platform**, go to **Developer Services** and click **Kubernetes Clusters**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment where you want to create a Kubernetes cluster that has Kubernetes secrets encrypted with a Vault service master encryption key.
3. Click **Create Cluster**, follow the instructions under **Using the Console to create a 'Custom Cluster' with Explicitly Defined Settings** on page 873 in **Creating a Kubernetes Cluster** on page 871, and select the **Encrypt Using Customer-Managed Keys** option.

**To assign a key to a new stream pool**

1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment where you want to create a stream pool that's encrypted with a Vault service master encryption key.
3. Click **Create Stream Pool**, and then follow the instructions in **To create a stream pool** on page 3865 in **Managing Stream Pools** on page 3864.

**To change or remove the master encryption key assigned to an existing stream pool**

1. Open the navigation menu. Under **Solutions and Platform**, click **Analytics**, and then click **Streaming**.
2. Click **Stream Pools**.
3. Click a stream pool to display the stream details page.
4. In **Stream Pool Information**, next to **Encryption Key**, do one of the following:

   - To stop using an Oracle-managed key in favor of a Vault master encryption key that you manage, click **Assign**, select a vault and encryption key you have access to, and then click **Assign**.
   - To select a different Vault master encryption key that you manage, click **Edit**, select a vault and encryption key you have access to, and then click **Update**.
   - Click **Unassign** to remove the assigned Vault master encryption key and let Oracle manage the encryption key, and then click **Unassign** again to confirm the removal of the existing key assignment.

**To remove a key assignment from a bucket**

1. Open the navigation menu. Under **Core Infrastructure**, click **Object Storage**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the bucket from which you want to remove a Vault service key assignment.
3. From the list of buckets, click the bucket name.
4. Next to **Encryption Key**, click **Unassign**.
5. In the **Confirm** dialog box, click **OK** to remove the key assignment from the bucket.

**To remove a key assignment from a Block Volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the block volume from which you want to remove a Vault service key assignment.
3. From the list of volumes, click the volume name.
4. Next to **Encryption Key**, click **Unassign**.
5. In the **Confirm** dialog box, click **OK** to remove the key assignment from the volume.

**To remove a key assignment from a boot volume**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Boot Volumes**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the boot volume from which you want to remove a Vault service key assignment.
3. From the list of volumes, click the volume name.
4. Next to **Encryption Key**, click **Unassign**.
5. In the **Confirm** dialog box, click **OK** to remove the key assignment from the volume.

**To change a key assignment for a file system**

1. Open the navigation menu. Under **Core Infrastructure**, click **File Storage** and then click **File Systems**.
2. Under **List Scope**, in the **Compartment** list, choose the compartment that contains the file system from which you want to remove or change a Vault service key assignment.
3. From the list of file systems, click the file system name.
4. Next to **Encryption Key**, click **Edit**.
5. If you want to use Oracle-managed keys:
   - In **Encryption Type**, select **Encrypt using Oracle-managed keys**.
6. If you want to assign a different customer-managed key:
   - In **Encryption Type**, select **Encrypt using customer-managed keys**.
   - Choose the vault compartment, vault, key compartment, and key.
7. When you are finished, click **Save Changes**.

**To create an X7 or X8 Exadata DB system**

**Tip:** Oracle recommends using the new **Exadata Cloud Service resource model** when provisioning a new service instance. The new resource model is compatible with all available Exadata shape families (X7, X8, and X8M).
The DB system resource described in this topic will be deprecated after a period where both resource models are supported. If you need to provision a service instance using the DB system resource model, you will be able to switch the instance to the new resource model. See To switch an Exadata DB system to the new Exadata resource model on page 1229 for more information. Customers with existing Exadata DB systems will be notified in advance regarding the deprecation of the DB system resource model.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.

2. Click Create DB System.

3. On the Create DB System page, provide the basic information for the DB system:
   - **Select a compartment**: By default, the DB system launches in your current compartment and you can use the network resources in that compartment.
   - **Name your DB system**: A friendly, display name for the DB system. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system. Avoid entering confidential information.
   - **Select an availability domain**: The availability domain in which the DB system resides.
   - **Select a shape type**: The shape type you select sets the default shape and filters the shape options in the next field.

When you select Exadata, you are asked if you would like to use the newer Exadata resource model that replaces the DB system resource with a cloud Exadata infrastructure resource and a cloud VM cluster. These resources are compatible with X7, X8, and X8M hardware generations. Click Continue Creating DB System if you do not want to use the new resource model.

   - **Select a shape**: The shape determines the type of DB system and the resources allocated to the system. To specify a shape other than the default, click Change Shape, and select an available shape from the list. See Exadata Fixed Hardware Shapes: X6, X7, X8 and Exadata Base on page 1351 for available shapes in Oracle Cloud Infrastructure.

   Note that the X8M shape is not available when using the DB system resource model.

   - **Configure the DB system**: Specify the following:
     - **Total node count**: The number of nodes in the DB system. The number depends on the shape you select.
     - **Oracle Database software edition**: The database edition supported by the DB system. Exadata DB systems only support Enterprise Edition - Extreme Performance.
     - **CPU core count**: The number of CPU cores for the DB system. The text below the field indicates the acceptable values for that shape. The core count is evenly divided across the nodes.

You can increase the CPU cores to accommodate increased demand after you launch the DB system.

For an X8 or X7 Exadata DB system, or an Exadata base system, you can specify zero (0) CPU cores when you launch the system. This will provision the system and immediately stop it. See Scaling CPU Cores Within an Exadata Cloud Service Instance on page 1222 for information about CPU core scaling and the impact on billing. Oracle recommends that if you are not provisioning a stopped system (0 cores), that you specify at least 3 cores per node.

   - **Configure storage**: Specify the following:
     - **Cluster Name**: (Optional) A unique cluster name for a multi-node DB system. The name must begin with a letter and contain only letters (a-z and A-Z), numbers (0-9) and hyphens (-). The cluster name can be no longer than 11 characters and is not case sensitive. Avoid entering confidential information.
     - **Storage Allocation**: The configuration settings that determine the percentage of storage assigned to DATA, RECO, and optionally, SPARSE disk:
       - **Database Backups on Exadata Storage**: Select this option if you intend to perform database backups to the local Exadata storage within your Exadata DB system environment. If you select this option, more space is allocated to the RECO disk group, which is used to store backups on Exadata storage.
you do not select this option, more space is allocated to the DATA disk group, which enables you to store more information in your databases.

- **Create Sparse Disk Group**: Select this configuration option if you intend to use snapshot functionality within your Exadata DB system environment. If you select this option, the SPARSE disk group is created, which enables you to use Exadata DB system snapshot functionality for PDB sparse cloning. If you do not select this option, the SPARSE disk group is not created and Exadata DB system snapshot functionality will not be available on any database deployments that are created in the environment.

### Important:

Creating a sparse disk group impacts the storage available for the ASM disk groups (DATA and RECO) and you cannot change the storage allocation configuration after you provision your DB system. For information about the percentage of storage that will be assigned to DATA, RECO, and SPARSE disk based on your configuration, see *Storage Configuration* on page 1224. Similar information will display under the options in the Console dialog.

- **Add public SSH keys**: The public key portion of each key pair you want to use for SSH access to the DB system. You can browse or drag and drop .pub files, or paste in individual public keys. To paste multiple keys, click + Another SSH Key, and supply a single key for each entry.

- **Choose a license type**: The type of license you want to use for the DB system. Your choice affects metering for billing.
  - **License Included** means the cost of the cloud service includes a license for the Database service.
  - **Bring Your Own License (BYOL)** means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premises licenses and cloud licenses.

4. Specify the network information:

- **Virtual cloud network**: The VCN in which to launch the DB system. Click Change Compartment to select a VCN in a different compartment.

- **Client subnet**: The subnet to which the Exadata DB system should attach. Click Change Compartment to select a subnet in a different compartment.

  Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.

- **Backup subnet**: The subnet to use for the backup network, which is typically used to transport backup information to and from Oracle Cloud Infrastructure Object Storage, and for Data Guard replication. Click Change Compartment to select a subnet in a different compartment, if applicable.

  Do not use a subnet that overlaps with 192.168.128.0/20. This restriction applies to both the client subnet and backup subnet.

  If you plan to back up databases to Object Storage, see the network prerequisites in *Managing Exadata Database Backups* on page 1320.

- **Network Security Groups**: Optionally, you can specify one or more network security groups (NSGs) for both the client and backup networks. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to your DB system. A maximum of five NSGs can be specified. For more information,
see Network Security Groups on page 2841 and Network Setup for Exadata Cloud Service Instances on page 1232.

Note that if you choose a subnet with a security list, the security rules for the DB system will be a union of the rules in the security list and the NSGs.

To use network security groups:

- Check the Use Network Security Groups to Control Client Traffic check box. Note that you must have already selected a VCN to be able to assign NSGs to the client network.
- Specify the NSG to use with the client network. You might need to use more than one NSG. If you're not sure, contact your network administrator.
- To use additional NSGs with the client network, click + Another Network Security Group.
- Check the Use Network Security Groups to Control Backup Traffic check box.
- Specify the NSG to use with the backup network just as described previously for the client subnet.
- Hostname prefix: Your choice of host name for the Exadata DB system. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for an Exadata DB system is 12.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The host name must be unique within the subnet. If it is not unique, the DB system will fail to provision.</td>
</tr>
</tbody>
</table>

- Host domain name: The domain name for the DB system. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. Hyphens (-) are not permitted.

If you plan to store database backups in Object Storage, Oracle recommends that you use a VCN Resolver for DNS name resolution for the client subnet because it automatically resolves the Swift endpoints used for backups.

- Host and domain URL: Combines the host and domain names to display the fully qualified domain name (FQDN) for the database. The maximum length is 64 characters.

5. Click Show Advanced Options to specify advanced options for the DB system:

- Disk redundancy: Exadata DB systems support only high redundancy (3-way mirroring).
- Time zone: The default time zone for the DB system is UTC, but you can specify a different time zone. The time zone options are those supported in both the Java.util.TimeZone class and the Oracle Linux operating system. For more information, see DB System Time Zone on page 1575.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to set a time zone other than UTC or the browser-detected time zone, and if you do not see the time zone you want, try selecting the Select another time zone option, then selecting &quot;Miscellaneous&quot; in the Region or country list and searching the additional Time zone selections.</td>
</tr>
</tbody>
</table>

- Tags: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

6. After you completed the network configuration and any advanced options, click Next.
7. Provide information for the initial database:

- **Database name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.

- **Database version:** The version of the initial database created on the DB system when it is launched. After the DB system is active, you can create additional databases on it. You can mix database versions on the DB system.

  **Note:**
  
  If you plan to run Oracle Database 19c on your Exadata DB system, you must specify version 19c when you create the DB system. Earlier database versions are supported on a 19c Exadata DB system and can be created at anytime. Exadata DB systems created with earlier Oracle Database versions will not automatically support Oracle Database 19c. The DB system must be upgraded manually.

- **PDB name:** Not applicable to version 11.2.0.4. The name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of 8 alphanumeric characters. The only special character permitted is the underscore (_).

- **Create administrator credentials:** A database administrator SYS user will be created with the password you supply.
  
  - **Username:** SYS
  - **Password:** Supply the password for this user. The password must meet the following criteria:
    
    A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word “oracle” either in forward or reversed order and regardless of casing.
  - **Confirm password:** Re-enter the SYS password you specified.

- **Select workload type:** Choose the workload type that best suits your application:
  
  - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
  - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.

- **Configure database backups:** Specify the settings for backing up the database to Object Storage:
  
  - **Enable automatic backups:** Check the check box to enable automatic incremental backups for this database.
  - **Backup retention period:** *(Optional)* If you enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
  - **Backup scheduling (UTC):** If you enable automatic backups, you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default
window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See Automatic Incremental Backups for more information.

- **Click Show Advanced Options** to specify advanced options for the initial database.

  In the **Management** tab you can specify the following options:

  - **Character set**: The character set for the database. The default is AL32UTF8.
  - **National character set**: The national character set for the database. The default is AL16UTF16.

  In the **Encryption** tab, **Use Oracle-managed keys** is the only selection and cannot be changed during this creation process. You can change encryption management to use encryption keys that you manage after the database is provisioned. See To administer Vault encryption keys on page 1311 for more information.

  In the **Tags** tab, you can add tags to the database. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

8. **Click Create DB System**. The DB system appears in the list with a status of Provisioning. The DB system's icon changes from yellow to green (or red to indicate errors).

After the DB system's icon turns green in the list of DB systems and displays the Available status, you can click the highlighted DB system name to see details about the DB system. Note the IP addresses. You’ll need the private or public IP address, depending on network configuration, to connect to the DB system.

**To create a database in an existing Exadata Cloud Service instance**

**Note:**

If IORM is enabled on the Exadata Cloud Service instance, the default directive will apply to the new database and system performance might be impacted. Oracle recommends that you review the IORM settings and make applicable adjustments to the configuration after the new database is provisioned.

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment.
3. Navigate to the cloud VM cluster or DB system you want to create the database in:

   - **Cloud VM clusters (new resource model)**: Under Exadata at Oracle Cloud, click Exadata VM Clusters. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.
   - **DB systems**: Under Bare Metal, VM, and Exadata, click DB Systems. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.
4. **Click Create Database**.
5. In the Create Database dialog, enter the following:
   - **Database name**: The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
   - **Database version**: The version of the database. You can mix database versions on the Exadata DB system.
   - **PDB name**: (Optional) For Oracle Database 12c (12.1.0.2) and later, you can specify the name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of eight alphanumeric characters. The only special character permitted is the underscore (_).
   - **Database Home**: The Oracle Database Home for the database. Choose the applicable option:
     - **Select an existing Database Home**: The Database Home display name field allows you to choose the Database Home from the existing homes for the database version you specified. If no Database Home with that version exists, you must create a new one.
     - **Create a new Database Home**: A database home will be created using the database version and the Database Home display name you specified.
   - **Create administrator credentials**: A database administrator SYS user will be created with the password you supply.
     - **Username**: SYS
     - **Password**: Supply the password for this user. The password must meet the following criteria:
       A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two numeric, and two special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.
     - **Confirm password**: Re-enter the SYS password you specified.
   - **Select workload type**: Choose the workload type that best suits your application:
     - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
     - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
   - **Configure database backups**: Specify the settings for backing up the database to Object Storage:
     - **Enable automatic backup**: Check the check box to enable automatic incremental backups for this database. If you are creating a database in a security zone compartment, you must enable automatic backups.
     - **Backup retention period**: If you enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The default selection is 30 days.
     - **Backup Scheduling**: If you enable automatic backups, you can choose a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database. See Automatic Incremental Backups for more information.

6. Click Show Advanced Options to specify advanced options for the database:
   - **Character set**: The character set for the database. The default is AL32UTF8.
   - **National character set**: The national character set for the database. The default is AL16UTF16.
   - If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information
about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

- If you are creating a database in an Exadata Cloud Service VM cluster, then you can choose to use encryption based on encryption keys that you manage. By default, the database is configured using Oracle-managed encryption keys. To configure the database with encryption based on encryption keys you manage:

  a. Click the Encryption tab.

  b. Select Use customer-managed keys. You must have a valid encryption key in Oracle Cloud Infrastructure Vault service. See Let security admins manage vaults, keys, and secrets on page 2151.

  c. Choose a vault from the Vault in compartment drop-down. You can change the compartment by clicking the CHANGE COMPARTMENT link.

  d. Select an encryption key from the Master encryption key in compartment drop-down. You can change the compartment containing the encryption key you want to use by clicking the CHANGE COMPARTMENT link.

  e. If you want to use an encryption key that you import into your vault, then select Choose the key version and enter the OCID of the key you want to use in the Key version OCID field.

  Note:

  - Oracle only supports AES-256 encryption keys.

  - Oracle supports customer-managed keys on databases after Oracle Database 11g release 2 (11.2.0.4).

  - If you choose to provide an OCID for the valid key version, then ensure that the OCID corresponds to the key version you want to use.

7. Click Create Database.

After database creation is complete, the status changes from Provisioning to Available, and on the database details page for the new database, the Encryption section displays the encryption key name and the encryption key OCID.

Caution:

Do not delete the encryption key from the vault. This causes any database protected by the key to become unavailable.

Using the Command Line Interface (CLI)

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

Tip:

Each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint. When using the CLI for key operations, you must provide the appropriate endpoint for the type of operation. To retrieve a vault's endpoints, see instructions in To view vault configuration details on page 3957.

To assign a key to an Object Storage bucket

Open a command prompt and run oci os bucket create to create a bucket that is encrypted with a Vault service master encryption key:

oci os bucket create --name <bucket_name> --compartment-id <target_compartment_id> --kms-key-id <target_key_id>
For example:

```
oci os bucket create --name Bucket-1 --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --kms-key-id ocid1.key.region1.sea.exampleaaacu2.exemploexamplem5cvblugmizcoeu2nfc6b3zfaux2lmgz25
--namespace-name example_namespace
```

Avoid entering confidential information.

**To update the key assigned to an Object Storage bucket**

Open a command prompt and run `oci os bucket update` to update the Vault service master encryption key assigned to a bucket:

```
oci os bucket update --name <bucket_name> --namespace-name <your_namespace> --kms-key-id <target_key_id>
```

For example:

```
oci os bucket update --name Bucket-1 --namespace-name example_namespace --kms-key-id ocid1.key.region1.sea.exampleaaacu2.exemploexamplem5cvblugmizcoeu2nfc6b3zfaux2lmgz25
```

**To create a block volume that’s encrypted with a Vault key**

Open a command prompt and run `oci bv volume create` to create a block volume that is encrypted with a Vault service master encryption key:

```
oci bv volume create --display-name <volume_name> --compartment-id <target_compartment_id> --size-in-gbs <volume_size> --availability-domain <target_availability_domain> --kms-key-id <target_key_id>
```

For example:

```
oci bv volume create --display-name EncryptedBlockVolume --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --size-in-gbs 50 --availability-domain AAbC:US-ASHBURN-AD-1 --kms-key-id ocid1.key.region1.sea.exampleaaacu2.exemploexamplem5cvblugmizcoeu2nfc6b3zfaux2lmgz25
```

**Caution:**

Avoid entering confidential information in the volume name.

**To update a key assigned to an existing Block Volume**

**Tip:**

If the volume is currently attached to an instance, you must first detach it. To do so, open a command prompt and run `oci compute volume-attachment detach --volume-attachment-id <target_blockvolume-attachment_id>`. For more information, see Oracle Cloud Infrastructure CLI Command Reference.
Open a command prompt and run `oci bv volume-kms-key update` to assign a new Vault service master encryption key to an existing block volume:

```
oci bv volume-kms-key update --volume-id <target_blockvolume_id> --kms-key-id <new_key_id>
```

For example:

```
oci bv volume-kms-key update --volume-id ocid1.volume.oc1.sea.examplerwzq7bnohn5vf6b7k4zkp54miqfcvg6xsuvkl1gzzw63mfuu6z5fa --kms-key-id ocid1.key.region1.sea.exampleaaacu2.examplestpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmqz2
```

**To create a boot volume that's encrypted with a Vault key**

Open a command prompt and run `oci bv boot-volume create` to create a boot volume that is encrypted with a Vault service master encryption key:

```
oci bv boot-volume create --display-name <volume_name> --compartment-id <target_compartment_id> --size-in-gbs <volume_size> --availability-domain <target_availability_domain> --kms-key-id <target_key_id>
```

For example:

```
oci bv boot-volume create --display-name EncryptedBlockVolume --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqggmuz2zzum45ibplooqtabwk3zz --size-in-gbs 50 --availability-domain AAbC:US-ASHBURN-AD-1 --kms-key-id ocid1.key.region1.sea.exampleaaacu2.examplestpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmqz2
```

**Caution:**

Avoid entering confidential information in the volume name.

**To create a Compute instance with a boot volume that's encrypted with a Vault key**

1. First, create the JSON input for configuring the instance and boot volume: Open a command prompt and run `oci compute instance launch --generate-full-command-json-input`.
2. Copy, and then paste the output from the command into a text file for editing. Edit the JSON to provide values appropriate for your tenancy and desired image operating system and instance shape. The following example shows the minimum settings required to create an instance and encrypted boot volume.

```json
{
    "availabilityDomain": "ABcD:US-ASHBURN-AD-1",
    "compartmentId": 
    ocid1.tenancy.oc1..examplea54hlbsuugecvb4g67tnth7ouk4iliqpysfauxctd55uiunrykhq",
    "displayName": "InstanceWithEncryptedBootVolume",
    "metadata": {
    },
    "shape": "VM.Standard1.1",
    "subnetId": 
    ocid1.subnet.oc1.iad.exampleaurihk3x3y12vcvb53uz22zgaoujtcwttbxvfauxdvsjmdfv4dza",
    "sourceDetails": {
        "sourceType": "image",
        "imageId": 
        ocid1.image.oc1.iad.exampleaooekczfwutjxzcvb2gcdgdx4yk6x1s7d5fhtlfauxzpaxdedny4a",
        "kmsKeyId": 
        ocid1.key.oc1.iad.exampleoaaeug.examplera4soq2vescvbjmwredhewtt07r1fauxhume73y7jayx
    }
}
```
Caution:
Avoid entering confidential information in the instance name.

3. Save the file with a "json" file extension.
4. In the command prompt, run `oci compute instance launch --from-json file://<file_path>`, providing the location of the file you saved in the previous step. For example:

   ```bash
   oci compute instance launch --from-json file://c:\temp\compute-boot-volume.json
   ```

To update a key assigned to an existing boot volume

Tip:
If the volume is currently attached to an instance, you must first detach the volume. To do so, you must first stop the instance. To stop an instance, open a command prompt and run `oci compute instance action --instance-id <target_instance_id> --action STOP`. Then, to detach the boot volume, run `oci compute boot-volume-attachment detach --boot-volume-attachment-id <target_bootvolume-attachment_id>`. For more information, see the Oracle Cloud Infrastructure CLI Command Reference.

Open a command prompt and run `oci bv boot-volume-kms-key update` to assign a new Vault service master encryption key to an existing boot volume:

   ```bash
   oci bv boot-volume-kms-key update --boot-volume-id <target_bootvolume_id> --kms-key-id <new_key_id>
   ```

   For example:

   ```bash
   oci bv boot-volume-kms-key update --boot-volume-id ocid1.bootvolume.oc1.sea.exampless6hvjs6j6mwc4gfrhtanon3fsqyviqeh522be6wv7x7abz7pq --kms-key-id ocid1.key.region1.sea.exampleaaacu2.examplestpsnuqmoym4rsb1ugmizcoeu2nfc6b3zfaux21mzq2
   ```

To create a Kubernetes cluster with encrypted secrets in the etcd key-value store

Note:
These instructions assume you have already followed the steps in Encrypting Kubernetes Secrets at Rest in Etcd on page 900 and created:

- a dynamic group including all clusters in the compartment
- a suitable policy to give the dynamic group access to the master encryption key in Vault

Open a command prompt and run `oci ce cluster create` to create a cluster where Kubernetes secrets at rest in the etcd data-store are encrypted with a Vault service master encryption key:

   ```bash
   oci ce cluster create --name <cluster_name> --compartment-id <target_compartment_id> --vcn-id <target_vcn_id> --kubernetes-version <kubernetes_version> --kms-key-id <target_key_id>
   ```

   For example:
oci ce cluster create --name EncryptedCluster --compartment-id ocid1.compartment.oc1..example1example25r1p04agcmothkbgqmu2zzum45ibploooqtabwk3zz --vcn-id ocid1.vcn.oc1.iad.exampleexamplesgwertshsdgftyp6c5fplejt3miqvya --kubernetes-version v1.14.8 --kms-key-id ocid1.key.region1.sea.exampleaacu2.examplestpsuqmoy4m5cvblugmixcoeu2nfc6b3zfaux2lmqz2

**Caution:**

Avoid entering confidential information in the cluster name.

**To remove the key assigned to an Object Storage bucket**

Open a command prompt and run `oci os bucket update` to remove the Vault service master encryption key assigned to a bucket:

```
oci os bucket update --name <bucket_name> --namespace-name <your_namespace> --kms-key-id ""
```

For example:

```
oci os bucket update --name Bucket-1 --kms-key-id "" --namespace-name example_namespace
```

**To remove a key assigned to a Block Volume**

Open a command prompt and run `oci bv volume-kms-key delete` to remove the Vault service master encryption key assigned to an existing block volume:

```
oci bv volume-kms-key delete --volume-id <target_blockvolume_id>
```

For example:

```
oci bv volume-kms-key delete --volume-id ocid1.volume.oc1.sea.examplerwzq7bnohn5vf6b7k4zkp54miqfvcvg6xsuvkl1gzzw63mfuu6z5fa
```

**To remove a key assigned to a Block Volume boot volume**

Open a command prompt and run `oci bv boot-volume-kms-key delete` to remove the Vault service master encryption key assigned to an existing boot volume:

```
oci bv boot-volume-kms-key delete --boot-volume-id <target_bootvolume_id>
```

For example:

```
oci bv boot-volume-kms-key delete --boot-volume-id ocid1.bootvolume.oc1.sea.exampleless6hvjs6j6mqwcdv4gfrhtanon3fsqyviqeh522be6wv7x7abz7pq
```

**Using the API**

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to assign keys:

- Container Engine for Kubernetes
  - CreateCluster
Core Services
- LaunchInstance
- CreateBootVolume
- CreateVolume
- UpdateBootVolumeKmsKey
- UpdateVolumeKmsKey
- DeleteBootVolumeKmsKey
- DeleteVolumeKmsKey

File Storage
- CreateFileSystem
- UpdateFileSystem

Object Storage
- CreateBucket
- UpdateBucket

Streaming
- CreateStreamPool
- UpdateStreamPool

Importing Keys and Key Versions

This topic describes how to import key material that you already have. When you create a key or key version, you can import your own key material instead of letting the Vault service generate the key material internally. You might want to "bring your own key" (BYOK) if you need more control over the source of the key material. Or, you might do so if you want to use the same keys that you already use for encryption purposes on-premises or on other clouds.

Imported keys can be AES symmetric keys or RSA asymmetric keys. (The Vault service does not support the import of ECDSA asymmetric keys.) For AES keys, the Vault service supports keys that are exactly 16 bytes (or 128 bits), 24 bytes (or 192 bits), or 32 bytes (or 256 bits) in length. For RSA keys, the service supports keys that are 256 bytes (or 2048 bits), 384 bytes (or 3072 bits), or 512 bytes (or 4096 bits). The key length of the key material itself must match what you specify at the time you create a key or import a key.

Furthermore, before you can import a key, you must wrap the key material by using the public wrapping key provided with each vault. The vault's wrapping key pair make it possible for the HSM to unwrap and store the key securely.

To meet payment card industry (PCI) compliance, you cannot import a key of greater strength than the key that you use to wrap it. Vault wrapping keys are 4096-bit RSA keys. As such, if you want to meet PCI compliance, you cannot import AES keys that are longer than 128 bits.

Also, if you plan to use the command line interface (CLI) to create a new external key or external key version, the key material must also be base64-encoded.

Required IAM Policy

Caution:

Keys associated with volumes, buckets, file systems, clusters, and stream pools will not work unless you authorize Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming to use keys on your behalf. Additionally, you must also authorize users to delegate key usage to these services in the first place. For more information, see Let a user group delegate key usage in a compartment on page 2152 and Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools on page 2153 in Common Policies on page 2142. Keys associated with databases will not work unless
you authorize a dynamic group that includes all nodes in the DB system to
manage keys in the tenancy. For more information, see Required IAM Policy
on page 1306 in Creating and Managing Exadata Databases on page 1306.

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see Let security admins manage vaults, keys, and secrets on page 2151. For more information about permissions or if you need to write more restrictive policies, see Details for the Vault Service on page 2347.

If you’re new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

Before You Begin

To bring your own key, you must first generate an AES or RSA key and then transform the key material by wrapping it. The process by which you transform the key material is called Optimal Asymmetric Encryption Padding (OAEP). OAEP is commonly used with the RSA encryption algorithm (RSA-OAEP). The Vault service supports RSA-OAEP with a SHA-256 hash. Applying RSA-OAEP to wrap the plaintext provides an additional layer of protection to the key material by making it possible for only the HSM in possession of the private RSA wrapping key to unwrap the key.

You can either import the key or key version by using the Console or the CLI. If you use the CLI, we’ve included an example script that you can refer to that includes all steps of the import process, including generating key material, wrapping the key material, and importing the key or key version. If you want to use the Console or the CLI to create a key or key version with imported key material, you must separately apply RSA-OAEP first to wrap the key. With the CLI, you must also base64 encode the wrapped key material before you import it.

If you're using MacOS or Linux, you'll need to install the OpenSSL 1.1.1 series to run commands. If you're using Windows, you'll need to install Git Bash for Windows and run commands with that tool.

Using the Console

The following procedures assume that you already generated key material by using the third-party tool of your choice. Once you have the key material, use the Console to get the public wrapping key that you'll need to wrap the key material. Wrap the key material, and then use the Console to import it as a new master encryption key or a new key version for an existing master encryption key.

To get the public RSA wrapping key

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault in which you want to create the new master encryption key or key version.
3. From the list of vaults in the compartment, click the name of the vault.
4. In Vault Information, click Public Wrapping Key, and then click Copy.

Save the copied wrapping key, and then continue to To apply RSA-OAEP to wrap the key material on page 3987.

To apply RSA-OAEP to wrap the key material

Open a command prompt and run the following command to wrap the AES or RSA key material with the public RSA wrapping key associated with the vault. Replace example file names and values as appropriate.

```
openssl pkeyutl -encrypt -in <key_material_to_import> -
inkey <public_RSA_wrapping_key> -pubin -out <wrapped_key_material> -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
```

For example:
After you wrap the key, you can then either import the key material by creating a new key or by rotating a key to a new key version.

### To import the key material as a new external key

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment where you want to create a key.
3. From the list of vaults in the compartment, do one of the following:
   - Click the name of the vault where you want to import key material for a new key.
   - Create a new vault for the key by following the instructions in To create a new vault, and then click the name of the vault.
4. Click Master Encryption Keys, and then click Create Key.
5. In the Create Key dialog box, choose a compartment from the Create in Compartment list. (Keys can exist outside the compartment the vault is in.)
6. Click Protection Mode, and then click HSM. (At this time, you cannot import key material for keys protected by software.)
7. Click Name, and then enter a name to identify the key. Avoid entering confidential information.
8. Click Key Shape: Algorithm, and then choose from one of the following algorithms:
   - AES. Advanced Encryption Standard (AES) keys are symmetric keys that you can use to encrypt data at rest.
   - RSA. Rivest-Shamir-Adleman (RSA) keys are asymmetric keys, also known as key pairs consisting of a public key and a private key, that you can use to encrypt data in transit.
9. Click Key Shape: Length, and then choose the key length, in bits. For AES keys, the Vault service supports keys that are exactly 128 bits, 192 bits, or 256 bits in length. For RSA keys, the service supports keys that are 2048 bits, 3072 bits, or 4096 bits.
10. Select the Import External Key check box.
11. Click Wrapping Algorithm, and then choose one of the following:
   - RSA_OAEP_SHA256. RSA encryption with Optimal Asymmetric Encryption Padding (RSA-OAEP) with a SHA-256 hash. (This option is not supported for importing RSA key material.)
   - RSA_OAEP_AES_SHA256. RSA-OAEP with a SHA-256 with a temporary AES key.
12. Under External Key Data Source, provide the file that contains the wrapped AES or RSA key material.
13. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
14. When you are finished, click Create Key.

### To import the key material as a new external key version

**Note:**

Key versions must match the shape of the key to which they're added.

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault with the key you want to rotate.
3. From the list of vaults in the compartment, click the name of the vault.
4. Click Master Encryption Keys, and then click the name of the master encryption key that you want to rotate to a new key version.
5. Under Resources, click Versions, and then, in the list of keys, click Rotate Key. (You can only rotate keys in an enabled state.)
6. In the Confirm dialog box, select the Import External Key Version check box.
7. Under **External Key Data Source**, provide the file that contains the wrapped key material.
8. When you're ready, click **Rotate Key**.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**Tip:**
Each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint. When using the CLI for key operations, you must provide the appropriate endpoint for the type of operation. To retrieve a vault's endpoints, see instructions in To view vault configuration details on page 3957.

When using the command line to import key material from outside Oracle Cloud Infrastructure, you can either refer to example scripts or you can run CLI commands individually.

**Example Scripts**

Example scripts illustrate how you might fully automate generating the key material, applying RSA-OAEP to wrap the key material, and then creating the new key or key version based on the imported, wrapped key material.

This section includes example scripts for importing AES key material and RSA key material. You cannot import ECDSA key material.

*Script to import AES key material as a new external key*

Automate the import of AES key material as a new key with the following example script.

Open a command prompt, and then run the following script, replacing example file names and values as appropriate:

```bash
#!/usr/bin/env bash

# This script is for demonstration purposes only. It provides
# a functioning set of calls to show how to import AES keys
# into the Vault service.
#

set -x

OPENSSL="<path_to_OpenSSL>"
AES_KEY="<path_to_AES_key>"
WRAPPING_KEY="<path_to_RSA_wrapping_key>"
WRAPPED_KEY="<path_to_wrapped_AES_key>"

VAULT_KEYMANAGEMENT_ENDPOINT="<target_vault_keymanagement_endpoint>"
COMPARTMENT_ID="<target_compartment_ID>"
DISPLAY_NAME="<key_display_name>"
KEY_SIZE="<key_size_as_bytes>" # Specify 16 (for 128 bits), 24 (for 192 bits), or 32 (for 256 bits).

BASE64="base64"
if [[ $(uname -s) == "MINGW"* ]]; then
  BASE64="base64 -w0"
fi

#
# Generate an AES key.
# Use OpenSSL to generate an AES key of ${KEY_SIZE} bytes.
# You can use any source for your AES key.
# ${OPENSSL} rand ${KEY_SIZE} > ${AES_KEY}

# Ask the Vault service for the public wrapping key by using
# the vault's key management endpoint.
# The public key is stored as ${WRAPPING_KEY}.
# key_text=$(oci kms management wrapping-key get --endpoint
$VAULT_KEYMANAGEMENT_ENDPOINT | grep public-key | cut -d: -f2 | sed 's#
"\(.*\)"#,\1#g')
echo -e $key_text > ${WRAPPING_KEY}

# Wrap the AES key by using RSA-OAEP with SHA-256.
# ${OPENSSL} pkeyutl -encrypt -in ${AES_KEY} -inkey ${WRAPPING_KEY}
-pubin -out ${WRAPPED_KEY} -pkeyopt rsa_padding_mode:oaep -pkeyopt
rsa_oaep_md:sha256

# Import the wrapped key to the Vault service after base64 encoding the
# payload.
# The service will provide a JSON document containing key details.
# key_material=$((${BASE64} ${WRAPPED_KEY}))
echo "{"wrappedAlgorithm": "RSA_OAEP_SHA256"}, "keyMaterial":
{"key_material"} }) > wrapped_import_key.json
echo "{"algorithm": "AES"}, "length": ${KEY_SIZE} ]" > key_shape.json

oci kms management key import --wrapped-import-key file://./wrapped_import_key.json --compartment-id ${COMPARTMENT_ID} --display-name
${DISPLAY_NAME} --endpoint ${VAULT_KEYMANAGEMENT_ENDPOINT} --key-shape
file://./key_shape.json

---

Script to import AES key material as a new external key version

Automate the import of AES key material as a new key version of an existing key with the following example script.

Open a command prompt, and then run the following script, replacing example file names and values as appropriate:

#!/usr/bin/env bash

# This script is for demonstration purposes only. It provides
# a functioning set of calls to show how to import AES keys
# into the Vault service.
#

set -x

OPENSSL="<path_to_OpenSSL>"
AES_KEY="<path_to_AES_key>"
WRAPPING_KEY="<path_to_RSA_wrapping_key>"
WRAPPED_KEY="<path_to_wrapped_AES_key>"
KEY_ID="<key_OCID>"
Vault

KEY_SIZE="<key_size_as_bytes>"

BASE64="base64"
if [ [ $(uname -s) == "MINGW"* ] ]; then
    BASE64="base64 -w0"
fi

# Generate an AES key.
# Use OpenSSL to generate an AES key of ${KEY_SIZE} bytes.
# You can use any source for your AES key.
# ${OPENSSL} rand ${KEY_SIZE} > ${AES_KEY}

# Ask the Vault service for the public wrapping key by using
# the vault's key management endpoint.
# The public key is stored as ${WRAPPING_KEY}.
# key_text=$(oci kms management wrapping-key get --endpoint
  $VAULT_KEYMANAGEMENT_ENDPOINT | grep public-key | cut -d: -f2 | sed 's#
    "\(.\)",\#\1\g'')
echo -e $key_text > ${WRAPPING_KEY}

# Wrap the AES key by using RSA-OAEP with SHA-256.
# ${OPENSSL} pkeyutl -encrypt -in ${AES_KEY} -inkey ${WRAPPING_KEY}
  -pubin -out ${WRAPPED_KEY} -pkeyopt rsa_padding_mode:oaep -pkeyopt
  rsa_oaep_md:sha256

# Import the wrapped key to the Vault service after base64 encoding the
# payload.
# The service will provide a JSON document containing key details.
# key_material=${(BASE64) ${WRAPPED_KEY})
echo "{"wrappingAlgorithm": "RSA_OAEP_SHA256", "keyMaterial":
  "${key_material}"}" > wrapped_import_key.json
echo "{"algorithm": "AES", "length": ${KEY_SIZE}}" > key_shape.json

oci kms management key import --wrapped-import-key file://./wrapped_import_key.json --compartment-id ${COMPARTMENT_ID} --display-name ${DISPLAY_NAME} --endpoint ${VAULT_KEYMANAGEMENT_ENDPOINT} --key-shape file://./key_shape.json

##### IMPORT NEW KEY VERSION #####
# import the key version by using the CLI
oci kms management key-version import --key-id ${KEY_ID} --wrapped-import-key ${WRAPPED_KEY}

Script to import RSA key material as a new external key
Automate the import of RSA key material as a new key with the following example script.

Open a command prompt, and then run the following script, replacing example file names and values as appropriate:

#!/bin/bash
# This script is for demonstration purposes only. It provides
# a functioning set of calls to show how to import RSA keys
# into the Vault service.
#
set -e;
set -x;

while getopts ":k:w:o:" opt; do
  case $opt in
    k) key_size=$OPTARG
    ;;
    w) wrapping_key=$OPTARG
    ;;
    o) output_file=$OPTARG
    ;;
    \?) echo "Invalid option -$OPTARG. Valid options are -k (keySize), -w
          (Public Wrapping Key), -o (Output file)" >&2
    ;;
  esac
done

OPENSSL_PATH="<path_to_OpenSSL>"
WORK_DIR=$(mktemp -d -t kms_XXXX)
echo "Openssl Path: ", ${OPENSSL_PATH}
echo "Work Dir: " , ${WORK_DIR}
echo

# Generate a private key.
private_key_path=${WORK_DIR}/private_key.pem
$(OPENSSL_PATH) genrsa -out ${private_key_path} ${key_size}

# Convert the private key to PKCS8 DER format.
target_key_path=${WORK_DIR}/target_key.key
$(OPENSSL_PATH) pkcs8 -topk8 -nocrypt -inform PEM -outform DER -in
          ${private_key_path} -out ${target_key_path}

# Generate a temporary AES key.
temp_aes_key_path=${WORK_DIR}/temp_aes_key.key
$(OPENSSL_PATH) rand -out ${temp_aes_key_path} 32

# Wrap the temporary AES key by using RSA-OAEP with SHA-256.
wrapped_temp_aes_key=${WORK_DIR}/wrapped_temp_aes_key.bin
$(OPENSSL_PATH) pkeyutl -encrypt -in ${temp_aes_key_path} -inkey
          ${wrapping_key} -pubin -out ${wrapped_temp_aes_key} -pkeyopt
          rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256

# Wrap the target RSA key.
wrapped_target_key=${WORK_DIR}/wrapped_target_key.bin

# Create the wrapped key material.
wrapped_key_material=${WORK_DIR}/wrappedKeyMaterial.bin

# Create the wrapped key material.
wrapped_key_material=${WORK_DIR}/wrappedKeyMaterial.bin

cp -fv ${wrapped_key_material} ${output_file}
rm -rfv ${WORK_DIR}
**Individual Commands**
Review the commands in this section if you want to run the CLI commands individually rather than use an example script or if you want to examine the individual steps in the example scripts.

The commands in this section assume that you already generated key material by using the third-party tool of your choice. Once you have the key material, use the CLI to get the public wrapping key that you’ll need to wrap the key material. Wrap the key material by applying RSA-OAEP, and then use the CLI again to import the key material as a new master encryption key or a new key version for an existing master encryption key.

<table>
<thead>
<tr>
<th>Tip:</th>
</tr>
</thead>
<tbody>
<tr>
<td>We recommend that you provide complex input, such as JSON, by providing a file that contains the input, rather than formatting the input in the command line.</td>
</tr>
</tbody>
</table>

**To get the public RSA wrapping key**

Open a command prompt and run `oci kms management wrapping-key get` to get the vault’s public RSA wrapping key:

```
oci kms management wrapping-key get --endpoint <control_plane_URL>
```

For example:

```
oci kms management wrapping-key get --endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```

After you get the public wrapping key, wrap the AES key material by applying RSA-OAEP.

**To apply RSA-OAEP to wrap the key material**

Open a command prompt and run the following command to wrap the AES or RSA key material with the public RSA wrapping key associated with the vault. Replace example file names and values as appropriate.

```
openssl pkeyutl -encrypt -in <key_material_to_import> -inkey <public_RSA_wrapping_key> -pubin -out <wrapped_key_material> -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
```

For example:

```
openssl pkeyutl -encrypt -in "aes_key.bin" -inkey "publickey.pem" -pubin -out "wrappedkey.bin" -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
```

After you wrap the key, you can then either import the key material by creating a new key or by rotating a key to a new key version.

**To import the key material as a new external key**

Open a command prompt and run `oci kms management key import` to import the wrapped AES or RSA key material with the public RSA wrapping key associated with the vault:

```
oci kms management key import --wrapped-import-key <wrapped_key_material> --compartment-id <compartment_id> --display-name <key_name> --endpoint <control_plane_URL> --key-shape <key_encryption_information>
```

For example:

```
oci kms management key import --wrapped-import-key file:///wrapped_import_key.json --compartment-id
```
To import the key material as a new external key version

Open a command prompt and run `oci kms management key-version import` to import the wrapped AES or RSA key material as a new key version for an existing key:

```
oci kms management key-version import --key-id <key_OCID> --wrapped-import-key <wrapped_key_material>
```

For example:

```
oci kms management key-version import --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2n6b3zfaux2lmqz245gezevsq --wrapped-import-key file://./wrapped_import_key.json
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to wrap and import keys:

- GetWrappingKey
- ImportKey
- ImportKeyVersion
- ExportKey

Exporting Keys and Key Versions

You can export a software-protected master encryption key or key version if you want to use it to perform cryptographic operations in an application running on a client instead of performing those same operations in the cloud with the Vault service. You can use the key locally, and then discard the key from local memory to protect the key contents. Using an exported key locally improves availability, reliability, and latency.

Required IAM Policy

**Caution:**

Keys associated with volumes, buckets, file systems, clusters, and stream pools will not work unless you authorize Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming to use keys on your behalf. Additionally, you must also authorize users to delegate key usage to these services in the first place. For more information, see Let a user group delegate key usage in a compartment on page 2152 and Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools on page 2153 in Common Policies on page 2142. Keys associated with databases will not work unless you authorize a dynamic group that includes all nodes in the DB system to manage keys in the tenancy. For more information, see Required IAM Policy on page 1306 in Creating and Managing Exadata Databases on page 1306.

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message

---

Oracle Cloud Infrastructure User Guide 3994
that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see Let security admins manage vaults, keys, and secrets on page 2151. For more information about permissions or if you need to write more restrictive policies, see Details for the Vault Service on page 2347.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Before You Begin**

Exporting a key requires you to generate your own RSA key pair to wrap and unwrap the key material. You can use the third-party tool of your choice to generate the RSA key pair.

You can export the key or key version by using the CLI only. We've included example scripts that you can refer to. The scripts include all steps of the export process, from wrapping the key material to exporting the software-protected key or key version.

If you're using MacOS or Linux, you'll need to install the OpenSSL 1.1.1 series to run commands. (If you plan to use the RSA encryption algorithm that uses a temporary AES key, then you must also patch OpenSSL with a patch that supports it.) If you're using Windows, you'll need to install Git Bash for Windows and run commands with that tool.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

Tip:

Each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint. When using the CLI for key operations, you must provide the appropriate endpoint for the type of operation. To retrieve a vault's endpoints, see instructions in To view vault configuration details on page 3957.

This section provides example scripts that you can use to fully automate applying RSA-OAEP to wrap the key material, and then exporting the wrapped key or key version. Choose the appropriate example script for the type of RSA key wrap mechanism, whether you want to use the RSA encryption algorithm (with OAEP padding using SHA-256) that includes a temporary AES key or not. Also ensure that you patch OpenSSL if you plan to use the script that uses a temporary AES key.

The example scripts are based on the `oci kms crypto key export` command, which exports a software-protected master encryption key:

```bash
oci kms crypto key export --key-id <key_OCID> --algorithm <encryption_algorithm> --public-key "<public_RSA_wrapping_key>" --endpoint <data_plane_url>
```

To export a software-protected master encryption key by applying RSA-OAEP with a temporary AES key

The following example script invokes the RSA AES key wrap mechanism to generate a temporary AES key that wraps and unwraps the exportable key material. The process by which you transform the temporary AES key is called Optimal Asymmetric Encryption Padding (OAEP). OAEP is commonly used with the RSA encryption algorithm (RSA-OAEP). The Vault service supports RSA-OAEP with a SHA-256 hash.

Applying OAEP with the RSA encryption algorithm (RSA-OAEP) with a SHA-256 hash to wrap the temporary AES key with the provided public RSA wrapping key generates a wrapped temporary AES key. The wrapped temporary
AES key and the wrapped exportable key material are concatenated to produce blob output that jointly represents them and which only the possessor of the private RSA wrapping key can decrypt.

To export a software-protected master encryption key, open a command prompt, and then run the following script, replacing example file names and values as appropriate:

```bash
#!/usr/bin/env bash

# This script is for demonstration purposes only. It provides
# a functioning set of calls to show how to export software-protected
# AES key material
# from the Vault service by using the RSA_OAEP_AES_SHA256 algorithm.
#

set -x

OPENSSL="<path_to_OpenSSL>" # Use OpenSSL 1.1.1.
KEY_OCID="<key_OCID>" # The Oracle Cloud Identifier (OCID) of the software-
# protected master encryption key to export.
ENCRYPTION_ALGORITHM="RSA_OAEP_AES_SHA256"
RSA_KEY_SIZE_IN_BYTES="<key_size_in_bytes>" # Specify 256 (for 2048 bits) or
# 512 (for 4096 bits).
VAULT_CRYPTO_ENDPOINT="<vault_data_plane_URL>" # The cryptographic endpoint
# of the vault that contains the software-protected master encryption key.
PUBLIC_KEY_STRING="<public_RSA_wrapping_key_in_PEM_format>" # The content of
# the public key.
PRIVATE_KEY_PATH="<path_to_private_RSA_wrapping_key>" # The location of the
# private key.
SOFTWARE_KEY_PATH="<path_to_output_exported_master_encryption_key>" # The
# location for outputting the software-protected master encryption key.
TEMP_AES_KEY_PATH="<path_to_output_temporary_AES_key>" # The location for
# outputting the temporary AES key.
TEMP_WRAPPED_AES_PATH="<path_to_output_wrapped_temporary_AES_key>" # The
# location for outputting the wrapped temporary AES key.
WRAPPED_SOFTWARE_KEY_PATH="<path_to_output_wrapped_master_encryption_key>"
# The location for outputting the wrapped software-protected master
# encryption key, otherwise known as the wrapped target key.

declare -a hex_array wrapped_temp_aes_key_array wrapped_targetKey_array
wrapped_targetKey_array_length

# Invoke the CLI to export a software-protected master encryption key. (The
# response contains the wrapped data in two parts.
# The first part is a wrapped temporary AES key. The second part is the
# wrapped software-protected master encryption key,
# also known as the wrapped target key.)
wrapped_data=$(oci kms crypto key export --key-id ${KEY_OCID} --algorithm
#${ENCRYPTION_ALGORITHM} --public-key "${PUBLIC_KEY_STRING}" --endpoint
${VAULT_CRYPTO_ENDPOINT} | grep encrypted-key | cut -d: -f2 | sed 's# "(.*
\"),\#1\g"')"

# Decode the encoded wrapped data and convert it to hexadecimal format.
wrapped_data_hex_array=('echo $(wrapped_data) | base64 -d | xxd -p -cl')
wrapped_data_hex_array_length=${#wrapped_data_hex_array[*]}

# Extract the wrapped temporary AES key. (The length of this first portion
of the wrapped data is equal to the length of the private RSA wrapping
key.)
wrapped_temp_aes_key_array=($"$(wrapped_data_hex_array[@]:0:
$RSA_KEY_SIZE_IN_BYTES")")
start_index_target_key=${#wrapped_temp_aes_key_array[*]}
To export a software-protected master encryption key by applying RSA-OAEP without a temporary AES key

The following example script transforms the software-protected master encryption key through a mechanism called Optimal Asymmetric Encryption Padding (OAEP). OAEP is commonly used with the RSA encryption algorithm (RSA-OAEP). The Vault service supports RSA-OAEP with a SHA-256 hash.

The script wraps the software-protected master encryption key with the provided public RSA wrapping key, and then unwraps and exports it with the private RSA wrapping key. Only the possessor of the private RSA wrapping key can decrypt the wrapped master encryption key.

To export a software-protected master encryption key, open a command prompt, and then run the following script, replacing example file names and values as appropriate:

```bash
#!/usr/bin/env bash

# This script is for demonstration purposes only. It provides
# a functioning set of calls to show how to export software-protected
# AES key material
# from the Vault service by using the RSA_OAEP_SHA256 algorithm.
#

set -x

OPENSSL="<path_to_OpenSSL>" # Use OpenSSL 1.1.1.
```
# Vault

## Key OCI ID

The Oracle Cloud Identifier (OCID) of the software-protected master encryption key to export:

```
KEY_OCID="<key_OCID>" # The Oracle Cloud Identifier (OCID) of the software-
protected master encryption key to export.
```

## Encryption Algorithm

The cryptographic endpoint of the vault that contains the software-protected master encryption key:

```
ENCRYPTION_ALGORITHM="RSA_OAEP_SHA256"
```

## Vault Crypto Endpoint

The cryptographic endpoint of the vault that contains the software-protected master encryption key:

```
VAULT_CRYPTO_ENDPOINT="<vault_data_plane_URL>" # The cryptographic endpoint
of the vault that contains the software-protected master encryption key.
```

## Public Key String

The content of the public key:

```
PUBLIC_KEY_STRING="<public_RSA_wrapping_key_in_PEM_format>" # The content of
the public key.
```

## Private Key Path

The location of the private key:

```
PRIVATE_KEY_PATH="<path_to_private_RSA_wrapping_key>" # The location of the
private key.
```

## Software Key Path

The location for outputting the software-protected master encryption key:

```
SOFTWARE_KEY_PATH="<path_to_output_exported_key>" # The location for
outputting the software-protected master encryption key.
```

## Wrapped Software Key Path

The location for outputting the decoded, wrapped software-protected master encryption key:

```
WRAPPED_SOFTWARE_KEY_PATH="<path_to_output_decoded_wrapped_target_key>" #
The location for outputting the decoded, wrapped software-protected master
encryption key.
```

# Invoke the CLI to export a software-protected master encryption key.

```
wrapped_data=$(oci kms crypto key export --key-id ${KEY_OCID} --algorithm
${ENCRYPTION_ALGORITHM} --public-key "${PUBLIC_KEY_STRING}" --endpoint
${VAULT_CRYPTO_ENDPOINT} | grep  encrypted-key | cut -d: -f2  | sed 's#
\(.*\),\#\1\g\1'#
```

# Decode the encoded wrapped data.

```
echo ${wrapped_data} | base64 -d > ${WRAPPED_SOFTWARE_KEY_PATH}
```

# Unwrap the wrapped software-protected key material by using the private RSA wrapping key.

```
${OPENSSL} pkeyutl -decrypt -in ${WRAPPED_SOFTWARE_KEY_PATH} -
inkey ${PRIVATE_KEY_PATH} -pkeyopt rsa_padding_mode:oaep -pkeyopt
rsa_oaep_md:sha256 -pkeyopt rsa_mgf1_md:sha256 -out ${SOFTWARE_KEY_PATH}
```

## Using Keys

This topic describes what you can do with keys in terms of cryptographic operations and signing operations. For information about managing keys, see Managing Keys on page 3962. For information about exporting keys, see Exporting Keys and Key Versions on page 3994. For information about managing the vaults in which you store keys, see Managing Vaults on page 3957.

Cryptographic operations include the following:

- Encrypting data
- Decrypting data
- Generating data encryption keys
- Signing data
- Verifying signed data

You can use either the command line interface (CLI) or API to perform cryptographic operations.

## Required IAM Policy

### Caution:

Keys associated with volumes, buckets, file systems, clusters, and stream pools will not work unless you authorize Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming to use keys on your behalf. Additionally, you must also authorize users to delegate key usage to these services in the first place. For more information, see Let a user group delegate key usage in a compartment on page 2152 and Let Block Volume, Object Storage, File Storage, Container Engine for Kubernetes, and Streaming services encrypt and decrypt volumes, volume backups, buckets, file systems, Kubernetes secrets, and stream pools on page 2153 in Common Policies on page 2142. Keys associated with databases will not work unless

Oracle Cloud Infrastructure User Guide 3998
you authorize a dynamic group that includes all nodes in the DB system to manage keys in the tenancy. For more information, see Required IAM Policy on page 1306 in Creating and Managing Exadata Databases on page 1306.

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see Let security admins manage vaults, keys, and secrets on page 2151. For more information about permissions or if you need to write more restrictive policies, see Details for the Vault Service on page 2347.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Monitoring Resources**

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring the traffic associated with your master encryption keys, see Vault Metrics on page 4020.

**Using the Console**

**To view the public key of an asymmetric key**

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment where the key exists.
3. From the list of vaults in the compartment, click the name of the vault that contains the key.
4. Under Master Encryption Keys, click the name of the key.
5. Under Resources, click Versions.
6. In the list of key versions, find the key for which you want to view the public key, click the Actions menu, and then click View Public Key.
7. Do one of the following:
   - To copy the contents of the public key, click Copy. The contents of the public key are copied to your clipboard.
   - To download the public key, click Download. The file is automatically downloaded to your local computer.
8. When you are finished, click Close.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see Command Line Interface (CLI). For a complete list of flags and options available for CLI commands, see the Command Line Reference.

**Tip:**

Each vault has a unique endpoint for create, update, and list operations for keys. This endpoint is referred to as the control plane URL or management endpoint. Each vault also has a unique endpoint for cryptographic operations. This endpoint is known as the data plane URL or the cryptographic endpoint. When using the CLI for key operations, you must provide the appropriate endpoint for the type of operation. To retrieve a vault's endpoints, see instructions in To view vault configuration details on page 3957.
To encrypt data by using your Vault master encryption key

You can use either AES symmetric keys or RSA asymmetric keys to encrypt or decrypt data. ECDSA keys do not support the cryptography required to encrypt or decrypt data. If you want to encrypt data by using an RSA asymmetric key, then you must also provide the --key-version-id of the key. To decrypt the data, you need to provide the same --key-version-id. The need to track key versions exists because, unlike symmetric keys, an asymmetric key’s ciphertext does not contain the information that the service needs for decryption purposes.

Open a command prompt and run `oci kms crypto encrypt` to encrypt data:

```bash
oci kms crypto encrypt --key-id <key_OCID> --plaintext <base64_string> --endpoint <data_plane_url>
```

For example:

```bash
oci kms crypto encrypt --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmqz2 --plaintext VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4= --endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```

Optionally, you can include the `--associated-data` option to provide an encryption context that might contain useful, but non-secret, information about the encrypted data. That information is associated with the encrypted data such that the data cannot be decrypted without it, providing an extra layer of protection. Associated data must be properly formatted JSON.

If using an RSA asymmetric key, provide the public key.

```bash
oci kms crypto encrypt --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmqz2 --plaintext VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4= --associated-data '{"CustomerId":"12345", "Custom Data":"custom data"}' --endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```

To decrypt data by using your Vault master encryption key

You can use AES symmetric keys or RSA asymmetric keys to encrypt or decrypt data. ECDSA keys do not support the cryptography required to encrypt or decrypt data.

Open a command prompt and run `oci kms crypto decrypt` to decrypt data:

```bash
oci kms crypto decrypt --key-id <key_OCID> --ciphertext <base64_string> --endpoint <data_plane_url>
```

For example:

```bash
oci kms crypto decrypt --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmqz2 --ciphertext VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4= --endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```
If you want to decrypt data previously encrypted by an RSA asymmetric key, then you must also provide the `--key-version-id` of the key that encrypted the data. The need to track key versions exists because, unlike symmetric keys, an asymmetric key's ciphertext does not contain the information that the service needs for decryption purposes. If the data you want to decrypt had an encryption context associated with it at the time of encryption, the same encryption context is required to decrypt the data. For example, the `--associated-data` in the following sample matches what was provided in the preceding sample command for encrypting data.

```bash
oci kms crypto decrypt --key-id
ocid1.key.region1.sea.exampleaaacu2.exampleesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmgz2
--ciphertext VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmyIy9HROZSBSYXp5IGRvZy4=
--associated-data '{"CustomerId":"12345", "Custom Data":"custom data"}'
--endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```

**To generate a data encryption key from your Vault master encryption key**

**Note:**
You can only use AES symmetric keys to generate data encryption keys. You cannot generate data encryption keys from RSA and ECDSA asymmetric keys.

Open a command prompt and run `oci kms crypto generate-data-encryption-key` to generate a data encryption key that you can then use to encrypt and decrypt data:

```bash
oci kms crypto generate-data-encryption-key --key-id <key_OCID> --key-shape <key_encryption_information> --include-plaintext-key <Boolean_value> --endpoint <data_plane_url>
```

For example:

```bash
oci kms crypto generate-data-encryption-key --key-id
ocid1.key.region1.sea.exampleaaacu2.exampleesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmgz2
--key-shape file://path/to/json/file --include-plaintext-key true
--endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```

**To view the public key of an asymmetric key**

Open a command prompt and run `oci kms management key-version get` to view the public key of an asymmetric key:

```bash
oci kms management key-version get --key-id <key_OCID> --key-version-id <keyversion_OCID> --endpoint <control_plane_url>
```

For example:

```bash
oci kms management key-version get --key-id
ocid1.key.region1.sea.exampleaaacu2.exampleesmtpsuqmoy4m5cvblugmizcoeu2nfc6b3zfaux2lmgz2
--key-version-id
ocid1.keyversion.region1.sea.example5aacuu.ajmfauxaaa.abuwcljt2lolvy7221paefa53mb12fr
--endpoint https://exampleaaacu2-management.kms.us-ashburn-1.oraclecloud.com
```
To sign data by using your Vault master encryption key

**Note:**
You can only use RSA or ECDSA asymmetric keys to digitally sign data and verify signed data. AES keys do not support the asymmetric cryptography required to sign data or to verify signed data.

Open a command prompt and run `oci kms crypto signed-data sign` to sign a message:

```
oci kms crypto signed-data sign --key-id <key_OCID> --key-version-id <keyversion_OCID> --message <base64_string> --signing-algorithm <key_algorithm> --endpoint <data_plane_url>
```

For example:

```
oci kms crypto signed-data sign --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtspuqmooy4m5cvblugmizcoeu2nfcbf3zaux21mq2fz2 --key-version-id ocid1.keyversion.region1.sea.example5aaccu.uumjmfauxaaa.abuwcljt2lo1vy7221paefaf53mb12f4 --message VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4= --signing-algorithm SHA_224_RSA_PKCS_PSS --endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```

To verify signed data by using your Vault master encryption key

**Note:**
You can only use RSA or ECDSA asymmetric keys to digitally sign data and verify signed data. AES keys do not support the asymmetric cryptography required to sign data or to verify signed data.

Open a command prompt and run `oci kms crypto verified-data verify` to verify the integrity of signed data:

```
oci kms crypto verified-data verify --key-id <key_OCID> --key-version-id <keyversion_OCID> --message <base64_string> --signature <base64_string> --signing-algorithm <key_algorithm> --endpoint <data_plane_url>
```

For example:

```
oci kms crypto verified-data verify --key-id ocid1.key.region1.sea.exampleaaacu2.examplesmtspuqmooy4m5cvblugmizcoeu2nfcbf3zaux21mq2fz2 --key-version-id ocid1.keyversion.region1.sea.example5aaccu.uumjmfauxaaa.abuwcljt2lo1vy7221paefaf53mb12f4 --message VGhlIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIHRoZSBsYXp5IGRvZy4= --signature VGhpcyBpcyBhIHNpZ25hdHVyZS4= --signing-algorithm SHA_224_RSA_PKCS_PSS --endpoint https://exampleaaacu3-crypto.kms.us-ashburn-1.oraclecloud.com
```

Using the API

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use the following operations to use keys in cryptographic operations:

- Decrypt
- Encrypt
- GenerateDataEncryptionKey
ExportKey
Sign
Verify

Back up vp vaults and keys

This topic describes how to preserve virtual private vaults and encryption keys. You can create backups of these resources to store in a bucket or offline, outside of Oracle Cloud Infrastructure.

Currently, the only type of vault you can back up is a virtual private vault. Similarly, the only type of encryption key that you can back up is a master encryption key protected by a hardware security module (HSM). You cannot back up master encryption keys protected by software. You also cannot back up secrets.

You might want to back up a vault or encryption key before deleting either if you don't need them now, but think you might need to use the key for decryption later. Deleting a vault and key otherwise means losing the ability to decrypt any resource or data that the key was used to encrypt. Restoring a key lets you resume using a resource that was previously encrypted by the key.

You might also create a backup of a vault to use in a disaster recovery scenario. You can restore a backup in any region within the realm, making it possible to access encrypted resources even in disaster recovery scenarios where the region of the backed-up resource is no longer available.

Note:

By default, a key backup includes metadata about the vault it's associated with. A vault backup might optionally include key metadata, but you cannot back up secrets, whether independently or as part of a vault backup. You can only back up and restore encryption keys protected by an HSM and virtual private vaults.

For information about creating and managing the use of keys, see Managing Keys on page 3962. For information about what you can do with vaults where you store keys and secrets, see Managing Vaults on page 3957. For information about creating and managing the use of secrets, see Managing Secrets on page 4007.

How it works

Keys are always associated with the vault where you created them. This relationship persists even as the key is backed up and restored. As a result, restoring a key always requires you to already have the vault associated with the key. You also need the vault because the vault hosts the management and cryptographic endpoints against which you manage and use the key. This might mean that you need to first restore the vault, and then restore the key, if both were backed up and subsequently deleted.

You back up a vault or key by exporting identifying information about the vault or key and what it contains. (The service encrypts the backups, and only the service can restore them.) Vault backups can optionally include keys, assuming the vault has keys and the keys are in a supported lifecycle state when you perform the backup. You can only back up active, enabled, or disabled keys. Backups exclude keys that are deleted or in a transitional state (for example, "Creating" or "Pending Deletion"). Key backups always include vault metadata, in addition to key metadata. Having vault metadata makes it possible to restore the key at all. You can only back up active vaults.

You can back up only one vault or one key at a time. (The exception is when you backup keys as part of a vault backup.) When you perform a key backup, the file includes all associated key versions in an enabled state. Backups exclude key versions in a deleted or pending deletion state.

Backup operations require you to specify where to download the backup. Downloads can be stored in a new or existing Object Storage bucket or a temporary URL that's created specifically for pre-authenticated requests. For more information about pre-authenticated requests, see Using Pre-Authenticated Requests on page 3482. Backups must be stored in buckets in the same region, but you can copy the backup to a different region by using Object Storage.

Backup and restore operations generate work requests to help you track their progress.

You restore a vault or key by importing the backup from storage to where you want it, as long as you restore the vault to the same tenancy and compartment where you originally created the backup. The key also can only be restored to
its original tenancy and compartment, which might be a different compartment from the vault. You can, however, restore vaults and keys to a different region if your tenancy spans multiple regions.

You can restore a vault or a key individually. If you included keys in a vault backup, then restoring the vault restores all the keys included in the backup. Restoring a key restores all the key versions included in the backup.

You can restore a vault or key even when the vault or key already exists in the region. Also, at any time, you can take a newer backup of a vault or key if you want to capture changes to the vault, such as a new name or tags, or the keys, such as new key versions. Updating an already restored vault or key reflects those changes. Updates from a backup are always additive. This means that updates can only append new information. For example, any new key versions created in a reference vault are added to its restored key when you update the restored key. But, if you delete a key from a reference vault, and then you update a restored vault from a backup of the reference vault, the update does not result in a corresponding key deletion in the restored vault. Similarly, any keys that you create for a restored vault are independent of any keys associated with the reference vault that you created the backup from. You manage them independently, too.

Most other operations are not allowed while a backup or restore operation is in progress. This prevents you from deleting a key while it's being backed up, for example. Prohibited operations include attempts to perform simultaneous backup or restore operations on the same resource.

To make it easier to reuse any policies that you created to allow management and use of vaults and keys, when you restore a vault and key, they maintain the same unique Oracle Cloud Identifier (OCID) if they're restored to the region where they were originally backed up. When you restore a vault or key to a different region, you must review and update policies to correspond to new OCIDs.

When you restore a vault or key, especially a key with a lot of key versions, tenancy service limits do apply.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators: for typical policies that give access to vaults, keys, and secrets, see Let security admins manage vaults, keys, and secrets on page 2151. For more information about permissions or if you need to write more restrictive policies, see Details for the Vault Service on page 2347.

Depending on where you want to store backups and retrieve them from, you might also need access to an Object Storage bucket. For administrators: for typical policies that gives access to buckets, see Let users write objects to Object Storage buckets on page 2149 and Let users download objects from Object Storage buckets on page 2149.

If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

**Using the Console**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only active virtual private vaults and active, enabled, or disabled keys can be exported to a backup.</td>
</tr>
</tbody>
</table>

To back up a vault

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault that you want to back up.
3. From the list of vaults in the compartment, click the name of the vault.
5. Choose a source: export a backup to either an Existing Object Storage Bucket (recommended) or a pre-authenticated Object Storage URL for an object that you can write to.
6. Do one of the following, depending on what you chose in the previous step:
   - Choose a bucket from the dropdown menu. If needed, you can change the compartment to find a bucket in a different compartment. Then, specify the **Backup Name**. Avoid entering confidential information.
   - Click **Object Storage URL**, and then provide a pre-authenticated URL for an object.

7. Optionally, to back up only the vault without any keys, select the **Back up vault metadata only** check box.

8. When you are finished, click **Back Up Vault**. (Note the compartment so that you can restore this resource to the right compartment later.)

**To back up a key**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the key that you want to back up.
3. From the list of vaults in the compartment, click the name of the vault that contains the key.
4. Click **Master Encryption Keys**, and then click the name of the key that you want to back up. (If needed, first change the list scope to the compartment that contains the key, and then click the key name.)
5. On the **Key Details** page, click **Back Up Key**.
6. Choose a source: export a backup to either an **Existing Object Storage Bucket** (recommended) or a pre-authenticated Object Storage URL that you can write to.
7. Do one of the following, depending on what you chose in the previous step:
   - Choose a bucket from the dropdown menu. If needed, you can change the compartment to find a bucket in a different compartment. Then, specify the **Backup Name**. Avoid entering confidential information.
   - Click **Object Storage URL**, and then provide a pre-authenticated URL to an object.
8. When you are finished, click **Back Up Key**. (Note the compartment so that you can restore this resource to the right compartment later.)

**To restore a vault**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment where you want to restore a vault. The compartment must match the compartment of the reference vault at the time of backup.
3. Click **Restore Vault**.
4. Choose a source. You can import a backup from an **Existing Object Storage Bucket** that you have access to or a pre-authenticated Object Storage URL. You can also **Upload a File** from your computer or a mapped network location.
5. Do one of the following, depending on what you chose in the previous step:
   - Choose a bucket from the dropdown menu. If needed, you can change the compartment to find a bucket in a different compartment. Then, specify the **Backup Name**. Avoid entering confidential information.
   - Click **Object Storage URL**, and then provide a pre-authenticated URL. Include the backup name.
   - In **Choose a file**, drag and drop a file or, to browse for a file, click **select one**.
6. When you are finished, click **Restore Vault**.

**To update a vault from a backup**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that you want to update from a backup.
3. From the list of vaults in the compartment, click the name of the vault.
4. On the **Vault Details** page, click **Update Vault from Backup**.
5. Choose a source. You can import a backup from an **Existing Object Storage Bucket** that you have access to or a pre-authenticated Object Storage URL. You can also **Upload a File** from your computer or a mapped network location.
6. Do one of the following, depending on what you chose in the previous step:
   • Choose a bucket from the dropdown menu. If needed, you can change the compartment to find a bucket in a different compartment. Then, specify the Backup Name. Avoid entering confidential information.
   • Click Object Storage URL, and then provide a pre-authenticated URL. Include the backup name.
   • In Choose a file, drag and drop a file or, to browse for a file, click select one.
7. When you are finished, click Update Vault.

To restore a key
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment of the vault that contains the key that you want to restore.
3. From the list of vaults in the compartment, click the name of the vault. You must choose the same vault where the key was backed up originally. (If needed, also change the list scope to the compartment where the key was at the time of backup.)
4. Click Master Encryption Keys, and then click Restore Key.
5. Choose a source. You can import a backup from an Existing Object Storage Bucket or a pre-authenticated Object Storage URL that you can write to. You can also Upload a File from your computer or a mapped network location.
6. Do one of the following, depending on what you chose in the previous step:
   • Choose a bucket from the dropdown menu. If needed, you can change the compartment to find a bucket in a different compartment. Then, specify the Backup Name. Avoid entering confidential information.
   • Click Object Storage URL, and then provide a pre-authenticated URL to an object.
7. When you are finished, click Restore Key.

To update a key from a backup
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment of the vault that contains the key that you want to update from a backup.
3. From the list of vaults in the compartment, click the name of the vault that contains the key.
4. Click Master Encryption Keys, click the key name, and then click Update Key from Backup. (If needed, change the list scope to the compartment of the key, if the key is in a different compartment from the vault.)
5. Choose a source. You can import a backup from an Existing Object Storage Bucket that you have access to or a pre-authenticated Object Storage URL. You can also Upload a File from your computer or a mapped network location.
6. Do one of the following, depending on what you chose in the previous step:
   • Choose a bucket from the dropdown menu. If needed, you can change the compartment to find a bucket in a different compartment. Then, specify the Backup Name. Avoid entering confidential information.
   • Click Object Storage URL, and then provide a pre-authenticated URL. Include the backup name.
7. When you are finished, click Update Key.

To view a work request for a backup or restore operation
1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment of the vault (or the vault of the key) that you're interested in.
3. From the list of vaults in the compartment, click the name of the vault, and then click Work Requests.
4. Optionally, click Master Encryption Keys, click the key name, and then click Work Requests. (If needed, change the list scope to the compartment of the key, if the key is in a different compartment from the vault.)
5. For detailed information about the work request, click the work request name.
Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following operations to back up and restore virtual private vaults and keys:

- BackupVault
- RestoreVaultFromFile
- RestoreVaultFromObjectStore
- RestoreKeyFromFile
- RestoreKeyFromObjectStore

Managing Secrets

**Note:**
Support for secrets is not available in Oracle Cloud Infrastructure US Government Cloud realms.

This topic describes how to manage secrets. Management of secrets includes the ability to do the following:

- Create secrets
- View secret details
- View a list of secrets
- View a list of secret versions for a specific secret
- Update a secret description
- Create a new secret version (by updating secret contents)
- Promote a secret version to current
- Manage a secret's tags
- View a secret's rules
- Add or edit secret rules
- Delete secrets or secret versions to permanently prevent the use of their secret contents
- Move a secret to a new compartment

Before You Begin

Before you begin, we recommend that you first read Rules for Secrets on page 4019 and Secret Versions and Rotation States on page 4018 to better understand the implications of working with rules, secret versions, and secret version rotation states.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

For administrators:

- The policy Let security admins manage vaults, keys, and secrets on page 2151 lets the specified group do everything with vaults, keys, and secrets.
- The policy Let security admins manage all secrets in a specific vault in a compartment on page 2153 lets the specified group do everything with secrets in a specific vault.
- The policy Let users read, update, and rotate all secrets on page 2153 lets the specified group read, update, and rotate all secrets in any vault in the tenancy.
- For more information about permissions or if you need to write more restrictive policies for secrets, see Details for the Vault Service on page 2347.
If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

### Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

### Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about monitoring the traffic associated with your secrets, see Vault Metrics on page 4020.

### Moving Resources to a Different Compartment

You can move secrets from one compartment to another. After you move a secret to a new compartment, inherent policies apply immediately and affect access to the secret and secret versions. Moving a secret doesn't affect access to the vault that a secret is associated with. Similarly, you can move a vault from one compartment to another independently of moving any of its secrets. For more information, see Managing Compartments on page 2431.

### Using the Console

**To create a new secret**

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment where you want to create a secret.
3. From the list of vaults in the compartment, do one of the following:
   - Click the name of the vault where you want to create a secret.
   - Create a new vault for the secret by following the instructions in To create a new vault, and then click the name of the vault.
4. Click Secrets, and then click Create Secret.
5. In the Create Secret dialog box, choose a compartment from the Create in Compartment list. (Secrets can exist outside the compartment the vault is in.)
6. Click Name, and then enter a name to identify the secret. Avoid entering confidential information.
7. Click Description, and then enter a brief description of the secret to help identify it. Avoid entering any confidential information in this field.
8. Choose the master encryption key that you want to use to encrypt the secret contents while they're imported to the vault. (The key must belong to the same vault. The key must also be a symmetric key. You cannot encrypt secrets with asymmetric keys.)
9. Specify the format of the secret contents you're providing by choosing a template type from the Secret Type Template list. (You can provide secret contents in plain-text when you use the Console to create a secret or secret version, but secret contents do need to be base64-encoded before they're sent to the service. The Console automatically encodes plain-text secret contents for you if you choose this format.)
10. Click Secret Contents, and then enter the secret contents. (The maximum allowable size for a secret bundle is 25 KB.)
11. Optionally, you can apply a rule to manage how secrets are used. You can either create a rule regarding the reuse of secret contents across versions of a secret, or you can create a rule specifying when the secret contents expire. For more information about rules, see Rules for Secrets on page 4019.

- **Rule Type.** You can specify a Secret Reuse Rule or a Secret Expiry Rule. At most, you can have one of each. If you already have one rule, but want to add another, click **+ Another Rule.**
- **Reuse rule configuration:** You can either enforce the reuse rule so it applies even to deleted secrets versions, or you can allow reuse of secret contents from deleted secret versions.
- **Expiry rule configuration:** You can set how frequently you want secret contents to expire and what you want to happen when the secret or secret version expires. Expiration of individual secret versions is represented by a period of 1 to 90 days that you can specify with the arrow buttons or entering a number. Expiration of the secret itself is represented by an absolute time and date between 1 to 365 days from the current time and date. Specify this date by using the date picker. You can configure expiry values for both the secret version and secret or just one of the two. (It's possible to clear the secret version expiry interval, but you must delete the entire expiry rule and start over if you want to set an absolute time to expire the secret.)

12. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

13. When you are finished, click **Create Secret.**

### To view secret details

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault.**
2. Under **List Scope,** in the **Compartment** list, click the name of the compartment that contains the vault that has the secret you're interested in.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Secrets,** and then click the name of the secret for which you want to see configuration details. (If needed, first change the list scope to the compartment that contains the secret, and then click the secret name.)
5. The console displays the following information:
   - **OCID:** The unique, Oracle-assigned ID of the secret.
   - **Created:** The date and time when you initially created the secret.
   - **Compartment:** The name of the compartment that contains the secret.
   - **Vault:** The name of the vault that contains the secret.

### To view a list of secrets

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault.**
2. Under **List Scope,** in the **Compartment** list, click the name of the compartment that contains the vault that has the secrets you're interested in.
3. From the list of vaults in the compartment, click the vault name.
4. To see a list of secrets in this vault, click **Secrets.** You can see secrets in different compartments by changing the list scope.

### To view a list of secret versions

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault.**
2. Under **List Scope,** in the **Compartment** list, click the name of the compartment that contains the vault that has the secret you're interested in.
3. From the list of vaults in the compartment, click the vault name.
4. Click **Secrets,** and then click the name of the secret for which you want to see a list of secret versions. (If needed, first change the list scope to the compartment that contains the secret, and then click the secret name.)
5. Under **Secret Version List,** you can see all versions that exist for the selected secret. For more information about secret versions, see Secret Versions and Rotation States on page 4018.

### To update a secret description

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault.**
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the secret with the description you want to update.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, and then click the name of the secret you want to edit. (If needed, first change the list scope to the compartment that contains the secret.)

5. Click **Edit**.

6. In the **Edit Secret** dialog box, click **Description**, and then enter a new description. Avoid entering any confidential information in this field.

7. When you are finished, click **Save Changes**.

**To update a secret's contents to create a new secret version**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.

2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault with the secret you want to provide with new secret contents.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, and then click the name of the secret with the secret contents you want to update. (If needed, first change the list scope to the compartment that contains the secret.)

5. Click **Create Secret Version**. (You can only create a new secret version for a secret that's not pending deletion.)

6. Specify the format of the secret contents you're providing by choosing a template type from the **Secret Type Template** list. (You can provide secret contents in plain-text when you use the Console to create a secret or secret version, but secret contents do need to be base64-encoded before they're sent to the service. The Console automatically encodes plain-text secret contents for you if you choose this format.)

7. Click **Secret Contents**, and then enter the secret contents. (The maximum allowable size for a secret bundle is 25 KB.)

8. If you don't want to immediately promote the new secret version to current, select the **Set to Pending** check box. Otherwise, this new secret version is automatically promoted as the current version.

9. Click **Create Secret Version**.

**To promote an existing secret version to current**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.

2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the secret that you want to update.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, and then click the name of the secret that you want to update to use a different secret version. (If needed, first change the list scope to the compartment that contains the secret.)

5. Make a different secret version the current secret version by doing one of the following:
   - Click **Edit**, click **Current Version**, and then click the version number you want to promote. When you're ready, click **Save Changes**.
   - Under **Secret Version List**, locate the version number that you want to promote, click the Actions icon (three dots) for that secret version, and then click **Promote to Current**. Confirm the promotion by clicking **Promote to Current**.

**To manage a secret's tags**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.

2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the secret for which you want to manage tags.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, locate the secret you want to manage, and then click the secret name. (If needed, first change the list scope to the compartment that contains the secret, and then click the secret name.)

5. On the **Secret Details** page, click the **Tags** tab to view or edit existing tags. Or, click **Add Tags** to add new ones.

**To view a secret's rules**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the secret for which you want to view configured rules.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, and then click the name of the secret that has rules you want to view. (If needed, first change the list scope to the compartment that contains the secret, and then click the secret name.)

5. On the **Secret Details** page, click **Rules** to view existing rules.

**To edit a secret’s rules**

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.

2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the secret for which you want to add or edit rules.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, and then click the name of the secret. (If needed, first change the list scope to the compartment that contains the secret, and then click the secret name.)

5. On the **Secret Details** page, click **Rules**, and then click **Add/Edit Rules**.

   • **Rule Type**. You can specify a **Secret Reuse Rule** or a **Secret Expiry Rule**. At most, you can have one of each. If you already have one rule, but want to add another, click **+ Another Rule**.

   • Reuse rule configuration: You can either enforce the reuse rule so it applies even to deleted secrets versions, or you can allow reuse of secret contents from deleted secret versions.

   • Expiry rule configuration: You can set how frequently you want secret contents to expire and what you want to happen when the secret or secret version expires. Expiration of individual secret versions is represented by a period of 1 to 90 days that you can specify with the arrow buttons or entering a number. Expiration of the secret itself is represented by an absolute time and date between 1 to 365 days from the current time and date. Specify this date by using the date picker. You can configure expiry values for both the secret version and secret or just one of the two. (It’s possible to clear the secret version expiry interval, but you must delete the entire expiry rule and start over if you want to set an absolute time to expire the secret.)

6. If you want to delete a rule while you're configuring them, do one of the following:

   • To delete the secret version rule, clear the days configured.

   • To delete the rule altogether, click the X next to the rule.

7. When you're ready, click **Save Changes**.

**To delete a secret**

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a secret is pending deletion, resources or services that rely on that secret immediately become inaccessible. The secret also can't be rotated or otherwise updated. When the secret is deleted, its are irreversibly destroyed. If you want to restore the use of a secret before it is permanently deleted, you can cancel its deletion.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under the **Governance and Administration** group, go to **Security** and click **Vault**.

2. Under **List Scope**, in the **Compartment** list, click the name of the compartment that contains the vault that has the secret you want to delete.

3. From the list of vaults in the compartment, click the vault name.

4. Click **Secrets**, locate the secret you want to delete, and then click the Actions icon (three dots) for that secret. (If needed, first change the list scope to the compartment that contains the secret.)

5. In the **Actions** menu, click **Delete Secret**.

6. Confirm that you want to delete the secret by clicking the box and then typing the secret name.

7. Schedule when you want Vault to delete the secret. By default, the service schedules secrets for deletion 30 days from the current date and time. You can set a range between 1 day and 30 days.

8. When you're ready, click **Delete Secret**. If needed, you can restore use of the secret and access to resources and services that use the contents of that secret by canceling the scheduled deletion and making the secret version current again.
To delete a secret version

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a secret version is pending deletion, resources or services that rely on that secret version immediately become inaccessible. The secret version also can't be rotated or otherwise updated. When the secret version is deleted, its contents are irreversibly destroyed. If you want to restore the use of a secret version before it is permanently deleted, you can cancel its deletion.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault that has the secret with the secret version you want to delete.
3. From the list of vaults in the compartment, click the vault name.
4. Click Secrets, and the click the secret name. (If needed, first change the list scope to the compartment that contains the secret.)
5. Under Secret Versions List, locate the secret version, and then click the Actions icon (three dots) for that secret version.
6. In the Actions menu, click Delete Secret Version.
7. Confirm that you want to delete the secret version by clicking the box and then typing the secret version number.
8. Schedule when you want Vault to delete the secret version. By default, the service schedules secret versions for deletion 30 days from the current date and time. You can set a range between 1 day and 30 days.
9. When you're ready, click Delete Secret Version. If needed, you can restore use of the secret version and access to resources or services that use the contents of that secret version by canceling the scheduled deletion and making the secret version current again.

To cancel the deletion of a secret

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault that has the secret you no longer want to delete.
3. From the list of vaults in the compartment, click the vault name.
4. Click Secrets, locate the secret for which you want to cancel deletion, and then click the Actions icon (three dots) for that secret. (If needed, first change the list scope to the compartment that contains the secret.)
5. In the Actions menu, click Cancel Deletion.
6. Confirm that you want to cancel the secret's deletion by clicking Cancel Deletion. Access to the secret and any resources or services that used the contents of the secret can be restored after the secret returns to active, current use.

To cancel the deletion of a secret version

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under List Scope, in the Compartment list, click the name of the compartment that contains the vault that has the secret with the secret version you no longer want to delete.
3. From the list of vaults in the compartment, click the vault name.
4. Click Secrets, locate the secret with the secret version for which you want to cancel deletion, and then click the secret name. (If needed, first change the list scope to the compartment that contains the secret.)
5. Under Secret Versions List, locate the secret version, and then click the Actions icon (three dots) for that secret version.
6. In the Actions menu, click Cancel Deletion.
7. Confirm that you want to cancel the secret version's deletion by clicking Cancel Deletion. Access to the secret version and any resources or services that used its contents can be restored after the secret version returns to active, current use.

To move a secret to a different compartment

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Under **Table Scope**, in the **Compartment** list, choose the compartment that contains the vault that has the secret that you want to move.

3. Click **Secrets**. Find the secret in the list, click the the Actions icon (three dots), and then click **Move Resource**. (If needed, first change the list scope to the compartment that contains the secret.)

4. Choose the destination compartment from the list.

5. Click **Move Resource**.

6. If there are alarms monitoring the secret, update the alarms to reference the new compartment. See **To update an alarm after moving a resource** on page 2737 for more information.

**Using the Command Line Interface (CLI)**

For information about using the CLI, see **Command Line Interface (CLI)**. For a complete list of flags and options available for CLI commands, see the **Command Line Reference**.

**Tip:**

Each region has a unique endpoint for create, update, and list operations for secrets. This endpoint is referred to as the control plane URL or secret management endpoint. Each region also has a unique endpoint for operations related to retrieving secret contents. This endpoint is known as the data plane URL or the secret retrieval endpoint. When using the CLI for secret operations, you must provide the appropriate endpoint for the type of operation. For regional endpoints, see the **API Documentation**.

**To create a new secret**

Open a command prompt and run `oci vault secret create-base64` to create a new secret:

```
oci vault secret create-base64 --compartment-id <target_compartment_id> --secret-name <secret_name> --vault-id <target_vault_id> --description <secret_description_text> --key-id <encryption_key_id> --secret-content-content <base64_encoded_secret_content> --secret-content-name <unique_content_name> --secret-content-stage <secret_version_rotation_state>
```

For example:

```
oci vault secret create-base64 --compartment-id ocid1.compartment.oc1..example1example25qrlpo4agcmothkbqgmmuz2zzum45ibplooqtabwk3zz --secret-name testSecret --vault-id ocid1.vault.oc1.iad.exampleyaaeuk.examplesuxtdqzvrwzk4ouq2mh2234o4oq4ghmt6rrzr9example --description "this is a test secret" --key-id ocid1.key.oc1.iad.exampleyaaeuk.abuwcvbrsvwr2nbvrraqomsmhpc74rlq2vpwyv3byhikd4577rxy7example --secret-content-content bXlwYXNzd29yZA== --secret-content-name testpassword1 --secret-content-stage CURRENT
```

Avoid entering confidential information.

**To view a secret's details**

Open a command prompt and run `oci vault secret get` to view a specific secret's details:

```
oci vault secret get --secret-id <secret_OCID>
```
For example:

```
oci vault secret get --secret-id
oci.vaultsecret.ocl.iad.exampleaz5qacpqahuecvbqzql4qmpbrtd7pprafhvckfik6wuitexample
```

To view a list of secrets

Open a command prompt and run `oci vault secret list` to list secrets in a vault:

```
oci vault secret list --compartment-id <target_compartment_id>
```

For example:

```
oci vault secret list --compartment-id
oci.compartment.ocl.example1.example2.5qrlpo4agcmothkbqgqvmuz2zzum45ibploooqtabwk3zz
```

To view a list of secret versions

Open a command prompt and run `oci vault secret-version list` to view a list of secret versions for a specific secret:

```
oci vault secret-version list --secret-id <secret_OCID>
```

For example:

```
oci vault secret-version list --secret-id
oci.vaultsecret.ocl.iad.exampleaz5qacpqahuecvbqzql4qmpbrtd7pprafhvckfik6wuitexample
```

To update a secret description

Open a command prompt and run `oci vault secret update` to edit a secret's description.

**Caution:**

Avoid entering confidential information in the secret description. Also, you must update the current secret version number, secret contents, and secret rules independently of one another. Lastly, you can only update secrets in an Active lifecycle state.

```
oci vault secret update --secret-id <secret_OCID> --description <secret_description_text>
```

For example:

```
oci vault secret update --secret-id
oci.vaultsecret.ocl.iad.exampleaz5qacpqahuecvbqzql4qmpbrtd7pprafhvckfik6wuitexample
--description "this is a new secret description"
```

To update a secret's contents to create a new secret version

Open a command prompt and run `oci vault secret update-base64` to update a secret's contents to create a new secret version:

```
oci vault secret update-base64 --secret-id <target_secret_id> --secret-content-content <base64_encoded_secret_content>
```
For example:

```bash
oci vault secret update-base64 --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbjqzql4qmpbrtd7pprafhivcfik6wuitexample
--secret-content-content bXluZXdwYXNzd29yZA==
```

**To promote an existing secret version to current**

Open a command prompt and run `oci vault secret update` to promote a secret version to current, active use:

```bash
oci vault secret update --secret-id <target_secret_id> --current-version-number <target_secret_version_number>
```

For example:

```bash
oci vault secret update --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbjqzql4qmpbrtd7pprafhivcfik6wuitexample
--current-version-number 3
```

**To manage a secret's tags**

Open a command prompt and run `oci vault secret update` to manage a secret's tags:

```bash
oci vault secret update --secret-id <target_secret_id> --defined-tags <defined_tags_in_JSON_format>
```

For example:

```bash
oci vault secret update --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbjqzql4qmpbrtd7pprafhivcfik6wuitexample
--defined-tags '{"ProdSecrets" : {"NodePool" : "10"}}'
```

**To view a secret's rules**

Open a command prompt and run `oci vault secret get` to view a secret's configured rules:

```bash
oci vault secret get --secret-id <target_secret_id>
```

For example:

```bash
oci vault secret get --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbjqzql4qmpbrtd7pprafhivcfik6wuitexample
```

**To edit a secret's rules**

Open a command prompt and run `oci vault secret update` to edit a secret's configured rules:

```bash
oci vault secret update --secret-id <target_secret_id> --secret-rules <secret_rules_in_JSON_format>
```

For example:

```bash
oci vault secret update --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbjqzql4qmpbrtd7pprafhivcfik6wuitexample
```
You can specify a secret reuse rule or a secret expiry rule. At most, you can have one of each rule type.

**To delete a secret**

**Caution:**

When a secret is pending deletion, resources or services that rely on that secret immediately become inaccessible. The secret also can't be rotated or otherwise updated. When the secret is deleted, secret contents are irreversibly destroyed. If you want to restore the use of a secret before it is permanently deleted, you can cancel its deletion.

Open a command prompt and run `oci vault secret schedule-secret-deletion` to schedule a secret's deletion:

```
oci vault secret schedule-secret-deletion --secret-id <target_secret_id> --time-of-deletion <time_in_rfc3339_format>
```

For example:

```
oci vault secret schedule-secret-deletion --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbqjzql4qmpbrtd7pprafhivcfik6wuitexample --time-of-deletion 2020-04-30T10:00:00Z
```

By default, the service schedules secrets for deletion 30 days from the current date and time. You can set a range between 1 day and 30 days.

**To delete a secret version**

**Caution:**

When a secret version is pending deletion, resources or services that rely on that secret version immediately become inaccessible. The secret version also can't be rotated or otherwise updated. When the secret version is deleted, its contents are irreversibly destroyed. If you want to restore the use of a secret version before it is permanently deleted, you can cancel its deletion.

Open a command prompt and run `oci vault secret-version schedule-deletion` to schedule a secret version's deletion:

```
oci vault secret-version schedule-deletion --secret-id <target_secret_id> --secret-version-number <target_secret_version_number> --time-of-deletion <time_in_rfc3339_format>
```

For example:

```
oci vault secret-version schedule-deletion --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbqjzql4qmpbrtd7pprafhivcfik6wuitexample --secret-version-number 1 --time-of-deletion 2020-04-09
```

By default, the service schedules secret versions for deletion 30 days from the current date and time. You can set a range between 1 day and 30 days. In the preceding example, because no time is specified, the time of deletion defaults to midnight Coordinated Universal Time (UTC).
To cancel the deletion of a secret
Open a command prompt and run `oci vault secret cancel-secret-deletion` to cancel the scheduled deletion of a secret:

```
oci vault secret cancel-secret-deletion --secret-id <target_secret_id>
```
For example:

```
oci vault secret cancel-secret-deletion --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbqzql1qmpbrtd7pprafhivcfik6wuiexample
```

To cancel the deletion of a secret version
Open a command prompt and run `oci vault secret-version cancel-deletion` to cancel the scheduled deletion of a secret version:

```
oci vault secret-version cancel-deletion --secret-id <target_secret_id> --secret-version-number <target_secret_version_number>
```
For example:

```
oci vault secret-version cancel-deletion --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbqzql1qmpbrtd7pprafhivcfik6wuiexample --secret-version-number 1
```

To move a secret to a different compartment
Open a command prompt and run `oci vault secret change-compartment` to move a secret to a different compartment:

```
oci vault secret change-compartment --secret-id <target_secret_id> --compartment-id <new_compartment_id>
```
For example:

```
oci vault secret change-compartment --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbqzql1qmpbrtd7pprafhivcfik6wuiexample --compartment-id ocid1.tenancy.oc1..exampleati4wjo6cvbxq4iusld51sdsnescfyz7lr4r46wfauxuwrwed5b3xea
```

To view the contents and properties of the current secret version
Open a command prompt and run `oci secrets secret-bundle get` to view the contents and properties of the current secret version:

```
oci secrets secret-bundle get --secret-id <target_secret_id> --stage <target_secret_version_rotation_state>
```
For example:

```
oci secrets secret-bundle get --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbqzql1qmpbrtd7pprafhivcfik6wuiexample --stage CURRENT
```
To view the properties for all versions of a secret

Open a command prompt and run `oci secrets secret-bundle-version list-versions` to view information about each of a secret's secret versions:

```
oci secrets secret-bundle-version list-versions --secret-id <target_secret_id>
```

For example:

```
oci secrets secret-bundle-version list-versions --secret-id ocid1.vaultsecret.oc1.iad.exampleaz5qacpqahuecvbjqzql4qmpbrtd7pprafhivcfik6wuitexample
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Tip:

Each region has a unique endpoint for create, update, and list operations for secrets. This endpoint is referred to as the control plane URL or secret management endpoint. Each region also has a unique endpoint for operations related to retrieving secret contents. This endpoint is known as the data plane URL or the secret retrieval endpoint. For regional endpoints, see the API Documentation.

Use the following operations to manage secrets:

- CreateSecret
- GetSecret
- UpdateSecret
- GetSecretVersion
- ListSecrets
- ListSecretVersions
- ScheduleSecretDeletion
- CancelSecretDeletion
- ScheduleSecretVersionDeletion
- CancelSecretVersionDeletion
- ChangeSecretCompartment

Use the following operations to retrieve secrets:

- GetSecretBundle
- ListSecretBundleVersions

Secret Versions and Rotation States

Note:

Support for secrets is not available in Oracle Cloud Infrastructure US Government Cloud realms.

This topic explains the relationship between secrets, secret versions, and rotation states. It also discusses the impact of service limits on secret versions. Understanding secret versions and rotation states will help you track and manage secret contents to stay in compliance with any limits, rotation or other rules, or regulations. For a basic definition of secret concepts, including secret versions and rotation states, see Key and Secret Management Concepts on page 3953. For information about working with secret versions, see Managing Secrets on page 4007.
Secret Versions

Every secret has at least one secret version. Every time you update the contents of a secret, you create a new secret version. Secret version numbers start at 1 and increment by 1. While every secret has at least one version, you might have multiple versions of a secret at any given time.

In addition to a version number, you can identify a secret version by its version name or rotation state. A secret version's rotation state represents how the secret is being used. Typically, applications need the current version of a secret. Marking a secret version as the 'current' version indicates that it has the secret contents currently used for access to the intended resource. Meaning, if you stored the password to connect to a database as a secret, when you request the current version of that secret, you do so with the knowledge that it's the password that the database currently expects.

Rotation States

Secret versions can have more than one rotation state at a time. Where only one secret version exists, such as when you first create a secret, the secret version is automatically marked as both 'current' and the 'latest'. The 'latest' version of a secret contains the secret contents that were last uploaded to the vault, in case you want to keep track of that.

When you rotate a secret to upload new secret contents, you can mark it as 'pending'. Marking a secret version's rotation state as 'pending' lets you upload the secret contents to the vault without immediately putting them into active use. You can continue using the 'current' secret version until you're ready to promote a pending secret version to 'current' status. This typically happens after you’ve rotated credentials on the target resource or service first. You don’t want to unexpectedly change a secret version. Changing what secret version is current prevents the application that needs it from retrieving the expected secret version from the vault.

For the purposes of rolling back to a previous version easily, such as when you've made a mistake in updating the secret contents or when you've restored a backup of an older resource and need to resume using older secret contents, secret versions can also be marked as 'previous.' A secret version marked as 'previous' was previously a secret version marked as 'current.' To roll back to a previous version, you update the secret to specify the secret version number you want.

As long as a secret version hasn't been deleted, you can update the secret to use that past secret version. When you update the secret, the secret version number you choose gets marked as 'current.' This has the same effect as promoting a secret version to 'current.'

You can only delete secret versions that have been marked as 'deprecated.' A deprecated secret version is one that’s not marked as 'current', 'pending', or 'previous.' This helps to prevent circumstances where you might delete a secret version that you need later (for example, when restoring a database you backed up previously). A secret version that’s marked as anything other than 'deprecated' can be marked as 'current' to return it to active use.

Secret Version Limits

The limits on secret versions applies to both a secret’s versions that are in use and versions that are deprecated, including those that have been scheduled for deletion. For information about limits on the number of versions for a given secret and for secret versions in a tenancy, see Service Limits.

Rules for Secrets

This topic explains how the rules you configure for secrets govern their usage. Configuring rules for secrets can help you meet compliance requirements. For information about how to configure or view rules, see Managing Secrets on page 4007.

When you create a secret, you can configure the following types of rules:
• **Secret Reuse Rule.** This type of rule prevents the reuse of secret contents across different versions of a secret.

• **Secret Expiry Rule.** This type of rule restricts how long the secret contents of a particular secret version can remain in use. This rule can also block the retrieval of secret contents for a secret or secret version past the configured expiration date.

You might want to configure either or both of these secret rules to establish best practices around security. You can improve your security posture by acting on secrets that don’t adhere to the rules or, in the case of expiry rules, are in danger of violating them in due time.

Secrets are protected at rest with the encryption guarantees of a Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification-compliant hardware security module (HSM) that backs the vault where the secret is created and stored. However, while in application memory, a secret could be compromised. Preventing the reuse of secret contents by multiple secret versions serves to limit the scope of affected resources in the event of a security breach involving the stored credentials. When only one resource uses the secret contents of a secret version, that resource is the only one that can be impacted. You can deprecate a secret version and then delete it if you find out you can no longer safely use its secret contents. You can choose whether secret reuse rules apply even to deleted secret versions.

Similarly, configuring an expiry rule to specify a time range for how long a secret version can exist also helps limit the impact of a potential security breach. The longer that a set of credentials are used, the more time an attacker has to try to access or decipher them. Frequently updating a secret with new secret contents helps keep credentials safer from users with malicious intent. Or, it at least makes shorter the period of time during which compromised credentials can unknowingly be used or disseminated. You can configure a secret version to expire after 1 to 90 days, but the secret can also have an absolute expiration date and time ranging from 1 to 365 days after its creation date. You can configure either of these values or both. You can also decide whether the secret contents are blocked past the expiration date.

The timer for a secret’s expiry rule resets according to the configured interval. No mechanism exists to update the secret contents. You must rotate the secret version manually.

**Vault Metrics**

You can monitor the usage of your Vault service master encryption keys and secrets by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

This topic describes the metrics emitted by the Vault service in the `oci_kms_keys` and `oci_secrets` namespace.

Resources: master encryption keys and secrets.

**Overview of the Vault Service Metrics**

Vault service metrics help you measure the success and error count of cryptographic operations on keys and the success and error count of HTTP responses to get, create, and update (getSecretBundle, listSecretBundleVersions, createSecret, and updateSecret) operations during the selected time range. You can use metrics data to diagnose and troubleshoot problems with keys and secrets.

To view a default set of metrics charts in the Console, navigate to the key or secret that you're interested in, and then click Metrics. You also can use the Monitoring service to create custom queries.

**Prerequisites**

IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.
**Available Metrics: oci_kms_keys**

The metrics listed in the following table are automatically available for any master encryption keys that you create. You do not need to enable monitoring on the resource to get these metrics.

Vault service metrics for keys include the following dimensions:

**RESOURCEDISPLAYNAME**

The friendly name of the resource to which the metrics apply.

**RESOURCEID**

The OCID of the resource to which the metrics apply.

**RESPONSECODE**

The HTTP response code to the cryptographic operation to which the metrics apply.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EncryptResponseCount</td>
<td>Encrypt Response Count</td>
<td>count</td>
<td>HTTP responses received by the service for Encrypt calls.</td>
<td>resourceDisplayName, resourceId, responseCode</td>
</tr>
<tr>
<td>DecryptResponseCount</td>
<td>Decrypt Response Count</td>
<td>count</td>
<td>HTTP responses received by the service for Decrypt calls.</td>
<td></td>
</tr>
<tr>
<td>GenerateDataEncryptionKeyResponseCount</td>
<td>GenerateDataEncryptionKey Response Count</td>
<td>count</td>
<td>HTTP responses received by the service for GenerateDataEncryptionKey calls.</td>
<td></td>
</tr>
</tbody>
</table>

**Available Metrics: oci_secrets**

The metrics listed in the following table are automatically available for any secrets that you create. You do not need to enable monitoring on the resource to get these metrics.

Vault service metrics for secrets include the following dimensions:

**DISPLAYNAME**

The friendly name of the resource to which the metrics apply.

**RESOURCEID**

The OCID of the resource to which the metrics apply.

**RESPONSECODE**

The HTTP response code to the operation to which the metrics apply.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetSecretBundle</td>
<td>GetSecretBundle</td>
<td>count</td>
<td>HTTP responses received by the service for GetSecretBundle calls during the selected time range.</td>
<td>displayName, resourceId, responseCode</td>
</tr>
<tr>
<td>ListSecretBundleVersions</td>
<td>ListSecretBundleVersions</td>
<td>count</td>
<td>HTTP responses received by the service for ListSecretBundleVersions calls during the selected time range.</td>
<td></td>
</tr>
<tr>
<td>CreateSecret</td>
<td>CreateSecret</td>
<td>count</td>
<td>HTTP responses received by the service for CreateSecret calls during the selected time range.</td>
<td></td>
</tr>
<tr>
<td>UpdateSecret</td>
<td>UpdateSecret</td>
<td>count</td>
<td>HTTP responses received by the service for UpdateSecret calls during the selected time range.</td>
<td></td>
</tr>
</tbody>
</table>

**Using the Console**

To view default metric charts for a single master encryption key

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Click a vault to view the resources it contains.
3. Click a key name to view its details.
4. Under Resources, click Metrics.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.

To view default metric charts for multiple master encryption keys

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that contains the master encryption keys that you're interested in.
3. For Metric Namespace, select oci_kms_keys.

The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

**Tip:**

If there are multiple master encryption keys in the compartment, the charts default to show a separate line for each master encryption key. You can instead show a single line aggregated across all master encryption keys in the compartment by selecting the Aggregate Metric Streams check box.
To view default metric charts for a single secret

1. Open the navigation menu. Under the Governance and Administration group, go to Security and click Vault.
2. Click a vault to view the resources it contains.
3. Click Secrets.
4. Click a secret name to view its details.
5. Under Resources, click Metrics.

To view default metric charts for multiple secrets

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Service Metrics.
2. For Compartment, select the compartment that contains the secrets that you're interested in.
3. For Metric Namespace, select oci_secrets.

The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

Tip:

If there are multiple secrets in the compartment, the charts default to show a separate line for each secret. You can instead show a single line aggregated across all secrets in the compartment by selecting the Aggregate Metric Streams check box.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the following APIs for monitoring:

- Monitoring API for metrics and alarms
- Notifications API for notifications (used with alarms)

Troubleshooting the Vault Service

This section covers common issues related to the Vault service and how you can address them:

- Creating a Secret Fails Due to Authorization or Resource Not Found on page 4023
- Operation Fails Due to Conflicting Vault State on page 4024

Creating a Secret Fails Due to Authorization or Resource Not Found

There are several reasons why you might receive the following error when creating a secret, "Either you don't have permission to create this resource or the vault where you want to create it doesn't exist."

You might not have the required permissions. You need permissions for the vault where you want to create the secret and for the master encryption key that you want to use to encrypt the secret. If there's no policy that grants you the permissions you need, then an administrator must create one for you or add you to a group that's already named in a policy. If you're an administrator, refer to the following example policy:
- The policy Let security admins manage vaults, keys, and secrets lets the specified group do everything with vaults, keys, and secrets.

To write more restrictive policies, see Details for the Vault Service on page 2347. If you're new to policies, see Getting Started with Policies on page 2135 and Common Policies on page 2142.

It's possible that the vault doesn't exist. You can only create a secret in a vault that exists and only when you have permissions to do so.

**Operation Fails Due to Conflicting Vault State**

There are several reasons why an operation might result in the following error, "The state of the vault that contains this resource conflicts with the requested operation."

The vault lifecycle state shows that the vault is in a state that prevents the requested operation from proceeding or succeeding. This includes interstitial lifecycle states (for example, "Creating") or terminal states (for example, "Deleted"). Most operations are blocked when a vault is pending deletion.

The service might not recognize the same vault state as seen by a client application. This can happen, for example, if you recently changed the vault lifecycle state. The Vault service is eventually consistent regarding resource state. So, if this is the issue, you can try again later.
Chapter 40

VMware Solution

This chapter explains how to set up and manage software-defined data centers (SDDCs) in Oracle Cloud Infrastructure.

Oracle Cloud VMware Solution

Oracle Cloud VMware Solution allows you to create and manage VMware enabled software-defined data centers (SDDCs) in Oracle Cloud Infrastructure.

Solution Highlights

An Oracle Cloud VMware Solution gives you full access to the features of a VMware SDDC, along with the following benefits:

• High availability: All VMware components are distributed across different fault domains within the Oracle Cloud Infrastructure region’s availability domains. vSAN converged storage technology replicates data across all of the ESXi hosts in the SDDC.
• Scalability: You can start with 3 ESXi hosts and scale up to 64 hosts in a single SDDC.
• Lift and shift: Migration of on-premises VMware workloads to a Oracle Cloud VMware Solution is seamless.
• Full integration: Because the SDDC resides in a virtual cloud network (VCN), it can be configured to communicate with other Oracle Cloud Infrastructure resources such as Compute instances, DB systems and Autonomous Databases, and so on.
• Manageability: The Oracle Cloud Infrastructure Console provides workflows to facilitate SDDC creation and networking configuration.
• Layer 2 networking: SDDCs are configured with VLANs, which support applications that need layer 2 networking to run in the public cloud.

Note:

Bring your own hypervisor deployment of ESXi on bare metal Compute instances is not supported.

SDDC Details

An Oracle Cloud Infrastructure SDDC base configuration has the following properties:

• From 3 to 64 ESXi hosts on Oracle Cloud Infrastructure bare metal BM.DenseIO2.52 Compute instances
• 156 OPCUs, 2304 GB of physical memory, and 153 TB of NVMe-based raw storage
• A version of VMware software on each ESXi host
• An subnet and VLANs in an Oracle Cloud Infrastructure VCN

Supported Shapes

Currently, the only shape supported for ESXi hosts is a two-socket BM.DenseIO2.52 with two CPUs each running 26 cores. See Dense I/O Shapes on page 657 for more detail.
Oracle Cloud VMware Solution Architecture

The following diagram shows how the various components of the Oracle Cloud VMware Solution SDDC are deployed on Oracle Cloud Infrastructure bare metal Compute instances, and how the solution is integrated into the Oracle Cloud Infrastructure environment.

The diagram shows three ESXi hosts of an SDDC that resides in an Oracle Cloud Infrastructure VCN. The center host shows the installed VMware software components for compute (vSphere), network (NSX-T), and storage (vSAN) support. The NSX overlay manages the flow of traffic between the VMs, and between the VMs and the rest of the resources in the solution. The VCN here includes various gateways that allow connectivity between the SDDC and an on-premises network, the internet, and the Oracle Services Network.

When you provision an SDDC, you can enable HCX Manager (not shown in the diagram). HCX is an application mobility platform that simplifies application migration, workload rebalancing, and business continuity across data centers and clouds. For HCX to function properly in your VMware solution, you must have:

- A FastConnect connection for intersite communication
- A NAT gateway as required by HCX Manager for license activation, updates, and VMware enhanced support

**Note:**

HCX Manager requires connectivity to a VMware SaaS portal provided by a NAT gateway. Read more about VMware's requirements for HCX Manager: Why does HCX Manager require connectivity for activation and updates?

About the VMware Software

Oracle Cloud Infrastructure's VMware software bundle contains vSphere, vSAN, NSX, vCenter, and HCX components to support compute, storage, and network needs for a fully functional VMware environment.

- **vSphere:** vSphere is VMware's virtualization platform for unified management of the SDDC's CPU, storage, and networking infrastructure. Two key components of vSphere are ESXi hypervisor and vCenter Server.
- **NSX-T:** NSX-T Data Center provides the SDDC with its virtual networking and security capabilities. The NSX-T deployment includes NSX Manager unified appliances with NSX-T Local Manager and NSX-T Controller, and NSX-T Edge nodes.
- **vSAN:** Oracle Cloud VMware Solution SDDCs use VMware's vSAN storage technology, which provides a single shared datastore for compute and management workloads (VMs).
- **HCX:** The Hybrid Cloud Extension is an application mobility platform that removes complexity from application and workload migration. HCX is optionally installed as a plug-in when you set up your SDDC.
The following table shows the available versions of the software bundle, along with the version of each component:

<table>
<thead>
<tr>
<th>Software Version</th>
<th>vSphere</th>
<th>vSAN</th>
<th>NSX-T</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.7 update 3</td>
<td>6.7 U3</td>
<td>6.7 U3</td>
<td>2.5.1</td>
</tr>
<tr>
<td>6.5 update 3</td>
<td>6.5 U3</td>
<td>6.5 U3</td>
<td>2.5.1</td>
</tr>
</tbody>
</table>

When you provision the SDDC, you select the version of this software bundle to install on the ESXi hosts. You can change the SDDC’s software version later. When you add ESXi hosts to the SDDC, the version of software installed on new hosts is the version currently associated with the SDDC.

**Note:**

Changes that you make to the SDDC by using the Oracle Cloud Infrastructure Console, API, or CLI are not automatically made in vCenter. For example, if you change the software version or the SSH keys, the change applies only to ESXi hosts that you add to the SDDC. To change these properties for existing hosts, you must make the applicable updates in vCenter manually.

**Working with SDDCs**

You use the Oracle Cloud Infrastructure Console, API, or CLI to provision and manage SDDC resources. You use VMware’s vCenter utility to create and manage workloads in the SDDC.

See the following topics for information and instructions on how to create and manage Oracle Cloud VMware Solution resources:

- Setting Up an Oracle Cloud VMware Solution SDDC on page 4029
- Managing Oracle Cloud VMware Solution SDDCs on page 4035
- Configuring Networking Connectivity for an SDDC on page 4032
- Managing Layer 2 Networking Resources for an SDDC on page 4038

**Additional Documentation Resources**

The following Oracle Cloud VMware Solution solution playbooks and white papers are available:

- Deploy Zerto to protect your VMware SDDC in the cloud against disasters
  Learn how to deploy Zerto to protect your Oracle Cloud VMware SDDC data in the cloud.
- Deploy Veeam to protect your VMware SDDC in the cloud against disasters
  Learn how to deploy Veeam to protect your Oracle Cloud VMware SDDC data in the cloud.
- Deploy Actifio to protect your VMware SDDC in the cloud against disasters
  Learn how you can configure Actifio backup and disaster recovery solution for guest VMs in Oracle Cloud VMware Solution.
- Deploy a highly available SDDC to the cloud
  Shows you how to deploy a VMware SDDC on Oracle Cloud Infrastructure and then integrate it with other Oracle services running on Oracle Cloud.
- Migrate your on-premises VMware workloads to the cloud
  Outlines the process of online, or live, migration of your VMware workloads from an on-premises data center environment to Oracle Cloud VMware Solution.
- Build a hybrid SDDC by extending your on-premises VMware deployment to Oracle Cloud
  Describes how to set up a hybrid VMware SDDC between your on-premises environment and Oracle Cloud Infrastructure by using Oracle Cloud VMware Solution.
• Learn about connecting to Oracle Cloud and VMware resources
  Describes several methods for connecting to your Oracle Cloud and VMware resources, plus their benefits, limitations, and how to get started.

• Implement disaster recovery for an Oracle Cloud VMware Solution SDDC on the cloud
  Describes how Oracle Cloud VMware Solution uses VMware Site Recovery Manager (SRM) to implement an automated, reliable, and flexible disaster recovery solution for your VMware SDDC.

• Deploy a multitier application stack on a VMware SDDC connected to an autonomous database
  Shows a 3-tier application stack in Oracle Cloud Infrastructure with the application tier deployed in a VMware SDDC that's created by using Oracle Cloud VMware Solution.

Setting Up an Oracle Cloud VMware Solution SDDC

This topic includes information and instructions for provisioning a software-defined data center (SDDC) by using the Oracle Cloud Infrastructure Console or the API.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

Prerequisites

• An existing VCN with an IP address CIDR size of /22 or larger available for running the SDDC.
• We recommend that you set up connectivity between the VCN and your on-premises network before provisioning your SDDC. See Access to Your On-Premises Network on page 3252.
• If you do not plan to use the workflow to create an SDDC, ensure that you configure the SDDC's networking resources with the security rules detailed in Security Rules for Oracle Cloud VMware Solution SDDCs on page 4043. Otherwise, provisioning the SDDC will fail.

If you do not yet have a VCN for your SDDC, you can quickly create one and set up an IPSec VPN between your on-premises network and the VCN by using the VPN Connect workflow. See VPN Connect Quickstart on page 2939 to learn how.

Using the Console

The Create SDDC workflow can create the required networking resources for you (recommended), or you can create them yourself and then select them in the workflow. If you plan to select existing networking resources for your SDDC, ensure that you create them before you start the workflow. The following networking resources are required:

• A provisioning subnet with a route table and a security list - See To create a subnet on page 2825.
• VLANs - See Managing Layer 2 Networking Resources for an SDDC on page 4038.

To create an SDDC

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click Create SDDC.
3. Provide basic information for the SDDC:

   • SDDC Name: A descriptive name for the SDDC. This name must be unique among all SDDCs in the creating, active, or updating state across all compartments in the region. Avoid entering confidential information.

   **Note:**

   Unlike most display names in the Oracle Cloud Infrastructure Console, this name has the following additional requirements because it is used by vCenter to build URLs:
• It must be from 1-16 characters long and must start with a letter
• It can contain only alphanumeric characters and hyphens (-), and hyphens cannot be next to each other
This name is not case sensitive. For example, "test" and "Test" are treated as the same name.

• **SDDC Compartment**: The compartment in which to create the SDDC. All ESXi hosts for this SDDC will be placed in this compartment.

• **Enable HCX**: Select this checkbox to have the workflow install the HCX Manager plugin and integrate it with vCenter in the SDDC. *You cannot install this plugin later.*

• **VMware Software Version**: The version of VMware software to install on the ESXi hosts. While the VMware software bundle includes vSphere, vSAN, NSX, and vCenter components, the version you specify here is the version of vSphere. Compatible versions of the other components are installed with the version of vSphere you select. See *About the VMware Software* on page 4027 for details about the vSAN, NSX, or vCenter component versions installed. You can change this software version after provisioning.

• **Number of ESXi Hosts**: The initial number of ESXi hosts to create. Specify at least 3 and at most 64 hosts.

• **Prefix for ESXi Hosts**: (Optional) You can enter a prefix to use for the names of the ESXi hosts to help identify them. This string has the same criteria as the SDDC name. It must be from 1-16 characters long, must start with a letter, and can contain only alphanumeric characters and hyphens (-). Avoid entering confidential information.

• **SSH Key**: Provide the public key portion of the SSH key. This key is required for remote connections to the ESXi hosts.

• **Availability Domain**: The availability domain in which to create the SDDC. ESXi hosts in the SDDC are distributed across the fault domains in the availability domain to ensure high availability. The management subnet and VLANs for this SDDC must be in this same availability domain.

If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see *Resource Tags* on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. To see the tagging options, click *Show Advanced Options*. The tags you specify are applied to all of the resources in the SDDC.

4. After you complete the Basic Information page, click **Next** to advance to the SDDC Networks page.

5. Choose a VCN for the SDDC. The VCN can be in a different compartment than the SDDC and its ESXi hosts.

6. If you enabled HCX in step 3, the selected VCN must have a NAT gateway attached to it.

   • If a NAT gateway already exists for the VCN, the name, compartment, and public IP address information is displayed.

   • If there is no NAT gateway attached to the selected VCN, the workflow creates one for you. Enter a name and select a compartment for the NAT gateway.

7. Select whether the workflow should create the network resources for this SDDC (recommended) or use existing network resources that you specify.

**To have the workflow create the network resources:**

   a. Click **Create New Subnet and VLANs**.

   b. Enter an available CIDR block in your selected VCN for the SDDC management CIDR. The workflow divides this CIDR into eight equal segments to use for the provisioning subnet and the seven required VLANs. If you are enabling HCX, the segment for the vSphere VLAN is further divided into two equal segments, one for
vSphere and the other for HCX. The size must be at least /22 to allow the maximum of 64 ESXi hosts to each have their own IP address.

c. Click **Check Availability** to ensure that CIDR block is available in the selected VCN. The check scans all subnets and VLANs in all compartments of the VCN.

You can show or hide details for the subnet and VLANs the workflow will create. Details include the route table and security list for the subnet, and the route table and NSG for each VLAN.

If you have enabled HCX, an additional route rule is created to allow traffic from the vSphere VLAN to the NAT gateway.

**To use existing network resources:**

a. Click **Select Existing Subnet and VLANs**.

b. Choose the compartment and provisioning subnet for your SDDC's management network. You cannot change the subnet after provisioning.

The CIDR value shown is the private address space for your chosen subnet.

c. Choose the compartment and VLAN for each function of your SDDC's management network.

The VLAN Gateway CIDRs shown are the CIDR blocks from which to derive IP addresses for each VLAN's layer 3 traffic. These CIDR blocks also provide the private IP addresses Oracle uses as attachment objects for public IP addresses when ESXi hosts require internet access.

- **NSX Edge Uplink 1:** Uplink used for communication between the VMware SDDC and Oracle Cloud Infrastructure.
- **NSX Edge Uplink 2:** Reserved for future use to deploy public-facing applications on the VMware SDDC.
- **NSX Edge VTEP:** Used for data plane traffic between the ESXi host and NSX Edge.
- **NSX VTEP:** Used for data plane traffic between ESXi hosts.
- **vMotion:** Used for vMotion (VMware migration tool) management and workload.
- **vSAN:** Used for vSAN (VMware storage) data traffic.
- **vSphere:** Used for management of the SDDC components (ESXi, vCenter, NSX-T, and NSX Edge).

**Note:**

If you checked the **Enable HCX** checkbox, verify that the VLAN selected for **vSphere** contains a route table rule that allows traffic to the NAT gateway. See **Managing Layer 2 Networking Resources for an SDDC** on page 4038 for more information.

- **HCX:** Used for HCX traffic. This VLAN appears only if you checked the **Enable HCX** checkbox.

8. (Optional) Provide an SDDC workload CIDR block for the workflow to create an initial logical segment for your VMs. The value must be /30 or larger and must not overlap with the VCN or the SDDC network CIDRs. Note that you can add network segments for the SDDC in NSX Manager after the SDDC is provisioned.

9. Click **Next** to review the summary of settings for creating the SDDC.

If you need to make changes, click **Edit Basic Information** or **Edit SDDC Networks** to return to a page, and update the settings, as applicable.

10. When you are satisfied with the summary information, click **Create SDDC**.

The page shows the provisioning status of each resource.

When provisioning is complete, the SDDC’s details page includes a username and an initial password that lets you access the vCenter management utility for the SDDC.

**Note:**

The password value displayed in the Oracle Cloud Infrastructure Console is not updated with your current password after you change it.
11. (Optional) You can check the status of provisioning by viewing its work request item from the SDDC's details page, under Resources.

    Provisioning takes approximately two and a half hours to complete.

    If errors occur, you can click Retry Provisioning. Clicking Cancel Provisioning cancels the provisioning process and deletes all resources created for the SDDC.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

Use the CreateSddc API to create a VMware solution.

Use these API operations to create networking infrastructure resources for your VMware solution:

- CreateSubnet
- CreateRouteTable
- CreateSecurityList
- CreateNetworkSecurityGroup
- CreateVlan

What's Next?

After you provisioning your SDDC, you might want to perform some of the following tasks:

- Configure network connectivity between the SDDC and resources in your on-premises network, the Oracle Services Network, the internet throught a NAT gateway, or other resources in the VCN. See Configuring Networking Connectivity for an SDDC on page 4032 for information and instructions.

- Modify resources or properties of your SDDC. For example, add ESXi hosts. See Managing Oracle Cloud VMware Solution SDDCs on page 4035.

- Create VMs in your SDDC or perform other VMware tasks. To do so, you can log into vCenter by using the vSphere Client link from the detail page of the SDDC.

Configuring Networking Connectivity for an SDDC

This topic covers configuring network connectivity for an Software-Defined Data Center (SDDC) by using quick action workflows in the Oracle Cloud Infrastructure Console.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don’t have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

About the SDDC Workflows

The SDDC quick action workflows make it easy for you to configure connectivity between your SDDC and various network resources within and outside of the VCN. Each workflow determines whether the required networking resources for connectivity already exist, and attempts to create or update them as needed. These networking resources can include gateways, subnets, route tables, rules, and network security groups. To use a workflow successfully, you must have the proper permissions for using and managing the applicable resources. See Details for the Core Services on page 2181 for information about networking resource permissions. Resource creation also relies on your limits and remaining capacity to create more resources.

Configuring Connectivity to Your On-premises Network

The workflow for configuring connectivity between your SDDC and an on-premises network does the following:
VMware Solution

- Determines whether the VCN has an attached dynamic routing gateway (DRG), and if not, helps you create one.
- Adds the route table, rules, or network security groups needed to enable routing between the DRG and the SDDC’s NSX Edge Uplink 1 VLAN.

The permissions required to run the workflow successfully depend on the resources the workflow needs to create or update. Before you begin, ensure you have the correct permissions to use and manage these resources.

**Note:**

- In the workflow, you are prompted for the CIDR of the on-premises network. If you do not know this value, check with the on-premises network engineer or administrator before you begin. This CIDR value cannot be the same as the SDDC workload CIDR, and cannot overlap with the VCN’s CIDR.
- The workflow adds required route rules and security rules to the VCN resources. If you have reached your limits, you are prompted to check your existing rules and delete some to free up capacity.

**To configure connectivity between the SDDC and your on-premises network**

1. On the Details page of the SDDC, click **Configure connectivity to your on-premises network**.
2. Use the Networking wizard to set up the DRG, if needed. After the DRG setup is complete, you can continue with the workflow.
3. Enter the SDDC workload CIDR. This CIDR block provides the IP addresses the VMware VMs use to run workloads. The minimum size is /30.
4. Enter the CIDR of the on-premises network.
5. Review the details of the planned updates to your networking resources. The workflow creates or updates route tables and rules that impact the NSX Edge Uplink 1 VLAN and the DRG.

   If you choose to disallow an update, your SDDC might not have connectivity to your on-premises network. To complete the configuration, you can either return to the workflow later or make the required resource update manually outside of the workflow.

   If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. To see the tagging options, click **Show Advanced Options**. The tags you specify are applied to all of the new resources created in this workflow.

6. When you are satisfied with the configuration settings, click **Apply Configuration**.

   The Console displays the status of each operation in the workflow. In an error occurs, you can retry the operation. When you close the Applying Configuration window, you return to the SDDC Details page, which shows a summary of the resources that were updated and allows you to view each one by clicking the applicable link.

**Configuring Connectivity to the Oracle Services Network**

The workflow for configuring connectivity between your SDDC and the Oracle Services Network does the following:

- Determines whether the VCN has a service gateway, and if not, helps you create one.
- Adds the route table, rules, or network security groups needed to enable routing between the SDDC’s NSX Edge Uplink 1 VLAN and the service gateway.

The permissions required to run the workflow successfully depend on the resources the workflow needs to create or update. Before you begin, ensure you have the correct permissions to use and manage these resources.

**Note:**

The workflow adds required route rules and security rules to the VCN resources. If you have reached your limits, you are prompted to check your existing rules and delete some to free up capacity.
To configure connectivity between the SDDC and Oracle Services Network

1. On the Details page of the SDDC, click **Configure connectivity to Oracle Services Network**.
2. Enter the SDDC workload CIDR. This CIDR block provides the IP addresses the VMware VMs use to run workloads. The minimum size is /30.
3. Click **Next**.
4. Review the details of the planned updates to your networking resources. The workflow creates or updates route tables and rules that impact the NSX Edge Uplink1 VLAN and the service gateway.

   If you choose to disallow an update, your SDDC might not have connectivity to Oracle Services Network. To complete the configuration, you can either return to the workflow later or make the required resource update manually outside of the workflow.

   If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. To see the tagging options, click **Show Advanced Options**. The tags you specify are applied to all of the new resources created in this workflow.

5. When you are satisfied with the configuration settings, click **Apply Configuration**.

   The Console displays the status of each operation in the workflow. In an error occurs, you can retry the operation. When you close the Applying Configuration window, you return to the SDDC Details page, which shows a summary of the resources that were updated and allows you to view each one by clicking the applicable link.

Configuring Connectivity to the Internet Through a NAT Gateway

The workflow for configuring connectivity between your SDDC and the internet through a NAT gateway does the following:

- Determines whether the VCN has a NAT gateway, and if not, helps you create one.
- Adds a default route rule to the SDDC's NSX Edge Uplink1 VLAN's route table to send traffic to the internet through the NAT gateway.

The permissions required to run the workflow successfully depend on the resources the workflow needs to create or update. Before you begin, ensure you have the correct permissions to use and manage these resources.

**Note:**

The workflow adds a required route rule to the VLAN's route table. If you have reached your route rule limits, you are prompted to check your existing rules and delete one to free up capacity.

To configure connectivity to the internet through a NAT gateway

1. On the Details page of the SDDC, click **Configure connectivity to the internet through NAT gateway**.
2. Review the details of the planned updates to your networking resources.

   If you choose to disallow an update, your SDDC might not have internet connectivity through the NAT gateway. To complete the configuration, you can either return to the workflow later or make the required resource update manually outside of the workflow.

   If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. To see the tagging options, click **Show Advanced Options**. The tags you specify are applied to all of the new resources created in this workflow.

3. When you are satisfied with the configuration settings, click **Apply Configuration**.

   The Console displays the status of each operation in the workflow. In an error occurs, you can retry the operation. When you close the Applying Configuration window, you return to the SDDC Details page, which shows a summary of the resources that were updated and allows you to view each one by clicking the applicable link.
Configuring Connectivity to Other Resources in the VCN

The workflow for configuring connectivity between your SDDC and other resources in the VCN does the following:

- Allows you to select subnets in the VCN that contain resources you want your SDDC to connect to. If the VCN has no subnets, you can use the Networking Wizard from the workflow to create them.
- Adds the route table, rules, or network security groups needed to enable routing between the SDDC's NSX Edge Uplink 1 VLAN and the resources in the selected subnets.

The permissions required to run the workflow successfully depend on the resources the workflow needs to create or update. Before you begin, ensure you have the correct permissions to use and manage these resources.

**Note:**
The workflow adds required route rules and security rules to the VCN resources. If you have reached your limits, you are prompted to check your existing rules and delete some to free up capacity.

To configure connectivity between the SDDC and other resources in the VCN

1. On the Details page of the SDDC, click **Configure connectivity to VCN resources**.
2. Enter the SDDC workload CIDR. This CIDR block provides the IP addresses the VMware VMs use to run workloads. The minimum size is /30.
3. Click **Select Subnets**.
4. Check the check boxes of the subnets that contain resources your SDDC needs to connect to. You filter and sort the list to help you find the subnets you're interested in.
5. Click **Save Selection**.
6. Click **Next**.
7. Review the details of the planned updates to your networking resources. The workflow creates or updates route tables and rules that impact the NSX Edge Uplink1 VLAN and the selected subnets.
   
   If you choose to disallow an update, your SDDC might not have connectivity to the resources in a subnet. To complete the configuration, you can either return to the workflow later or make the required resource update manually outside of the workflow.
   
   If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. To see the tagging options, click **Show Advanced Options**. The tags you specify are applied to all of the new resources created in this workflow.
8. When you are satisfied with the configuration settings, click **Apply Configuration**.

   The Console displays the status of each operation in the workflow. In an error occurs, you can retry the operation. When you close the Applying Configuration window, you return to the SDDC Details page, which shows a summary of the resources that were updated and allows you to view each one by clicking the applicable link.

Managing Oracle Cloud VMware Solution SDDCs

This topic describes how to manage your Oracle Cloud VMware solution software-defined data center (SDDC) resources by using the Oracle Cloud Infrastructure Console or API. SDDC resources include SDDCs and ESXi hosts. To create and manage VMs on the ESXi hosts, you use VMware's vCenter utility.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be granted security access in a **policy** by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which **compartments** you should work in.
Using the Console

The procedures that follow include steps for managing SDDCs and ESXi hosts.

To update basic properties of an SDDC

You can modify basic properties of the SDDC, including the name, the VMware software version, and the SSH keys.

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. Click Edit SDDC.
4. Make the applicable changes:
   - **SDDC Name**: Enter a new name for SDDC. This name must be unique among all SDDCs in the creating, active, or updating state across all compartments in the region. Avoid entering confidential information.
     
     **Note:**
     Unlike most display names in the Oracle Cloud Infrastructure Console, this name has the following additional requirements because it is used by vCenter to build URLs:
     - It must be from 1-16 characters long and must start with a letter
     - It can contain only alphanumeric characters and hyphens (-), and hyphens cannot be next to each other
     This name is not case sensitive. For example, "test" and "Test" are treated as the same name.
   - **VMware Software Version**: Select the version of VMware software to install on new ESXi hosts. While the VMware software bundle includes vSphere, vSAN, NSX, and vCenter components, the new version you specify here is the vSphere version only. The update does not impact the versions of the vSAN, NSX, or vCenter components.
   - **SSH Key**: Provide the public key portion of the SSH key. This key is required for remote connections to the ESXi hosts.

5. (Recommended) Click the vSphere Client link to go to vCenter, and make the appropriate updates for the SDDC properties you changed in the Console. You can do this task now or after you save your changes.
6. Click Save Changes.

To add an ESXi host to an SDDC

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. Click Create ESXi Host.
4. (Optional) Enter a name for the new host that helps to identify it later. The name must be from 1-16 characters long, must start with a letter, and can contain only alphanumeric characters and hyphens (-). Hyphens cannot be next to each other. Avoid entering confidential information.
5. (Optional) Show the ESXi host details to view or modify the following host properties:
   - VMware software version
   - SSH key
   - VLANs
6. When you are satisfied with the properties for this host, click Create ESXi Host.
To rename an ESXi host

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. In the list of ESXi hosts, click the Actions icon (three dots) for the host you want to rename, and then click Rename.
4. Enter the new name for the host. The name must be from 1-16 characters long, must start with a letter, and can contain only alphanumeric characters and hyphens (-). Hyphens must not be next to each other. Ensure that the name is unique within the SDDC. Avoid entering confidential information.
5. Click Rename.

To remove ESXi hosts from an SDDC

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. In the list of ESXi hosts, click the Actions icon (three dots) for the host you want to remove, and then click Terminate ESXi Host.

To change VLANs the SDDC uses

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. Under Resources, click SDDC Networks.
4. On the VLANs tab, click Change VLANs.
5. Make the applicable changes. See VLANs Required for an SDDC on page 4038 for information about VLANs.

Note:

Changes that you make to the SDDC's VLAN assignments by using the Oracle Cloud Infrastructure Console, API, or CLI are not automatically made in vCenter. You must make these updates in vCenter manually.

6. Click Save Changes.

To move an SDDC to a different compartment

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. Click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.

To terminate an SDDC

SDDC termination automatically removes the SDDC's associated instances and boot volumes. With a failed SDDC, you can opt to also delete all of its associated networking resources. These resources include the subnet and its route table and security list, and the VLANs and their route tables and NSGs. A networking resource cannot be deleted if that resource is used by another SDDC or networking resource. A networking resource in use will remain after the SDDC is terminated.

1. Open the navigation menu. Under Solutions and Platform, click VMware Solution.
2. Click the name of the SDDC to view details about it.
3. Click Terminate.

   Termination removes the SDDC and its associated resources. Terminated resources cannot be restored.

4. Follow the prompt to confirm termination, and click Terminate All.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.
Use these API operations to manage VMware solution resources:

- ListSddcs
- GetSddc
- UpdateSddc
- ChangeSddcCompartment
- DeleteSddc
- ListEsxiHosts
- GetEsxiHost
- CreateEsxiHost
- UpdateEsxiHost
- DeleteEsxiHost

Managing Layer 2 Networking Resources for an SDDC

This topic describes how to manage layer 2 networking resources for a software-defined data center (SDDC) by using the Oracle Cloud Infrastructure Console or the API.

About SDDC Layer 2 Networking Resources

An Oracle Cloud Infrastructure SDDC requires a management subnet and layer 2 networking resources. The layer 2 networking resources include seven VLANs and their configured external access objects.

When you provision an SDDC by using the Oracle Cloud Infrastructure Console's Create SDDC workflow, you can have the workflow create these required networking resources for you. We recommend that you select this option. If you prefer, you can create them yourself before you start the Create SDDC workflow, and then select the existing subnet and VLANs you created for this purpose. If you create the SDDC using an existing subnet and VLANs, Oracle recommends that you create a size /22 CIDR network segment in your VCN for the SDDC’s networking resources. The documentation and the console refer to this segment as the “SDDC CIDR.” Divide this SDDC CIDR into eight segments of size /25 to use for the subnet and the seven required VLANs indicated in this topic. In addition, you must configure the security rules for these networking resources as detailed in Security Rules for Oracle Cloud VMware Solution SDDCs on page 4043. Otherwise, provisioning the SDDC will fail.

Note:
You can update VCN, VLAN, and subnet CIDR block information after creation. Ensure that any changes you make to the VCN after the SDDC is provisioned follow the preceding requirements.

For more information about editing your VCN, see VCNs and Subnets on page 2821.

VLANs Required for an SDDC

An SDDC requires VLANs for the following functions:

- **NSX Edge Uplink 1:** Uplink used for communication between the VMware SDDC and Oracle Cloud Infrastructure.
- **NSX Edge Uplink 2:** Reserved for future use to deploy public-facing applications on the VMware SDDC.
- **NSX Edge VTEP:** Used for data plane traffic between the ESXi host and NSX Edge.
- **NSX VTEP:** Used for data plane traffic between ESXi hosts.
- **vMotion:** Used for vMotion (VMware migration tool) management and workload.
- **vSAN:** Used for vSAN (VMware storage) data traffic.
- **vSphere:** Used for management of the SDDC components (ESXi, vCenter, NSX-T, and NSX Edge).
• **HCX: (Optional)** Used for HCX traffic. Create this VLAN if you plan to enable HCX when you provision the SDDC.

**Note:**

If you allow the Create SDDC workflow to create the VLANs, the workflow divides the SDDC management CIDR you specify into eight equal segments to use for the provisioning subnet and the seven required VLANs. If you enable HCX, the workflow further divides the vSphere segment into two equal parts, one for the vSphere VLAN and the other for the HCX VLAN. You can follow this model if you choose to create your VLANs manually.

HCX also requires that the vSphere VLAN has a route table rule that allows traffic to a NAT gateway attached to the VCN. See Route Tables on page 2921 for more information.

These VLANs must all be in the same VCN and availability domain you specify when you create the SDDC, but they can be in different compartments.

**External Access to VLAN Resources**

You can enable external access to an SDDC's ESXi hosts by creating a private IP object for the VLAN that can be used as a route target. Additionally, you can enable internet access to hosts in the VLAN by assigning a public IP address to the VLAN's private IP address object. When you configure external access, you have the option to indicate that it be accessible as a route target only and, as such, have no associated public IP address. See To add external access to a VLAN on page 4040 for the steps to configure external access.

**Required IAM Policy**

To use Oracle Cloud Infrastructure, you must be granted security access in a policy by an administrator. This access is required whether you're using the Console or the REST API with an SDK, CLI, or other tool. If you get a message that you don't have permission or are unauthorized, verify with your administrator what type of access you have and which compartment you should work in.

**Using the Console**

Use the procedures that follow to create and manage VLANs and external access objects for your SDDCs.

**To create a VLAN for an SDDC**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Choose a compartment you have permission to work in (on the left side of the page). The page updates to display only the resources in that compartment. If you're not sure which compartment to use, contact an administrator. For more information, see Access Control on page 2831.
3. Click the VCN in which you plan to provision your SDDC.
4. Under Resources, click VLANs.
5. Click Create VLAN.
6. Enter the following:

- **Name:** (Optional) A descriptive name for the VLAN. It doesn't have to be unique, and you can change it later. Avoid entering confidential information.

- **Create in Compartment:** The compartment for the VLAN.

- **Availability Domain:** Select the availability domain you plan select when you provision the SDDC. The ESXi hosts must be in the same availability domain as the SDDC's VLANs.

- **IEEE 802.1Q VLAN Tag:** (Optional) The VLAN uses this unique value to identify a broadcast domain for layer 2 traffic. Enter a number from 1 to 4094. If you don't enter a value, Oracle assigns one. You cannot change this value later.

- **VLAN Gateway CIDR:** This CIDR provides IP addresses used by the VLAN for external layer 3 communication and routing. This CIDR block also provides the private IP addresses Oracle uses as attachment objects for public IP addresses when instances require access to internet hosts. You can't change this value later.

  - **Note:**
    This CIDR must be within the VCN's CIDR and cannot overlap with the CIDRs of the other subnets and VLANs in the VCN.

- **Route Table:** The route table contains rules that specify the next hop for traffic from the VLAN to external destinations.

- **Network Security Groups:** Select the NSGs with the security rules to apply to all VNICs in this VLAN. You can select up to 5 NSGs for a VLAN.

  You manage NSG membership for VNICs in a VLAN at the VLAN level. You cannot add or remove individual VNICs in a VLAN from an NSG.

If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. If you don't see the tagging option, click **Show Advanced Options**.

7. Click **Create VLAN**.

The new VLAN displays in the list of VLANs for the VCN in the selected compartment.

8. Repeat steps 5 through 7 for each VLAN you need for your SDDC. See **VLANs Required for an SDDC** on page 4038.

**To add external access to a VLAN**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.

2. Click the VCN that contains the VLAN you want to modify.

   If you do not see the VCN listed, ensure that you have the correct compartment selected.

3. Under **Resources**, click **VLANs**.

4. Click the name of the VLAN to view details about it.

5. Click **Add External Access**.
6. Specify the type of external access to configure.

**Route Target Only**: Select this option to assign a private IP address only for use as a route target for traffic that needs to reach the VMware overlay. The IP address must be within VLAN gateway CIDR block. If you do not specify a name or a private IP address, or both, Oracle generates the needed values for you.

**Public Access**: Select this option to also provide a public IP address for internet access to the resources such as VNICs and VMs in the VLAN. The public IP address must be attached to a private IP address to enable internet access.

- **Private IP Address**: (Optional) Specify a name and/or a private IP address within the VLAN gateway CIDR block. If you do not specify these values, Oracle generates them for you. Note that as with the route target only option, this private IP address can also be used as a route target for non-internet traffic.
- **Reserved Public IP Address**: (For public access only) Choose whether to specify an existing reserved public IP address or have a new one created for this external access.

If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator. To see the tagging options, click Show Advanced Options.

7. Click Add External Access.

**To modify external access to a VLAN**

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN that contains the VLAN you want to modify.
   If you do not see the VCN listed, ensure that you have the correct compartment selected.
3. Under Resources, click VLANs.
4. Click the name of the VLAN to view details about it.
5. In the External Access list, select the external access you want to modify, click the Actions icon (three dots), and then click the Edit.

   The settings you can modify depend on the external access type. Consider the following:

   - You can change the external access type from route target only to public access, or the other way around.

     If you change the type from public access to route target only, the private IP address will no longer have an associated reserved IP address. Therefore, any host that uses the private IP address will not be accessible from the internet.

     If you change the type from route target only to public access, you'll need to attach a reserved public IP address to it to enable access from the internet. You can select an existing public IP address or have a new one created for this purpose.

     For both route target only and public access types, you can rename the private IP address but you cannot change the IP address value itself.

     For a public access type, you can rename the reserved public IP address but you cannot change the IP address value itself.

6. When you are done making your updates, click Save Changes.

**To remove external access to a VLAN**

<table>
<thead>
<tr>
<th><strong>Important:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If an existing route rule targets the private IP address associated with the external access you are removing, the route rule will drop traffic to that private IP address.</td>
</tr>
</tbody>
</table>

1. Open the navigation menu. Under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
2. Click the VCN that contains the VLAN you want to modify.
   If you do not see the VCN listed, ensure that you have the correct compartment selected.
3. Under **Resources**, click **VLANs**.
4. Click the name of the VLAN to view details about it.
5. In the External Access list, select the external access you want to remove, and click **Remove**.
6. Click **Remove** to complete the action.

**To move a VLAN to a different compartment**
1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN that contains the VLAN you want to move.
   
   If you do not see the VCN listed, ensure that you have the correct compartment selected.
3. Under **Resources**, click **VLANs**.
4. Click the name of the VLAN to view details about it.
5. Click **Move Resource**.
6. Choose the destination compartment from the list.
7. Click **Move Resource**.

**To modify basic properties of a VLAN**
You can rename a VLAN, or change its route table or network security groups.

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN that contains the VLAN you want to modify.
   
   If you do not see the VCN listed, ensure that you have the correct compartment selected.
3. Under **Resources**, click **VLANs**.
4. Click the name of the VLAN to view details about it.
5. Click **Edit**.
6. Change the applicable settings:
   
   - **VLAN Name**: Use a descriptive name that helps to identify the VLAN. The name doesn't have to be unique. Avoid entering confidential information.
   - **Route Table**: The route table provides mapping for traffic from the VLAN to external destinations.
     
     (To select a route table in a different compartment, click Change Compartment, and select the compartment the target route table is in.)
   - **Network Security Groups**: Select the NSGs with the security rules to apply to all VNICs in this VLAN. You can select up to 5 NSGs for a VLAN.
7. When you are done making changes, click **Save Changes**.

**To modify the network security groups of a VLAN**

1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN that contains the VLAN you want to modify.
   
   If you do not see the VCN listed, ensure that you have the correct compartment selected.
3. Under **Resources**, click **VLANs**.
4. Click the name of the VLAN to view details about it.
5. Next to **Network Security Groups**, click **Edit**.
6. Make the applicable changes to the list of security groups. The VLAN can be associated with up to 5 security groups.
7. Click **Save Changes**.

**To delete a VLAN**

**Note:**

You cannot delete a VLAN if it has any external access resources. You must first remove all external access. See **To remove external access to a VLAN** on page 4041.
1. Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.
2. Click the VCN that contains the VLAN you want to delete.
   - If you do not see the VCN listed, ensure that you have the correct compartment selected.
3. Under **Resources**, click **VLANs**.
4. Click the name of the VLAN to view details about it.
5. Click **Delete**.

**Using the API**

For information about using the API and signing requests, see **REST APIs** on page 4368 and **Security Credentials** on page 179. For information about SDKs, see **Software Development Kits and Command Line Interface** on page 4225.

Use these API operations to create and manage layer 2 networking resources for an Oracle Cloud VMware solution SDDC:

- GetVlan
- ListVlans
- CreateVlan
- UpdateVlan
- ChangeVlanCompartment
- DeleteVlan

For a list of API operations to create and manage networking resources used by the VLANs in an SDDC, see the following topics:

- Route tables
- NSGs
- Private IPs

**Security Rules for Oracle Cloud VMware Solution SDDCs**

This topic details the security rules the Console's Create SDDC workflow configures for the new SDDC's subnet and VLANs. The rules are based on the requirements set by VMware.

**Important:**

If you do not use the workflow to create an SDDC, ensure that you configure the SDDC's networking resources with these security rules. Otherwise, provisioning the SDDC will fail.

**Provisioning Subnet**

The security lists for the provisioning subnet have the following stateful ingress security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
<td>Allow SSH traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>ICMP</td>
<td>All</td>
<td>Type and Code: All</td>
<td>Allow ICMP traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>80</td>
<td>Allow HTTP traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
<td>Allow HTTPS traffic</td>
</tr>
</tbody>
</table>
### Ingress
<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>902</td>
<td>Allow vCenter Server agent to manage ESXi host</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>902</td>
<td>Allow vCenter Server agent to manage ESXi host</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>903</td>
<td>Allow vCenter Server agent to manage ESXi host</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>53</td>
<td>Allow DNS traffic</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>53</td>
<td>Allow DNS traffic</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>27010</td>
<td>Allow VMware license server traffic</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>27000</td>
<td>Allow VMware license server traffic</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>123</td>
<td>Allow NTP time server traffic</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>3260</td>
<td>Allow iSCSI traffic</td>
</tr>
<tr>
<td><strong>Ingress</strong></td>
<td>SDDC CIDR</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process</td>
</tr>
</tbody>
</table>

**Oracle Cloud Infrastructure User Guide**
<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td></td>
<td>Type and Code: 3,4</td>
<td>ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set</td>
</tr>
<tr>
<td>Ingress</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td></td>
<td>Type and Code: 3</td>
<td>ICMP traffic for: 3 Destination Unreachable</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process communication</td>
</tr>
</tbody>
</table>

**NSX Edge Uplink 2 VLAN**

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
<td>Allow SSH traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td></td>
<td>Type and Code: 3,4</td>
<td>ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set</td>
</tr>
<tr>
<td>Ingress</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td></td>
<td>Type and Code: 3</td>
<td>ICMP traffic for: 3 Destination Unreachable</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process communication</td>
</tr>
</tbody>
</table>

**NSX Edge VTEP VLAN**

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
</tbody>
</table>
### NSX VTEP VLAN

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>6081</td>
<td>Allow traffic for GENEVE Termination End Point (TEP) Transport N/W</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>3784-3785</td>
<td>Allow traffic for BFD Session between TEPs</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process communication</td>
</tr>
</tbody>
</table>

### vMotion VLAN

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
<td>Allow HTTPS traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>8000</td>
<td>Allow vMotion traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>902</td>
<td>Allow ESXi NFC traffic</td>
</tr>
</tbody>
</table>
### vSAN VLAN

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>8006</td>
<td>Allow traffic used for Virtual SAN health monitoring</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>8006</td>
<td>Allow traffic used for Virtual SAN health monitoring</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>80</td>
<td>Allow vSAN HTTP traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>2233</td>
<td>Allow vSAN Transport traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>12345</td>
<td>Allow vSAN Clustering Service traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>12321</td>
<td>Allow Unicast agent traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>23451</td>
<td>Allow vSAN Clustering Service traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process communication</td>
</tr>
</tbody>
</table>

### vSphere VLAN

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>UDP</td>
<td>All</td>
<td>123</td>
<td>Allow NTP port traffic</td>
</tr>
<tr>
<td>Direction</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port</td>
<td>Destination Port</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
<td>Allow SSH traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>1234</td>
<td>Allow traffic for NSX messaging channel to NSX Manager</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>1234-2345</td>
<td>Allow traffic for vSAN Cluster Monitoring, Membership, and Directory Service</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>1232</td>
<td>Allow Unicast agent traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>2233</td>
<td>Allow RDT traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>2480</td>
<td>Allow NestDB traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>3260</td>
<td>Allow iSCSI traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>3784-3785</td>
<td>Allow BFD traffic between nodes</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>UDP</td>
<td>All</td>
<td>427</td>
<td>Allow CIM client traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>UDP</td>
<td>All</td>
<td>427</td>
<td>Allow CIM client traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
<td>Allow HTTPS traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>5026</td>
<td>Allow Edge HA traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>53</td>
<td>Allow DNS traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>UDP</td>
<td>All</td>
<td>53</td>
<td>Allow DNS traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>UDP</td>
<td>All</td>
<td>5355</td>
<td>Allow systemd-resolve traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>5480</td>
<td>Allow appliance management traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>5555</td>
<td>Allow NSX Agent traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>5671</td>
<td>Allow AMQP traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>1234</td>
<td>Allow NSX messaging traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8080</td>
<td>Allow HTTP traffic</td>
</tr>
<tr>
<td>Direction</td>
<td>Source</td>
<td>Protocol</td>
<td>Source CIDR</td>
<td>Destination Port</td>
<td>Port</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------</td>
<td>------</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>5900</td>
<td>5900</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>5988</td>
<td>5988</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>6500</td>
<td>6500</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>6500</td>
<td>6500</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>6666</td>
<td>6666</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>6999</td>
<td>6999</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN</td>
<td>TCP</td>
<td>All</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8100</td>
<td>8100</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>8100</td>
<td>8100</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8000</td>
<td>8000</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>8000</td>
<td>8000</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8010</td>
<td>8010</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8006</td>
<td>8006</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>8006</td>
<td>8006</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8301</td>
<td>8301</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>8889</td>
<td>8889</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>TCP</td>
<td>All</td>
<td>902</td>
<td>902</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDD</td>
<td>UDP</td>
<td>All</td>
<td>902</td>
<td>902</td>
</tr>
<tr>
<td>Direction</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port</td>
<td>Destination Port</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>9080</td>
<td>Allow I/O Filter traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>9090</td>
<td>Allow vSphere Web Client traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>9090</td>
<td>Allow vSphere Web Client traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>9443</td>
<td>Allow vSphere Web Client traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>9443</td>
<td>Allow vSphere Web Client traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
<td>Allow traffic to TCP ports for VMware cluster</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>All</td>
<td>Allow traffic to UDP ports for VMware cluster</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process communication</td>
</tr>
</tbody>
</table>

**HCX VLAN**

The NSG for this VLAN has the following stateful security rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow all egress traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>31031</td>
<td>Allow HCX bulk migration traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>8000</td>
<td>Allow HCX X-cloud vMotion traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
<td>Allow HCX X-cloud control traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>9443</td>
<td>Allow HCX REST API traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>902</td>
<td>Allow HCX cold migration traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>TCP</td>
<td>All</td>
<td>80</td>
<td>Allow OVF import traffic</td>
</tr>
<tr>
<td>Ingress</td>
<td>VCN CIDR</td>
<td>UDP</td>
<td>All</td>
<td>4500</td>
<td>Allow HCX WAN transport traffic</td>
</tr>
<tr>
<td>Direction</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port</td>
<td>Destination Port</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Ingress</td>
<td>SDDC CIDR</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>Allow ingress traffic for VMware inter-process communication</td>
</tr>
</tbody>
</table>
Chapter 41

Web Application Firewall

This chapter explains how to make your endpoints more secure by monitoring and filtering out potentially malicious traffic.

Overview of the Web Application Firewall Service

Oracle Cloud Infrastructure Web Application Firewall (WAF) is a cloud-based, Payment Card Industry (PCI) compliant, global security service that protects applications from malicious and unwanted internet traffic. WAF can protect any internet facing endpoint, providing consistent rule enforcement across a customer's applications.

WAF provides you with the ability to create and manage rules for internet threats including Cross-Site Scripting (XSS), SQL Injection and other OWASP-defined vulnerabilities. Unwanted bots can be mitigated while tactically allowed desirable bots to enter. Access rules can limit based on geography or the signature of the request.

The global Security Operations Center (SOC) will continually monitor the internet threat landscape acting as an extension of your IT infrastructure.

Web Application Firewall Service Components

WEB APPLICATION FIREWALL POLICY

WAF policies encompass the overall configuration of your WAF service, including origin management, protection rule settings, and bot detection features.

ORIGIN

Your web application's origin host server. An origin must be defined in your WAF policy in order to set up protection rules or other features.

PROTECTION RULES

Protection rules can be configured to either allow, block, or log network requests when they meet the specified criteria of a protection rule. The WAF will observe traffic to your web application over time and suggest new rules to apply. To view a list of available WAF rules, see Supported Protection Rules.

BOT MANAGEMENT

The WAF service includes several features that allow you to detect and either block or allow identified bot traffic to your web applications. Bot management features include: JavaScript Challenge, CAPTCHA Challenge, and GoodBot whitelists. For more information, see Bot Management.

Ways to Access the WAF Service

You can access Oracle Cloud Infrastructure using the Console (a browser-based interface), command line interface (CLI), or the REST API. Instructions for the Console and API are included in topics throughout this guide.

To access the Console, you must use a supported browser. You can use the Console link at the top of this page to go to the sign-in page. Enter your tenancy, user name, and your password.
**Authentication and Authorization**

Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups, compartments, and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, etc. For more information, see Getting Started with Policies on page 2135. For specific details about writing policies for each of the different services, see Policy Reference on page 2167.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

**Note About The API**

The WAF service is powered by the Oracle Cloud Infrastructure Web Application Acceleration and Security (WAAS) API. All WAF related calls must be made using the WAAS API. To create a WAF configuration using the API, you must first create a WAAS policy with a defined origin and domain using the API. For the purposes of access control, you must provide the OCID of the compartment where you want the service to reside. For information about access control and compartments, see Overview of the IAM Service.

**WAF Service Capabilities and Limits**

The WAF service is limited to 50 policies per tenant. See Service Limits on page 215 for a list of applicable limits and instructions for requesting a limit increase. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

The WAF service allows a total run time of 20 minutes for upload and download processes through the WAF.

**Required IAM Service Policy**

To use Oracle Cloud Infrastructure, you must be given access in a policy for waas-policy. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in.

**Policy examples:**

- To allow a specific user group to manage policies in the WAF:

  ```
  Allow group <GroupName> to manage waas-policy in compartment <CompartmentName>
  ```

- To allow a specific user group to read waas-work-request in compartment <CompartmentName>:

  ```
  Allow group <GroupName> to read waas-work-request in compartment <CompartmentName>
  ```

- To allow a specific user group to manage certificates in the WAF:

  ```
  Allow group <GroupName> to manage waas-certificate in compartment <CompartmentName>
  ```

- To allow a specific user group view policies in the WAF:

  ```
  Allow group <GroupName> to read waas-policy in tenancy <TenancyName>
  ```

If you’re new to policies, see Getting Started with Policies and Common Policies. For more details about policies for WAF, see Details for the WAF Service on page 2353.
Moving WAF Policies to a Different Compartment

You can move WAF policies from one compartment to another. After you move a WAF policy to the new compartment, inherent policies apply immediately and affect access to the WAF policies through the Console, SDK or CLI. For more information, see Managing Compartments on page 2431.

Monitoring Resources

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring Overview on page 2660 and Notifications Overview on page 3350.

For information about available WAF service metrics and how to view them, see WAF Metrics on page 4170.

Creating Automation with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events on page 1784.

Tagging Resources

You can apply tags to your resources to help you organize them according to your business needs. You can apply tags at the time you create a resource, or you can update the resource later with the wanted tags. For general information about applying tags, see Resource Tags on page 211.

Getting Started with WAF

If you're new to Oracle Cloud Infrastructure WAF, this topic gives guidance on how to proceed.

Before You Begin

To begin using the WAF service, you must have the following available if you plan to run your site on HTTPS/443:

- Public certificate for the fully qualified domain name (FQDN) of the application.
- Corresponding private key for the site.
- IP address of the LBaaS or other public facing endpoint of application.
- Ability to update DNS records for the domain.
- WAF only supports traffic on ports 80/443. Make sure your application is not running on other ports.

Securing Your WAF

To secure your WAF, you must configure your servers to accept traffic from the WAF servers. Configure your origin's ingress rules to only accept connections from the following CIDR ranges.

CIDR Ranges

- 129.146.12.128/25
- 129.146.13.128/25
- 129.146.14.128/25
- 129.213.0.128/25
- 129.213.2.128/25
- 129.213.4.128/25
- 130.35.0.0/20
- 130.35.112.0/22
- 130.35.116.0/25
- 130.35.120.0/21
- 130.35.128.0/20
- 130.35.144.0/20
- 130.35.16.0/20
- 130.35.176.0/20
- 130.35.192.0/19
- 130.35.224.0/22
- 130.35.232.0/21
- 130.35.240.0/20
- 130.35.48.0/20
- 130.35.64.0/19
- 130.35.96.0/20
- 132.145.0.128/25
- 132.145.2.128/25
- 132.145.4.128/25
- 134.70.16.0/22
- 134.70.24.0/21
- 134.70.32.0/22
- 134.70.56.0/21
- 134.70.64.0/22
- 134.70.72.0/22
- 134.70.76.0/22
- 134.70.8.0/21
- 134.70.80.0/22
- 134.70.84.0/22
- 134.70.88.0/22
- 134.70.92.0/22
- 134.70.96.0/22
- 138.1.0.0/20
- 138.1.104.0/22
- 138.1.128.0/19
- 138.1.16.0/20
- 138.1.160.0/19
- 138.1.192.0/20
- 138.1.208.0/20
- 138.1.224.0/19
- 138.1.32.0/21
- 138.1.40.0/21
- 138.1.48.0/21
- 138.1.64.0/20
- 138.1.80.0/20
- 138.1.96.0/21
- 140.204.0.128/25
- 140.204.12.128/25
- 140.204.16.128/25
- 140.204.20.128/25
- 140.204.24.128/25
- 140.204.4.128/25
- 140.204.8.128/25
- 140.91.10.0/23
- 140.91.12.0/22
- 140.91.22.0/23
- 140.91.24.0/22
Create a Policy to Route Traffic Through the WAF

To begin, create a policy to route traffic through the WAF without rules enabled. Creating a policy without rules enabled ensures that there are no regressions by having a reverse proxy in front of the application.

To create a policy

1. Select the region and compartment where the policy should be maintained (there is no constraint around the WAF co-existing with Load Balancing or other application resources in Oracle Cloud Infrastructure.)
2. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.

3. Click Create WAF Policy.

4. In the Create WAF Policy dialog box, enter the following:
   - **Name**: A unique name for the policy. Avoid entering confidential information.
   - **Domains**:
     - **Primary Domain**: The fully qualified domain name (FQDN) of the application where the policy will be applied.
     - **Additional Domains**: (Optional) Subdomains where the policy will be applied.

   **Note**: Wildcard domains are accepted, however, only as additional domains and only through the API and CLI.

   - **WAF Origin**: The host or IP address of the public internet facing application that is being protected by the application.
     - **Origin Name**: A unique name for the origin.
     - **URI**: Enter the public facing endpoint (IPv4 or FQDN) of the application.
     - **HTTPS Port**: The port used for secure HTTP connection. The default port is 443.
     - **HTTP Port**: The HTTP port the origin listens on. The default port is 80.
     - **Headers**: (Optional)
       - **Header Name**: The name displayed in the HTTP request header and the header value that can be added and passed to the origin server with all requests.
       - **Header Value**: Specifies the data requested by the header.
     - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click Create WAF Policy. The WAF Policy overview appears. Expect the policy to become active within 15 minutes of creation.

**Update Origin Keep Alive Timeout**

WAF requires that your origin’s (load balancer or web server) keep alive timeouts are maintained for 301 seconds or more as our upstream timeout value is 300 seconds. During this period of time, the connections will be safely maintained while TCP is optimized. This is due to the network multiplexing methodology our nodes use to maintain connectivity with your origin.

**Update DNS to Enable WAF**

In this step, you update the CNAME for your zone to route requests from internet clients to WAF. Use the following instructions to make this DNS change in the Console. If your DNS setup resides with another provider, refer to their documentation for instructions.

**To update the CNAME for your zone**

1. In the Policy Information tab of the WAF Policy overview, select the CNAME Target.
2. Copy the CNAME target to your clipboard.
3. Open the navigation menu. Under Core Infrastructure, go to Networking, DNS Management, and click Zones.
4. Click the Zone Name of the primary domain where you want to update the record. Zone details and a list of records appear.
5. Select the check box for the CNAME record and select Edit from the Actions drop-down menu.
6. In the Edit Record dialog box, update the Target field with the CNAME Target from your clipboard.
7. Click Submit.
8. Click **Publish Changes**.
9. In the confirmation dialog box, click **Publish Changes**.

**Upload Your Certificate and Key**

This step assumes that your site runs on HTTPS/443.

**To upload your certificate and key**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of your WAF Policy. The WAF Policy overview appears.
3. Click **Settings**.
4. Click **General Settings**.
5. Click **Edit**.
6. In the **Edit Settings** dialog box, enter the following:
   
   - **Enable HTTPS Support**: Click this check box to enable all communications between the browser and web app to be encrypted.
   
   - **Certificate Source**: Choose one of the following methods:
     
     - **Choose Certificate**: Select an existing certificate from the drop down menu. Click **Change Compartment** to select a certificate from another compartment.
     
     - **Upload or Paste Certificate and Private Key**
       
       - Drag and drop, select, or paste a valid SSL certificate in PEM format. You must also include intermediate certificates (the website certificate must be first). The following is an example:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate_Base64_encoded_certificate>
-----END CERTIFICATE-----
```

- **Private Key**: Drag and drop, select, or paste a valid private key in PEM format in this field. The private key cannot be protected by a passphrase. The following is an example:

```
-----BEGIN PRIVATE KEY-----
<Base64_encoded_private_key>
```
• **Self Signed Certificate:** Enable this field when using a self-signed certificate to show an SSL warning in the browser.

• **HTTP to HTTPS Redirect:** When enabled, all HTTP traffic is automatically redirected to HTTPS.

• **TLS Protocols Support:** Select a TLS protocol from the drop down list.

  **Caution:**

  TLS versions 1 and 1.1 have been deprecated and cannot be used in policy configurations. If you use these versions, a validation error might occur. Use versions 1.2 or 1.3 instead.

• **Enable SNI:** Server Name Indication (SNI) is an extension of the TLS protocol, which allows multiple secure hostnames to be served from a single IP address.

• **Advanced Options**
  - **Enable Response Buffering:** Enable or disable buffering of the response from the origin.
  - **Cache Control Respected:** Enable or disable automatic content caching based on the response cache-control header.
  - **Behind CDN:** Enable this to allow the collection of IP addresses from the client request if WAF is connected to a CDN.

7. Click **Save Changes**. Updates to your WAF policy appear in the list to be published in Unpublished Changes.

8. In the WAF Policy overview, under **Unpublished Changes**, click **View**.

9. In the Unpublished Changes list, click the drop down arrow beside an unpublished change to review the change.

10. Click **Publish All**.

11. In the Publish Changes dialog box, click **Publish All**.

---

**Test Your Application**

In this step, you ensure that requests are being routed to the WAF and that your application continues to function normally with a reverse proxy in the topology.

**To test your application**

1. Open a browser.

2. Enter the FQDN of the website protected by WAF.

3. Test the functionality of the application.

4. Inspect HTTP Response Headers to see if traffic is flowing through WAF. Some HTTP Response Headers to look for are:

   - **X-Cdn: Served-By-Zenedge**
   - **Server: ZENEDGE**

5. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.

6. Click the name of your WAF Policy. The WAF Policy overview appears.


  **Note:**

  You may experience a one-minute delay on logs aggregated and available through the console.

8. Copy the IP address and User-Agent value of your requests to your clipboard. You can use this information when you enable WAF to passively detect for access rules.
Enable WAF to Passively Detect Rules

In this step, you enable WAF to detect protection rules without blocking requests. Enabling WAF to passively detect rules helps you visualize the traffic that may pose a threat to your site and help you tune the WAF to exclude false positives.

To enable WAF to detect protection rules

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure rule settings for. The WAF Policy overview appears.
3. Click Protection Rules.
4. Use the Protection Rules table to locate the rules you want to detect.
5. Enter the Rule IDs you located from the table into the Rule ID filter. For this example, enter 941140 (Cross-Site Scripting) in the Rule ID filter.
6. Select Detect from the Actions drop down menu for the protection rules you filtered.

To enable WAF to detect access rules

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure access rules for. The WAF Policy overview appears.
3. Click Access Control.
4. Click Add Access Rule.
5. In the Add Access Rule dialog box, enter the following:
   a. Name: DetectRequestsFromMySpecificBrowser
   b. Rule Action: Select Detect Only.
   c. Conditions: Select IP Address is from the drop down and enter the IP address you copied to your clipboard while testing your application in the IP Address field.
   d. Click +Additional Condition.
   e. Condition: Select User Agent is from the drop down and enter the agent value you copied to your clipboard while testing your application in the User Agent Header field.

   Note:
   Both the IP Address and the User Agent in the preceding example must match for the rule to be triggered. If a different User Agent is used to test your application, the request will not be detected.

6. Click Add Access Rule.
7. Click Unpublished Changes.
8. Click Publish All.

Test the Rules

When the policy is active, you can test that your rules are detected by WAF.

To initiate requests

1. Use the same browser you used when you tested your application to do the following:
   a. Request the FQDN of your application.
   b. Request the FQDN of your application with the following query parameter appended: ?id=<script>alert("TEST");</script>.
2. Use a different browser on the same machine and repeat the preceding requests. All requests should go through the application.

To verify that WAF is detecting requests

To verify that WAF is detecting requests identified as a risk:
1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to view logs for. The WAF Policy overview appears.
3. Click **Logs**. Logs for the WAF policy appear.
4. Select the **Detect** check box from the **Actions** filter.
5. Verify that there are two entries for the protection rule triggered by the Cross-Site Scripting request and one entry for detecting the User Agent and IP Address.

View Recommendations

To view protection rule recommendations

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to view protection rule recommendations for. The WAF Policy overview appears.
3. Click **Protection Rules**.
4. Click the **Recommendations** tab. This list is generated based on the traffic the WAF detects flowing through the WAF. If nothing appears in this list, keep testing the FQDN of your application and check back later.
5. Select the protection rules with a **Detect** recommended action and then click **Accept Recommendations**.

**Tip:**

You can use the **Recommended Action** filter to locate a recommendation by **Detect**.

Enable WAF to Actively Block Requests

After you verify that requests are being detected, you can start blocking the undesired traffic.

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to configure rule settings for. The WAF Policy overview appears.
3. Click **Protection Rules**.
4. Enter rule ID **941140** in the **Rule ID** filter.
5. (Optional) To search for rules with a Detect action, select the **Detect** check box from the **Rule Action** filter.
6. Select **Block** from the **Actions** drop down menu for rule ID **941140** and any other protection rules you filtered.
7. Under WAF Policy, click **Unpublished Changes**.
8. Click **Publish All**.
9. In the Publish Changes dialog box, click **Publish All**.
10. Test the rules again by initiating requests. You should get 403 Forbidden errors when testing with the JavaScript on the URL.

Managing WAF Policies

The Oracle Cloud Infrastructure WAF service enables you to create a WAF policy and origin.

Order of Processing

The order in which rules and handlers are processed is:

1. IP Whitelists/Blocklists/Good Bot Whitelists
2. Access Rules
3. JavaScript Challenge
4. Device Fingerprinting Challenge (available in the API)
5. Human Interaction Challenge (available in the API)
6. Captcha Challenge
7. Protection Rules
8. Rate Limiting (available in the API)

**Using the Console**

**Create and Manage WAF Policies**

**To create a WAF policy**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click Create WAF Policy.
3. In the Create WAF Policy dialog box, enter the following:
   - **Name**: Optional. A unique name for the policy. Avoid entering confidential information.
   - **Domains**:
     - **Primary Domain**: The fully qualified domain name (FQDN) of the application where the policy will be applied.
     - **Additional Domains**: (Optional) Subdomains where the policy will be applied.
   - **WAF Origin**: The host or IP address of the public internet facing application that is being protected by the application.
     - **Origin Name**: A unique name for the origin. Avoid entering confidential information.
     - **URI**: The IPv4 address or fully qualified domain name (FQDN) of the origin. The URI can be a full URI, not just a host/IP.
     - **HTTPS Port**: The port used for secure HTTP connection. The default port is 443.
     - **HTTP Port**: The HTTP port the origin listens on. The default port is 80.
   - **Header(s)**: (Optional)
     - **Header Name**: The name displayed in the HTTP request header and the header value that can be added and passed to the origin server with all requests.
     - **Header Value**: Specifies the data requested by the header.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

   **Note:**
   You can add multiple origins to your WAF policy and load balance them accordingly using the origins and originGroups field of the UpdateWaasPolicy operation in the WAAS API.

4. Click Create WAF Policy. The WAF Policy overview appears. You can access Origin Management, Access Control, WAF, Bot Management, Alerts, and any unpublished changes. While the policy is being created, no changes can be made until the process has completed. Expect the policy to become active within 15 minutes of creation.

   A CNAME target is generated for each policy. The CNAME target is a hyphenated version of your FQDN within the Oracle Cloud Infrastructure domain (for example, myapp-mydomain-com.oraclecloud.net).

5. In your DNS zone, update the CNAME record entry with the value of the CNAME target that is generated. This enables traffic to be routed through the WAF before the application. This value is presented soon after you publish your policy the first time on the main page of the policy.

**To update a WAF policy**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to update. The WAF Policy overview appears.

   | Tip: |
   | You can use the Date Created sort filter to sort policies by the date they were created in ascending or descending order. |

3. Click Edit.
4. In the Edit WAF Policy dialog box, make the needed changes and then click Save Changes.

**To delete a WAF policy**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Select the check box for the policy you want to delete.

   | Tip: |
   | You can use the Date Created sort filter to sort policies by the date they were created in ascending or descending order. |

3. Click Delete.
4. In the confirmation dialog box, click Delete.

   The status of the policy changes from Active to Deleting. Deleted policies are maintained for a short time before they are unavailable in the Console.

**To publish changes**

Updates to your WAF policy appear in the list to be published in Unpublished Changes. Pending changes do not persist across browser sessions. Once you publish changes, it cannot be edited until changes propagate to the edge nodes.

1. In the WAF Policy overview, click Unpublished Changes.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Click Publish All.
4. In the Publish Changes dialog box, click Publish All.

**To manage tags for a WAF policy**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to view. The WAF Policy overview appears.
3. Click the Tags tab to view or edit existing tags. Or click Apply tag(s) to add new ones.

For more information, see Resource Tags on page 211.

**To move a WAF policy to a different compartment**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. In the Scope section, select a compartment.
3. Find the WAF policy in the list, click the the Actions icon (three dots), and then click Move Resource to a Different Compartment.
4. Choose the destination compartment from the list.
5. Click Move Resource.

**Using the CLI**

Open a command prompt and run the following command to get the details of a WAAS policy:

```
oci waas waas-policy get --waas-policy-id <policy_ocid>
```
This can be useful in retrieving the necessary information when opening a ticket with Oracle Cloud Infrastructure support. For more information about how to access and use the CLI, see Command Line Interface (CLI).

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- CreateWaasPolicy
- GetWaasPolicy
- UpdateWaasPolicy
- DeleteWaasPolicy
- ChangeWaasPolicyCompartment

Origin Management

An origin is an endpoint (typically an IP address) of the application protected by the WAF. An origin can be an Oracle Cloud Infrastructure load balancer public IP address which can be used for high availability to an origin. When you create a WAF policy, you define a default origin and optional HTTP headers. An origin must be defined in your WAF policy in order to set up protection rules or other features. The details for the origin can be modified later in the Settings of the WAF policy. In the Origin Settings you can modify or set up HTTP headers for outbound traffic from the WAF to the origin server. These name value pairs are then available to the application.

Origin Groups

Multiple origins can be defined for a WAF policy using Origin Groups. When at least two origins are configured, load balancing is enabled. You can group together multiple origins in an origin group. An origin group can include origin servers and their weights. The weight of each origin in the origin group determines the priority when load balancing across origins in this group. Origins with higher weights receive larger proportions of client requests. You can use origin groups to specify the default origin that will be used in your WAF policy.

Securing Your WAF

To secure your WAF, you must configure your servers to accept traffic from the WAF servers. Configure your origin's ingress rules to only accept connections from the following CIDR ranges.

CIDR Ranges

- 129.146.12.128/25
- 129.146.13.128/25
- 129.146.14.128/25
- 129.213.0.128/25
- 129.213.2.128/25
- 129.213.4.128/25
- 130.35.0.0/20
- 130.35.112.0/22
- 130.35.116.0/25
- 130.35.120.0/21
- 130.35.128.0/20
- 130.35.144.0/20
- 130.35.16.0/20
- 130.35.176.0/20
- 130.35.192.0/19
- 130.35.224.0/22
- 130.35.232.0/21
- 130.35.240.0/20
- 130.35.48.0/20
- 130.35.64.0/19
- 130.35.96.0/20
- 132.145.0.128/25
- 132.145.2.128/25
- 132.145.4.128/25
- 134.70.16.0/22
- 134.70.24.0/21
- 134.70.32.0/22
- 134.70.56.0/21
- 134.70.64.0/22
- 134.70.72.0/22
- 134.70.76.0/22
- 134.70.8.0/21
- 134.70.80.0/22
- 134.70.84.0/22
- 134.70.88.0/22
- 134.70.92.0/22
- 134.70.96.0/22
- 138.1.0.0/20
- 138.1.104.0/22
- 138.1.128.0/19
- 138.1.16.0/20
- 138.1.160.0/19
- 138.1.192.0/20
- 138.1.208.0/20
- 138.1.224.0/19
- 138.1.32.0/21
- 138.1.40.0/21
- 138.1.48.0/21
- 138.1.64.0/20
- 138.1.80.0/20
- 138.1.96.0/21
- 140.204.0.128/25
- 140.204.12.128/25
- 140.204.16.128/25
- 140.204.20.128/25
- 140.204.24.128/25
- 140.204.4.128/25
- 140.204.8.128/25
- 140.91.10.0/23
- 140.91.12.0/22
- 140.91.22.0/23
- 140.91.24.0/22
- 140.91.28.0/23
- 140.91.30.0/23
- 140.91.32.0/23
- 140.91.34.0/23
- 140.91.36.0/23
- 140.91.38.0/23
Using the Console  
To add an origin or origin group

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to add an origin to. The WAF Policy overview appears.
3. Click Settings.
4. Click Origin Groups. If there is more than one origin for the WAF policy, the origins and its group appear.
5. Click Edit. If there is only one origin defined for the WAF policy, the origin belongs to a default origin group.
6. Optionally, you can edit the name of the existing default group or add an additional group to group together multiple origins. You can use origin groups to specify the default origin that will be used in your WAF policy.
7. Click + Additional Origin below the origin group where you want to add an origin.
8. Enter the following:
   - **Name**: A unique name for the origin. Avoid entering confidential information.
   - **Default Origin**
     - **Name**: A unique name for the origin.
     - **URI**: The IPv4 address or FQDN of the origin.
     - **HTTP Port**: The HTTP port on the origin that the web application listens on. The default port is 443.
     - **HTTPS Port**: The HTTPS port on the origin that the web application listens on. The default port is 80.
     - **Weight**: The weight of the origin within the group is used for load balancing purposes. Origins with higher weights will receive larger proportions of client requests.

9. Click **Save Changes**.

   The changes must be published before they take affect. See To publish changes on page 4069.

**To edit an origin**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy where you want to edit the origin. The WAF Policy overview appears.
3. Click **Settings**.
4. Click the **Origin Settings** tab.
5. Click **Edit**.
6. In Origin Management Settings, make the necessary changes:
   - **Enable Health Checks**: Optional. Click the check box to enable Health Checks, then enter the following:
     - **Request and URL**: The type of request and the specific path to visit on the origin when performing the check.
     - **Host Header**: The value of the host header in the HTTP health check request. If this field is left blank, the policy domain will be used instead.
     - **User Agent**: The value of the user agent header in the HTTP health check request.
     - **Expected Response Code Group**: The HTTP response codes that signify the health state.
     - **Check Interval (seconds)**: Interval (in seconds) between health checks to the origin.
     - **Response Timeout (seconds)**: Enter the time to wait for a reply before marking the health check as failed.
     - **Healthy Threshold (number of times)**: Number of successful health checks after which the origin server is marked up.
     - **Unhealthy Threshold (number of times)**: Number of failed health checks after which the origin server is marked down.
     - **Enable Response Text Checking**: Enable to check for predefined text in addition to the response code.
     - **Expected Response Text**: Optional. Health checks will search for the given text in a case-sensitive manner within the response body and will fail if the text is not found.
   - **Load Balancing Method**:
     - **Note**: Load balancing is only enabled when at least two origins have been defined. To define additional origins, see To add an origin or origin group on page 4066.

Select one of the following methods:
   - **IP_HASH**: All of the incoming requests from the same client IP address should go to the same content origination server. IP_HASH load balancing method uses origin weights when choosing which origin should be hashed assigned to initially.
   - **ROUND_ROBIN**: Forwards requests sequentially to the available origin servers. The first request is to the first origin server, the second request is to the next origin server, and so on. After it sends a request to the last origin server, it starts again with the first origin server. When using weights on origins, Weighted
Round Robin assigns more requests to origins with a greater weight. Over a period of time, origins will receive a number of requests in proportion to their weight.

- **STICKY_COOKIE**: Adds a session cookie to the first response from the origin server and identifies the server that sent the response. The client's next request contains the cookie value, and nginx routes the request to the origin server that responded to the first request. STICKY_COOKIE load balancing method falls back to Round Robin for the first request.

- **Enable Origin Compression**: Enable or disable GZIP compression of origin responses.
- **Custom Headers**: Optional. Enter the custom HTTP headers to set or override in requests to origin servers.

7. Click Save Changes.

**To edit an origin group**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to edit the origin for. The WAF Policy overview appears.
3. Click **Settings**.
4. Click **Origin Groups**. If there is more than one origin for the WAF policy, the origins and its group appear.
5. Click **Edit**. If there is only one origin defined for the WAF policy, the origin belongs to a default origin group.
6. Edit the name of the existing default group or add an additional group to group together multiple origins. You can use origin groups to specify the default origin that will be used in your WAF policy.
7. Click Save Changes.

The changes must be published before they take effect. See To publish changes on page 4069.

**To edit the load balancing method for origins**

Note:

Load balancing is only enabled when at least two origins have been defined. To define additional origins, see To add an origin or origin group on page 4066.

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy where you want to edit the origin. The WAF Policy overview appears.
3. Click **Settings**.
4. Click the **Origin Settings** tab.
5. Click **Edit**.
6. In Origin Management Settings, select one of the following options:
   - **IP_HASH**: All of the incoming requests from the same client IP address should go to the same content origination server. IP_HASH load balancing method uses origin weights when choosing which origin should the hash be assigned to initially.
   - **ROUND_ROBIN**: Forwards requests sequentially to the available origin servers. The first request is to the first origin server, the second request is to the next origin server, and so on. After it sends a request to the last origin server, it starts again with the first origin server. When using weights on origins, Weighted Round Robin assigns more requests to origins with a greater weight. Over a period of time, origins will receive a number of requests in proportion to their weight.
   - **STICKY_COOKIE**: Adds a session cookie to the first response from the origin server and identifies the server that sent the response. The client's next request contains the cookie value, and nginx routes the request to the origin server that responded to the first request. STICKY_COOKIE load balancing method falls back to Round Robin for the first request.
7. **Enable Origin Compression**: Optional. Enable or disable GZIP compression of origin responses.
8. **Custom Headers**: Optional. Enter the custom HTTP headers to set or override in requests to origin servers.
9. Click Save Changes.
To publish changes

Updates to your WAF policy appear in the list to be published in Unpublished Changes. Pending changes do not persist across browser sessions. Once you publish changes, it cannot be edited until changes propagate to the edge nodes.

1. In the WAF Policy overview, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Click **Publish All**.
4. In the Publish Changes dialog box, click **Publish All**.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- CreateWaasPolicy
- GetWaasPolicy
- UpdateWaasPolicy  To remove an origin from the policy using the API, use the UpdateWaasPolicy method and leave the origin field empty upon update.

Example

Each origin has a unique name (key). The name of the origin to be used by the WAF must be referenced in the wafConfig portion of the settings. For example, if you have the following origins in your configuration:

```json
{
   "compartmentId":"ocid1.compartment.oc1..<unique_ID>",
   "lifecycleState":"ACTIVE",
   "displayName":"myWAFprotectedApp",
   "origins":{
      "primaryorigin":{
         "httpPort":80,
         "httpsPort":443,
         "uri":"67.205.161.231",
         "customHeaders":[
            
            
         ],
      },
      "secondaryorigin":{
         "httpPort":80,
         "httpsPort":443,
         "uri":"54.175.154.7",
         "customHeaders":{
            
            
         }
      }
   }
}
```

Then within the wafConfig, the origin in use would be referenced by name. In this example, the WAF is actively using secondaryorigin.

```
"wafConfig":{
```
"deviceFingerprintChallenge":{
    "isEnabled":false
},
"origin":"secondaryorigin",
"whitelists":[]
],

Example

Using the API, you can define multiple origins for the WaasPolicy.origins field, however, only one of those defined origins can be used in the WaasPolicy.wafConfig.origin field. The following example shows multiple origins defined for the WaasPolicy.origins field, however, only one of these defined origins is used in the WaasPolicy.wafConfig.origin field, as only one origin can be active for a policy.

"origins": {
    "origin1": {
        "uri": "6.6.6.6",
        "httpPort": 80
    },
    "origin2": {
        "uri": "1.1.1.2",
        "httpPort": 80
    }
},
"wafConfig": {
    "origin": "origin1"
}

Example

The following is an example of origin groups being used to specify the weight of each origin:

{
    "originGroup1": {
        "origins": [
            {
                "origin": "origin1",
                "weight": 2
            },
            {
                "origin": "origin2",
                "weight": 1
            }
        ]
    },
    "originGroup2": {
        "origins": [
            {
                "origin": "origin3",
                "weight": 1
            },
            {
                "origin": "origin4",
                "weight": 1
            }
        ]
    }
}
Bot Management

Bot Management enables you to mitigate undesired bot traffic from your site using CAPTCHA and JavaScript detection tools, while enabling known published bot providers to bypass these controls.

Non-human traffic makes up most of the traffic to sites. Bot Manager is designed to detect and block, or otherwise direct, non-human traffic that may interfere with site operations. The Bot Manager features mitigate bots that conduct content and price scraping, vulnerability scanning, comment spam, brute force attacks, and application-layer DDoS attacks. You can also allowlist good bots.

Caution:

When you enable Bot Management, you incur a higher rate on requests to the WAF.

JavaScript Challenge

JavaScript Challenge validates that the client can accept JavaScript with a binary decision. JavaScript Challenge is generally the first level of bot mitigation, but not sufficient with more advanced bot tools, which require more advanced challenges. Additional functionality, like detecting Network Address Translation (NAT) traffic, can mitigate the risk of blocking legitimate user traffic from users behind a shared IP address.

The Action Threshold parameter defines the number of requests that fail the challenge before the action is taken. The requests that fail under this threshold are not logged. For example, if you set the JavaScript challenge action to Block and the Action Threshold to 10, and a client that doesn't accept JavaScript makes 11 requests within the Action Expire Time, the first 10 requests will be allowed through to origin (assuming there are no other rules) and logs will show one Block entry action taken for the JavaScript Challenge.

Human Interaction Challenge

Human Interaction Challenge is an advanced countermeasure that looks for natural human interactions such as mouse movements, time on site, and page scrolling to identify bots. When an EDGE server receives requests from a client, instead of instantly reporting with the requested content, the human interaction challenge checks various event listeners in the user's browser to determine if there is a human user making a request.

Device Fingerprint Challenge

The device fingerprint challenge generates hashed signatures of both virtual and real browsers to identify and block malicious bots.

CAPTCHA Challenge

If a specific URL should be accessed only by a human, you can control it with CAPTCHA protection. You can customize the comments for the CAPTCHA Challenge for each URL. Bots are kept from accessing protected web application functionality using CAPTCHA images designed to be out of reach of computer vision and OCR technologies.

Good Bot Whitelist

Good Bots provides the list of bots managed by known providers, such as Baidu or Google. You can allow the access from a specific good bot, or block the bot if they serve no business purpose. Allowed good bots from this section are allowlisted.

Allowlisted bots are flagged with a Bypass action in the WAF policy Logs. You can select the Bypass check box from the Action filter in Logs to search for the traffic allowed from these rules. Logged good bot events are categorized as a Threat Intelligence Leads log type, however, they are not a threat when the action taken is to Bypass.

The list of good bots on this menu are managed and continuously updated. Additional good bots can be added as a new access control rule in Access Control.
Using the Console
To configure JavaScript Challenge settings

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure JavaScript Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click Edit JavaScript Challenge.
5. In the JavaScript Challenge dialog box, select the Enable JavaScript Challenge check box.
6. In the JavaScript Challenge Action section, choose one of the following methods:
   • Detect Only: Select this option if you want to be alerted for every matched request.
   • Block: Select this option to block requests by returning a response code, error page, or CAPTCHA.
     • Block Action: Select the action that will be taken when a matching request is blocked.
     • Show CAPTCHA
       • CAPTCHA Title: Enter the text for the CAPTCHA page title.
       • CAPTCHA Header: Enter the text that will appear before the CAPTCHA image (for example, "I am not a robot").
       • CAPTCHA Footer Text: Enter the text that will be shown after the CAPTCHA input box and before the submit button.
       • CAPTCHA submit button: Enter the text for the Submit button (for example, "Yes, I am human.").
   • Set Response Code: Select a status code to return in response to blocked requests.
   • Show Error Page
     • Block Error Page Message: Defines the error or error code.
     • Block Error Page Description: Provides more details about the error, including the cause and further instructions.
     • Block Error Page Code: The error code that is displayed with the error.
7. Enter the following information:
   • Enable Conditions: When enabled, conditions must match for a set action to be taken. See Access Control on page 4149 for more information about conditions and rules.
   • Action Threshold (number of requests): Specify the number of failed requests before taking action. Due to the asynchronous request from the browser during page loading, it is recommended to set a threshold of 10 for web applications with basic ajax usage, and 100 for apps with heavy ajax usage.
   • Action Expire Time (seconds): Enter the number of seconds between challenges to the same IP address. Due to client IP address changes, it is recommended that the expiry time is set to 120 seconds for apps with mobile users and 3600 seconds for apps with desktop users only.
   • Follow Redirects: When enabled, redirect responses from the origin will also be challenged.
   • Enable NAT Support: When enabled, the user is identified not only by the IP address but also by a unique additional hash, which prevents blocking visitors with shared IP addresses. It is recommended that this NAT support is disabled for high-load apps (200+RPS).
8. Click Save Changes.

To edit JavaScript Challenge settings

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to edit JavaScript Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click Edit JavaScript Challenge.
5. In the Edit JavaScript Challenge dialog box, make the needed changes.
6. Click Save.

To configure Human Interaction Challenge settings
1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure JavaScript Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the Human Interaction Challenge tab.
5. Click Edit Human Interaction Challenge.
6. In the Edit Human Interaction Challenge dialog box, select the Enable Human Interaction Challenge check box.
7. In the Human Interaction Action section, choose one of the following methods:
   - Detect Only: Select this option if you want to be alerted for every matched request.
   - Block: Select this option to block requests by returning a response code, error page, or CAPTCHA.
     - Block Action: Select the action that will be taken when a matching request is blocked.
     - Show CAPTCHA
       - CAPTCHA Title: Enter the text for the CAPTCHA page title.
       - CAPTCHA Header: Enter the text that will appear before the CAPTCHA image (for example, "I am not a robot").
       - CAPTCHA Footer Text: Enter the text that will be shown after the CAPTCHA input box and before the submit button.
       - CAPTCHA submit button: Enter the text for the Submit button (for example, "Yes, I am human.").
     - Set Response Code: Select a status code to return in response to blocked requests.
     - Show Error Page
       - Block Error Page Message: Defines the error or error code.
       - Block Error Page Description: Provides more details about the error, including the cause and further instructions.
       - Block Error Page Code: The error code that is displayed with the error.
8. Enter the following information:
   - Action Threshold (number of requests): Specify the number of failed requests before taking action. Due to the asynchronous request from the browser during page loading, it is recommended to set a threshold of 10 for web applications with basic ajax usage, and 100 for apps with heavy ajax usage.
   - Threshold Expiry Period (seconds): The number of seconds before the threshold expires.
   - Action Expire Time (seconds): Enter the number of seconds between challenges to the same IP address. Due to client IP address changes, it is recommended that the expiry time is set to 120 seconds for apps with mobile users and 3600 seconds for apps with desktop users only.
   - Interaction Threshold (number of interactions): Number of interactions before the threshold expires.
   - Recording Period (seconds): The period of time to record the user's events.
   - NAT Support: When enabled, the user is identified not only by the IP address but also by an unique additional hash, which prevents blocking visitors with shared IP addresses. It's recommended to disable the support for the high-load apps (200+ RPS).
9. Click Save Changes.

The Human Interaction Challenge is added to the list of changes to be published.

To edit Human Interaction Challenge settings
1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure Human Interaction Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the Human Interaction Challenge tab.
5. Click Edit Human Interaction Challenge.
6. Update the Human Interaction Challenge and then click Save Changes.

To configure Device Fingerprint Challenge settings
1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure Device Fingerprint Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the Device Fingerprint Challenge tab.
5. Click Edit Device Fingerprint Challenge.
6. In the Device Fingerprint Challenge dialog box, select the Enable Device Fingerprint Challenge check box.
7. In the Device Fingerprint Action section, choose one of the following methods:
   • Detect Only: Select this option if you want to be alerted for every matched request.
   • Block: Select this option to block requests by returning a response code, error page, or CAPTCHA.
     • Block Action: Select the action that will be taken when a matching request is blocked.
       • Show CAPTCHA
         • CAPTCHA Title: Enter the text for the CAPTCHA page title.
         • CAPTCHA Header: Enter the text that will appear before the CAPTCHA image (for example, "I am not a robot").
         • CAPTCHA Footer Text: Enter the text that will be shown after the CAPTCHA input box and before the submit button.
         • CAPTCHA submit button: Enter the text for the Submit button (for example, "Yes, I am human.").
       • Set Response Code: Select a status code to return in response to blocked requests.
       • Show Error Page
         • Block Error Page Message: Defines the error or error code.
         • Block Error Page Description: Provides more details about the error, including the cause and further instructions.
         • Block Error Page Code: The error code that is displayed with the error.
8. Enter the following information:
   • Action Threshold (number of requests): Specify the number of failed requests before taking action. Due to the asynchronous request from the browser during page loading, it is recommended to set a threshold of 10 for web applications with basic ajax usage, and 100 for apps with heavy ajax usage.
   • Threshold Expiry Period (seconds): The number of seconds before the threshold expires.
   • Action Expire Time (seconds): Enter the number of seconds between challenges to the same IP address. Due to client IP address changes, it is recommended that the expiry time is set to 120 seconds for apps with mobile users and 3600 seconds for apps with desktop users only.
   • Max Address Count (IP addresses): The maximum number of IP addresses that are added to the list before the specified action is taken.
   • Max Address Count Expiration (seconds): The number of seconds an IP address is kept in the list before it is removed.
9. Click Save Changes.
To edit Device Fingerprint Challenge settings

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure JavaScript Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the Device Fingerprint Challenge tab.
5. Click Edit Device Fingerprint Challenge.
6. Update the Device Fingerprint Challenge and then click Save Changes.

To add a CAPTCHA Challenge

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to edit CAPTCHA challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the CAPTCHA Challenge tab.
5. Click Add CAPTCHA Challenge.
6. In the Add CAPTCHA Challenge dialog box, enter the following information:
   - CAPTCHA Title: Enter the text for the CAPTCHA page title.
   - CAPTCHA URL Path: Enter the URL path challenged by CAPTCHA.
   - Session Duration: Enter the number of seconds after which the CAPTCHA challenge cannot be resubmitted to the same user.
   - CAPTCHA Header: Enter the text that will appear before the CAPTCHA image (for example, "I am not a robot").
   - Footer Text: Enter the text that will be shown after the CAPTCHA input box and before the submit button.
   - Incorrect CAPTCHA Text: Enter the text that will appear when incorrect text is entered (for example, "The CAPTCHA was incorrect. Please try again.").
   - Submit button: Enter the text for the Submit button (for example, "Yes, I am human.").
7. Click Preview CAPTCHA to preview the CAPTCHA challenge in a new tab.
8. Click Add.

To edit a CAPTCHA Challenge

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to edit CAPTCHA Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the CAPTCHA Challenge tab.
5. Select the check box for the CAPTCHA you want to edit.
6. Select Edit from the Actions drop down menu.
7. Update the CAPTCHA Challenge and then click Save.

To delete a CAPTCHA Challenge

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to delete CAPTCHA Challenge settings for. The WAF Policy overview appears.
3. Click Bot Management.
4. Click the CAPTCHA Challenge tab.
5. Select the check box for the CAPTCHA Challenge you want to delete.
6. Click **Delete**.
7. In the Confirm dialog box, click **Delete**.

**To manage the Good Bot Whitelist**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to configure Bot Management for. The WAF Policy overview appears.
3. Click **Bot Management**.
4. Click the **Good Bot Whitelist** tab.
5. Select each bot you want to designate as a good bot.

The designated good bots are added to the list of changes to be published.

**To publish changes**

Updates to your WAF policy appear in the list to be published in Unpublished Changes. Pending changes do not persist across browser sessions. Once you publish changes, it cannot be edited until changes propagate to the edge nodes.

1. Under WAF Policy, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Click **Publish All**.
4. In the Publish Changes dialog box, click **Publish All**.

**To discard changes**

Updates to your WAF policy appear in the list to be published in Unpublished Changes.

1. Under WAF Policy, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Select the check box for the change you want to discard.
4. Click **Discard**.
5. In the Discard Change dialog box, click **Discard**.

**Using the CLI**

You can use the CLI to enable rate limiting, device fingerprinting, and human interaction challenges.

**To enable rate limiting**

Open a command prompt and run the following command to enable rate limiting:

```
oci waas address-rate-limiting update-waf --is-enabled true --allowed-rate-per-address 1 --max-delayed-count-per-address 2 --waas-policy-id <policy_ocid>
```

This default rate limit setting will allow one request per second before starting to delay. It will delay for two requests until the traffic falls within the threshold boundaries. It will use the default error response code of 503.

**To enable device fingerprinting to detect**

Open a command prompt and run the following command to enable device fingerprinting to detect:

```
oci waas device-fingerprint-challenge update --is-enabled true --action DETECT --failure-threshold 2 --action-expiration-in-seconds 240 --failure-threshold-expiration-in-seCONDS 600 --max-address-count 2 --max-address-count-expiration-in-seconds 255 --waas-policy-id <policy_ocid>
```
To enable the human interaction challenge to detect

Open a command prompt and run the following command to enable the human interaction challenge to detect:

```
oci waas human-interaction-challenge update --is-enabled true --waas-policy-id <policy_ocid>
```

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- UpdateJsChallenge
- GetJsChallenge
- UpdateCaptchas
- GetCaptchas
- GetDeviceFingerprintChallenge
- UpdateDeviceFingerprintChallenge
- GetHumanInteractionChallenge
- UpdateHumanInteractionChallenge
- GetWafAddressRateLimiting
- UpdateWafAddressRateLimiting

WAF Protection Rules

Protection rules match web traffic to rule conditions and determine the action to be taken when the conditions are met. Protection Rule Settings allow you to define the parameters for enforcement any time a protection rule is matched. Recommendations aid in the optimization of your WAF security profile. The Security Operations team proactively monitors all events to provide recommendations about the action of a specific ruleset. See Supported Protection Rules on page 4081 for additional information.

Using the Console

To apply an action to a protection rule

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure rule settings for. The WAF Policy overview appears.
3. Click Protection Rules.
4. Click the Rules tab.
5. Find the protection rule you want to apply an action to.

Tip:

You can use the Rule ID or Rule Action filters to locate a protection rule.
6. Click the Actions icon (three dots) and select one of the following options:
   - **Detect**: Matching requests generate an alert and the request is proxied.
   - **Block**: Matching requests are blocked.
   - **Off**: The rule is disabled.
   - **Exclusions**: Exclusions are set to specify the types of request that are to be bypassed by the protection rule(s). If a request matches any of the set exclusions, the protection rule(s) will not be executed for that request.
     a. In the Exclusions dialog box, enter the following criteria:
        - **Exclusion**: Select request cookie values, request cookie names, request parameters, or request parameter names.
        - **Value**: Enter the value for the selected exclusion.
     b. Click **Save Changes**.

The protection rule action is added to the list to be published.

**To edit rule settings**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to configure rule settings for. The WAF Policy overview appears.
3. Click **Protection Rules**.
4. Click the **Settings** tab.
5. Click **Edit Rule Settings**.
6. In the Edit Rule Settings dialog box, enter the following:
   - **Block Action**: The action taken on malicious requests blocked by WAF.
   - **Block Response Code**: Provides information indicating why the request was blocked.
   - **Max Number of Arguments**: The maximum number of arguments allowed in the request. The recommended setting is 255.
   - **Max Length of Argument**: The maximum argument length allowed in the request. The recommended setting is 400.
   - **Max Total Argument Length**: The maximum argument length for all arguments in the request. The recommended setting is 64000.
   - **Recommendations Period**: The period in days to analyze for recommended actions.
   - **Allowed HTTP Methods**: The list of allowed HTTP protocol methods.
7. Click **Save Changes**.

The accepted protection rules are added to the list to be published.

**To accept recommendations**

Recommendations will begin appearing once sufficient traffic has gone through the WAF to profile the right security posture.

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click the name of the WAF Policy you want to configure rule settings for. The WAF Policy overview appears.
3. Click **Protection Rules**.
4. Click the **Recommendations** tab.
5. Select the protection rules you want to accept.
   - **Tip**: You can use the **Recommended Action** filter to locate a recommendation by **Detect** or **Block**.
6. Click **Accept Recommendations**.

The accepted protection rules are added to the list to be published.
To publish changes

Updates to your WAF policy appear in the list to be published in Unpublished Changes. Pending changes do not persist across browser sessions. Once you publish changes, it cannot be edited until changes propagate to the edge nodes.

1. Under WAF Policy, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Click **Publish All**.
4. In the Publish Changes dialog box, click **Publish All**.

To discard changes

Updates to your WAF policy appear in the list to be published in Unpublished Changes.

1. Under WAF Policy, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Select the check box for the change you want to discard.
4. Click **Discard**.
5. In the Discard Change dialog box, click **Discard**.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- GetProtectionRule
- ListProtectionRules
- UpdateProtectionRules
- GetProtectionSettings
- UpdateProtectionSettings
- ListRecommendations
- AcceptRecommendations

Listing and Accepting Protection Rule Recommendations

Use the following operations to get the list of recommended rules:

- ListRecommendations

```json
{
  "name": "SQL authentication bypass attempts",
  "action": "OFF",
  "description": "Detects basic SQL authentication bypass attempts."
}
{
  "modSecurityRuleIds": [
    "950001",
    "959070",
    "959071",
    "959072",
    "950908",
    "959073"
  ],
  "name": "Common SQL Injections"
}
```
"action": "OFF",
"description": "detects common SQL injection attacks",
"exclusions": [],
"key": "950001",
"tags": "SQL Injections, WASCTC, OWASP, A1, PCI, Recommended"
},

Using the key values from the output of the GET call above, you can accept one or more of the recommendations using the following operation passing an array of the keys:

- **AcceptRecommendations**

**Body:**

```json
[
  "981244",
  "950001"
]
```

### Protection Rule Specific Settings

Several protection rule settings are settings for specific protection rules.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Rule ID</th>
<th>Rule Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed HTTP Methods</td>
<td>911100</td>
<td>Restrict HTTP Request Methods</td>
</tr>
<tr>
<td>Max Total Argument Length</td>
<td>960341</td>
<td>Total Arguments Limits</td>
</tr>
<tr>
<td>Max Number of Arguments</td>
<td>960335</td>
<td>Number of Arguments Limits</td>
</tr>
<tr>
<td>Max Length of Argument</td>
<td>960208</td>
<td>Values Limits</td>
</tr>
</tbody>
</table>

The term "Arguments" refers to either query parameters or body parameters in a PUT/POST request. For instance, if the Max Number of Arguments is 2 and RuleID 960335 is set to BLOCK, any of the following requests would be blocked:

```text
GET /myapp/path?query=one&query=two&query=three
POST /myapp/path with Body {"arg1":"one","arg2":"two","arg3":"three"}
POST /myapp/path?query=one&query=two with Body {"arg1":"one"}
```

**Max Length of Argument** is the length of either a name or the value of the argument. **Total Argument Length** refers to the sum of the name and value length.

### Exclusions

Sometimes a protection rule can trigger a false positive. You can configure an exception if the request(s) generating the false positive have a particular argument or cookie that can be used to identify that request be excluded from the action normally taken on the rule. Exclusions have to be created through the API. The following exclusion parameters can be used:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQUEST_COOKIES</td>
<td>Cookie Value</td>
</tr>
<tr>
<td>REQUEST_COOKIES_NAMES</td>
<td>Cookie Name (value is irrelevant)</td>
</tr>
</tbody>
</table>
Web Application Firewall

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARGXS</td>
<td>Argument (Query Parameter or POST/PUT data)</td>
</tr>
<tr>
<td>ARGXS_NAMES</td>
<td>Query Parameter Name (value is irrelevant)</td>
</tr>
</tbody>
</table>

**Example**

In this example, a block is applied to WAF Rule 911100 (Restrict HTTP Request Methods) with an exception to allow requests with an argument that contains “passthrough”.  

```
PUT / waasPolicies /<policy_ocid>/wafConfig/protectionRules
```

With the body:

```
[
  {
    "key":"911100",
    "action":"BLOCK",
    "exclusions":
    [
      {
        "target":"REQUEST_COOKIES",
        "exclusions":["yourcompany.com", "Wed, 21 Oct 2015 07:28:00 GMT", "12345", "219ffwef9w0f"]
      },
      {
        "target":"REQUEST_COOKIES_NAMES",
        "exclusions":["OAMAuthnCookie", "JSESSIONID", "HCM-PSJSESSIONID"]
      },
      {
        "target":"ARGS",
        "exclusions":["passthrough"]
      }
    ]
  }
]
```

This will return a 202 Accepted HTTP status, which means the policy will enter an UPDATING state until changes are provisioned to the edge nodes.

**Supported Protection Rules**

The Oracle Cloud Infrastructure WAF service supports many protection rule types. The following list provides a brief explanation of the purpose of each protection rule type.

**Protection Rules**

<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90001</td>
<td>Filter Profanity</td>
<td>Detects profanity used in request headers and body.</td>
</tr>
<tr>
<td>90002</td>
<td>United States Social Security Number Leakage</td>
<td>Detects leakage of US SSN in C3 body and headers.</td>
</tr>
<tr>
<td>90004</td>
<td>Executable file upload attempt</td>
<td>Detects attempts to upload executable files through input forms.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>90005</td>
<td>Brazilian Social Security Number (CPF) Leakage</td>
<td>Detects leakage of Brazilian CPF in response body and headers.</td>
</tr>
<tr>
<td>90006</td>
<td>Credit card leakage in request: GSA SmartPay</td>
<td>Detects GSA SmartPay credit card numbers in user input.</td>
</tr>
<tr>
<td>90007</td>
<td>Credit card leakage in request: MasterCard</td>
<td>Detects MasterCard credit card numbers in user input.</td>
</tr>
<tr>
<td>90008</td>
<td>Credit card leakage in request: Visa</td>
<td>Detects Visa credit card numbers in user input.</td>
</tr>
<tr>
<td>90009</td>
<td>Credit card leakage in request: American Express</td>
<td>Detects American Express credit card numbers in user input.</td>
</tr>
<tr>
<td>90010</td>
<td>Credit card leakage in request: Diners Club</td>
<td>Detects Diners Club credit card numbers in user input.</td>
</tr>
<tr>
<td>90011</td>
<td>Credit card leakage in request: enRoute</td>
<td>Detects enRoute credit card numbers in user input.</td>
</tr>
<tr>
<td>90012</td>
<td>Credit card leakage in request: Discover</td>
<td>Detects Discover credit card numbers in user input.</td>
</tr>
<tr>
<td>90013</td>
<td>Credit card leakage in request: JCB</td>
<td>Detects JCB credit card numbers in user input.</td>
</tr>
<tr>
<td>90014</td>
<td>Credit card leakage in response: GSA SmartPay</td>
<td>Detects GSA SmartPay credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90015</td>
<td>Credit card leakage in response: MasterCard</td>
<td>Detects MasterCard credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90016</td>
<td>Credit card leakage in response: Visa</td>
<td>Detects Visa credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90017</td>
<td>Credit card leakage in response: American Express</td>
<td>Detects American Express credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90018</td>
<td>Credit card leakage in response: Diners Club</td>
<td>Detects Diners Club credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90019</td>
<td>Credit card leakage in response: enRoute</td>
<td>Detects enRoute credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90020</td>
<td>Credit card leakage in response: Discover</td>
<td>Detects Discover credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>90021</td>
<td>Credit card leakage in response: JCB</td>
<td>Detects JCB credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90022</td>
<td>Credit card Track 1 data leakage</td>
<td>Detects credit card track 1 data in the response body.</td>
</tr>
<tr>
<td>90023</td>
<td>Credit card Track 2 data leakage</td>
<td>Detects credit card track 2 data in the response body.</td>
</tr>
<tr>
<td>90024</td>
<td>Credit card PAN leakage</td>
<td>Detects credit card primary account number in the response body.</td>
</tr>
<tr>
<td>90025</td>
<td>visitorTracker_isMob malware detection</td>
<td>Detects and/or blocks visitorTracker_isMob malware.</td>
</tr>
<tr>
<td>120133</td>
<td>Canadian Social Identification Number (SIN) leakage</td>
<td>Detects leakage of Canadian SIN in response body and headers.</td>
</tr>
<tr>
<td>900032</td>
<td>HTTP Parameter Polution (HPP) detection</td>
<td>Rule Detects requests that have multiple arguments with the same name indicative of HPP attack.</td>
</tr>
<tr>
<td>911100</td>
<td>Restrict HTTP Request Methods</td>
<td>Allows only request methods specified by the configurable &quot;Allowed http methods&quot; parameter.</td>
</tr>
<tr>
<td>920021, 920022, 920023</td>
<td>Credit card PAN leakage</td>
<td>Detects credit card primary account number in the response body.</td>
</tr>
<tr>
<td>920100</td>
<td>Invalid HTTP Request Line</td>
<td>Invalid HTTP Request Line.</td>
</tr>
<tr>
<td>920120</td>
<td>File Name Validation</td>
<td>Detects multipart/form-data file name evasion attempts.</td>
</tr>
<tr>
<td>920160</td>
<td>Content-Length Header Validation</td>
<td>Detects if content-length HTTP header is not numeric.</td>
</tr>
<tr>
<td>920170</td>
<td>GET/HEAD Requests Validation</td>
<td>Detects if GET/HEAD requests contain request body by checking for content-length header, since it is not a common practice.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>920171</td>
<td>GET/HEAD Requests Validation</td>
<td>Detects if GET/HEAD requests contain request body by checking for Transfer-Encoding header since it is not a common practice.</td>
</tr>
<tr>
<td>920180</td>
<td>Content-Length Header Validation</td>
<td>Detects if content-length and Transfer-Encoding headers are provided with every POST request.</td>
</tr>
<tr>
<td>920190</td>
<td>Range Header Validation</td>
<td>This rule inspects the Range request header to see if it starts with 0.</td>
</tr>
<tr>
<td>920200, 920201</td>
<td>Range Header Validation</td>
<td>Detects range header inconsistencies and invalid formatting.</td>
</tr>
<tr>
<td>920220, 920240</td>
<td>Check URL encodings</td>
<td>There are two different chained rules. We need to separate them as we are inspecting two different variables - REQUEST_URI and REQUEST_BODY. For REQUEST_BODY, we only want to run the @validateUrlEncoding operator if the content-type is application/x-www-form-urlencoded.</td>
</tr>
<tr>
<td>920230</td>
<td>Detect multiple url encoding</td>
<td>Detection of multiple url encodings.</td>
</tr>
<tr>
<td>920260</td>
<td>Disallow use of full-width unicode as decoding evasions may be possible.</td>
<td>This rule looks for full-width encoding by looking for %u followed by 2 'f' characters and then 2 hex characters. It is a vulnerability that affected IIS circa 2007.</td>
</tr>
<tr>
<td>920270</td>
<td>Restrict type of characters sent</td>
<td>This rule uses the @validateByteRange operator to restrict the request payloads.</td>
</tr>
<tr>
<td>920280</td>
<td>Missing/Empty Host Header</td>
<td>Missing/Empty Host Header.</td>
</tr>
<tr>
<td>920300</td>
<td>Missing Accept Header</td>
<td>Detection of missing accept header.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>920310, 920311</td>
<td>Empty Accept Header</td>
<td>Checks if an Accept header exists, but has an empty value. Also detects an empty Accept header if there is no user agent.</td>
</tr>
<tr>
<td>920320</td>
<td>Missing User-Agent header</td>
<td>Detection of missing user-agent header.</td>
</tr>
<tr>
<td>920330</td>
<td>Empty User-Agent Header</td>
<td>Detects empty request user-agent header.</td>
</tr>
<tr>
<td>920350</td>
<td>Invalid HTTP Request Line</td>
<td>Invalid HTTP Request Line.</td>
</tr>
<tr>
<td>920360</td>
<td>Limit length of argument names</td>
<td>Detects HTTP requests argument name length exceeding the configurable &quot;Max length of argument name&quot; value.</td>
</tr>
<tr>
<td>920370</td>
<td>Limit argument value length</td>
<td>Detects HTTP requests argument values exceeding the configurable &quot;Max argument value length&quot; parameter.</td>
</tr>
<tr>
<td>920380</td>
<td>Number of Arguments Limits</td>
<td>Detects HTTP requests with number of arguments exceeding the configurable &quot;Max amount of arguments&quot; value.</td>
</tr>
<tr>
<td>920390</td>
<td>Limit arguments total length</td>
<td>Detects HTTP requests argument length exceeding the configurable &quot;Max argument length&quot; parameter.</td>
</tr>
<tr>
<td>920400</td>
<td>Limit file size</td>
<td>Limits the size of a file by checking Content-Length Header for a variable max_file_size.</td>
</tr>
<tr>
<td>920410</td>
<td>Limit combined file size</td>
<td>Limits the size of combined files by checking Content-Length Header for a variable combined_file_sizes.</td>
</tr>
<tr>
<td>920420</td>
<td>Check content-type header</td>
<td>Restrict Content Types by checking the variable allowed_request_content_type.</td>
</tr>
<tr>
<td>920430</td>
<td>Request protocol version</td>
<td>Restrict protocol versions by using the variable allowed_http_versions.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>920440</td>
<td>Restriction by file extension</td>
<td>Restrict file extensions using the variable restricted_extensions.</td>
</tr>
<tr>
<td>920450</td>
<td>Restricted HTTP headers</td>
<td>The use of certain headers is restricted. They are listed in the variable restricted_headers.</td>
</tr>
<tr>
<td>920470</td>
<td>Restrict Content Type</td>
<td>Restrict Content Types by checking the content-type header.</td>
</tr>
<tr>
<td>920480</td>
<td>Charset restriction in content-type</td>
<td>Restrict charset in Content Types by checking the variable allowed_request_content_type_charset.</td>
</tr>
<tr>
<td>920500</td>
<td>Detect backup or working files</td>
<td>Detect backup or working files.</td>
</tr>
<tr>
<td>921110</td>
<td>HTTP Request Smuggling</td>
<td>Looks for CR/LF characters in combination with HTTP / WEBDAV.</td>
</tr>
<tr>
<td>921120, 921130</td>
<td>HTTP Response Splitting</td>
<td>Looks for CR/LF characters, may cause problems if the data is returned in a responses header and may be interpreted by an intermediary proxy server and treated as two separate responses.</td>
</tr>
<tr>
<td>921140</td>
<td>HTTP Header Injection</td>
<td>These rules look for Carriage Return (CR) %0d and Linefeed (LF) %0a characters, on their own or in combination with header field names. These characters may cause problems if the data is returned in a responses header and interpreted by the client.</td>
</tr>
<tr>
<td>921150, 921160</td>
<td>Argument Newline Detection</td>
<td>Detect newlines in argument names.</td>
</tr>
<tr>
<td>921151</td>
<td>Newline in GET Args</td>
<td>Detect newlines in GET arguments which may point to HTTP header injection attacks.</td>
</tr>
<tr>
<td>921190</td>
<td>HTTP Splitting</td>
<td>This rule detect \n or \r in the REQUEST FILENAME.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>930120</td>
<td>OS File Access Attempt</td>
<td>OS File Access Attempt, Cookies and Arguments.</td>
</tr>
<tr>
<td>930130</td>
<td>Restricted File Access</td>
<td>Restricted File Access. Detects attempts to retrieve application source code, metadata, credentials and version control history possibly reachable in a web root.</td>
</tr>
<tr>
<td>931120</td>
<td>Remote File Inclusion (RFI) Attempt: RFI Attack: URL Payload Used w/Trailing Question Mark Character (?)</td>
<td>Remote File Inclusion (RFI). These rules look for common types of Remote File Inclusion (RFI) attack methods. Possible RFI Attack: URL Payload Used w/Trailing Question Mark Character (?)</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>932106</td>
<td>Unix Command Injection</td>
<td>Detects several Unix command injections (and its attempts of obfuscation and evasion). The vulnerability exists when an application executes a shell command without proper input escaping/validation.</td>
</tr>
<tr>
<td>932110</td>
<td>Remote Command Execution (RCE) Attempt: RCE Windows command injection</td>
<td>Remote Command Execution (RCE) Attempt: RCE This rule Detects Windows shell command injections. If you are not running Windows, it is safe to disable this rule.</td>
</tr>
<tr>
<td>932115</td>
<td>Remote Command Execution (RCE) Attempt: RCE Windows command injection</td>
<td>Remote Command Execution (RCE) Attempt: RCE This rule Detects Windows shell command injections. If you are not running Windows, it is safe to disable this rule.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>932120</td>
<td>Remote Command Execution (RCE) Attempt: RCE Windows PowerShell, cmdlets and options</td>
<td>Remote Command Execution (RCE) Attempt: RCE Detect some common PowerShell commands, cmdlets and options. These commands should be relatively uncommon in normal text, but potentially useful for code injection. If you are not running Windows, it is safe to disable this rule.</td>
</tr>
<tr>
<td>932130</td>
<td>Remote Command Execution (RCE) Attempt: Unix shell expressions</td>
<td>Remote Command Execution (RCE) Attempt: RCE Unix Shell Expression Found. Detects the following patterns which are common in Unix shell scripts and oneliners: Command substitution, Parameter expansion, Process substitution, Arithmetic expansion</td>
</tr>
<tr>
<td>932140</td>
<td>Remote Command Execution (RCE) Attempt: RCE Windows FOR, IF commands</td>
<td>Remote Command Execution (RCE) Attempt: RCE Windows FOR/IF Command Found. This rule Detects Windows command shell FOR and IF commands. If you are not running Windows, it is safe to disable this rule.</td>
</tr>
<tr>
<td>932150</td>
<td>Remote Command Execution (RCE) Attempt: RCE Unix direct remote command execution</td>
<td>Remote Command Execution (RCE) Attempt: RCE Direct Unix Command execution Found. This case is different from command injection (rule 932100), where a command string is appended (injected) to a regular parameter, and then passed to a shell unescaped.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>932180</td>
<td>Restricted File Upload</td>
<td>Detects attempts to upload a file with a forbidden filename. Many applications contain Unrestricted File Upload vulnerabilities. These might be abused to upload configuration files or other files that affect the behavior of the web server, possibly causing remote code execution.</td>
</tr>
<tr>
<td>932190</td>
<td>Remote Command Execution - OS File Access Attempt</td>
<td>A Remote Command Execution (RCE) could be exploited bypassing rule 93012032 (OS File Access Attempt) by using wildcard characters. Keep in mind that this rule could lead to many false positives.</td>
</tr>
<tr>
<td>933100</td>
<td>PHP Injection Attacks: PHP Open Tag Found</td>
<td>PHP Injection Attacks: Detects PHP open tags &quot;&lt;?&quot; and &quot;&lt;?php&quot;. Also Detects &quot;[php]&quot;, &quot;/[php]&quot; and &quot;/[php]&quot; tags used by some applications to indicate PHP dynamic content.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>933110</td>
<td>PHP Injection Attacks: PHP Script Uploads</td>
<td>Block file uploads with PHP extensions (.php, .php5, .phtml and so on), also block files with just dot (.) characters after the extension. Many application contain Unrestricted File Upload vulnerabilities. Attackers may use such a vulnerability to achieve remote code execution by uploading a .php file. Some AJAX uploaders use the nonstandard request headers X-Filename, X_Filename, or X-File-Name to transmit the file name to the server; scan these request headers as well as multipart/form-data file names.</td>
</tr>
<tr>
<td>933111</td>
<td>PHP Injection Attacks: PHP Script Uploads: Superfluous extension</td>
<td>Block file uploads with PHP extensions (.php, .php5, .phtml and so on) anywhere in the name, followed by a dot.</td>
</tr>
<tr>
<td>933120</td>
<td>PHP Injection Attacks: PHP Configuration Directives</td>
<td>PHP Injection Attacks: Configuration Directive Found</td>
</tr>
<tr>
<td>933130</td>
<td>PHP Injection Attacks: PHP Variables</td>
<td>PHP Injection Attacks: Variables Found</td>
</tr>
<tr>
<td>933131</td>
<td>PHP Injection Attacks: PHP Variables - Common Variable Indexes</td>
<td>PHP Injection Attacks: Common Variable Indexes</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>933140</td>
<td>PHP Injection Attacks: PHP I/O Streams</td>
<td>PHP Injection Attacks: Variables Found. The &quot;php://&quot; syntax can be used to refer to various objects, such as local files (for LFI), remote urls (for RFI), or standard input/request body. Its occurrence indicates a possible attempt to either inject PHP code or exploit a file inclusion vulnerability in a PHP web app.</td>
</tr>
<tr>
<td>933150</td>
<td>PHP Injection Attacks: High-Risk PHP Function Names</td>
<td>PHP Injection Attacks: High-Risk PHP Function Names, Approx. 40 words highly common to PHP injection payloads and extremely rare in natural language or other contexts. Examples: 'base64_decode', 'file_get_contents'.</td>
</tr>
<tr>
<td>933151</td>
<td>PHP Injection Attacks: Medium-Risk PHP Function Names</td>
<td>PHP Injection Attacks: Medium-Risk PHP Function Names, Medium-Risk PHP injection payloads and extremely rare in natural language or other contexts.</td>
</tr>
<tr>
<td>933160</td>
<td>PHP Injection Attacks: High-Risk PHP Function Calls</td>
<td>PHP Injection Attacks: High-Risk PHP Function Calls, some PHP function names have a certain risk of false positives, due to short names, full or partial overlap with common natural language terms, uses in other contexts, and so on. Some examples are 'eval', 'exec', and 'system'.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>933161</td>
<td>PHP Injection Attacks: PHP Functions - Low-Value PHP Function Calls</td>
<td>Most of these function names are likely to cause false positives in natural text or common parameter values, such as 'abs', 'copy', 'date', 'key', 'max', 'min'. Therefore, these function names are not to be used if high false positives are expected.</td>
</tr>
<tr>
<td>933170</td>
<td>PHP Injection Attacks: PHP Object Injection</td>
<td>PHP Injection Attacks: PHP Object Injection, is an application level vulnerability that could allow an attacker to perform different kinds of malicious attacks, such as Code Injection, SQL Injection, Path Traversal and Application Denial of Service, depending on the context. The vulnerability occurs when user-supplied input is not properly sanitized before being passed to the unserialize() PHP function.</td>
</tr>
<tr>
<td>933180</td>
<td>PHP Injection Attacks: PHP Functions - Variable Function Calls</td>
<td>PHP Injection Attacks: PHP Functions - Variable Function Calls, PHP 'variable functions' provide an alternate syntax for calling PHP functions. An attacker may use variable function syntax to evade detection of function names during exploitation of a remote code execution vulnerability.</td>
</tr>
<tr>
<td>933190</td>
<td>PHP Injection Attacks: PHP Closing Tag Found</td>
<td>PHP Injection Attacks: PHP Closing Tag Found.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>933200</td>
<td>PHP Injection Attacks: PHP Wrappers</td>
<td>PHP Injection Attacks: PHP Wrappers, PHP comes with many built-in wrappers for various URL-style protocols for use with the filesystem functions such as fopen(), copy(), file_exists() and filesize(). Abusing of PHP wrappers like phar://, zlib://, glob://, rar://, zip://, and so on... could lead to LFI and expect:// to RCE.</td>
</tr>
<tr>
<td>933210</td>
<td>PHP Injection Attacks: PHP Functions - Variable Function Prevent Bypass</td>
<td>PHP Injection Attacks: PHP Functions - Variable Function Calls. This rule blocks bypass filter payloads.</td>
</tr>
<tr>
<td>941100</td>
<td>Cross-Site Scripting (XSS) Attempt: Libinjection - XSS Detection</td>
<td>Cross-Site Scripting (XSS) Attempt: Detects XSS Libinjection</td>
</tr>
<tr>
<td>941101</td>
<td>Cross-Site Scripting (XSS) Attempt: SS Attack Detected via libinjection</td>
<td>Cross-Site Scripting (XSS) Attempt: SS Attack Detected via libinjection</td>
</tr>
<tr>
<td>941110</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 1</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 1. Script tag based XSS vectors, e.g., <code>&lt;script&gt;alert(1)&lt;/script&gt;</code></td>
</tr>
<tr>
<td>941120</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 2</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 2. XSS vectors making use of event handlers like onerror, onload and so on, e.g., <code>&lt;body onload=&quot;alert(1)&quot;&gt;</code></td>
</tr>
<tr>
<td>941130</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 3</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 3. XSS vectors making use of Attribute Vectors</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>941140</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4. XSS vectors making use of javascript URI and tags, e.g., <code>&lt;p style=&quot;background:url(javascript:alert(1))&quot;&gt;</code></td>
</tr>
<tr>
<td>941150</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5. HTML attributes - <code>src</code>, <code>style</code>, and <code>href</code></td>
</tr>
<tr>
<td>941180</td>
<td>Cross-Site Scripting (XSS) Attempt: Blacklist Keywords from Node-Validator</td>
<td>Cross-Site Scripting (XSS) Attempt: Blacklist Keywords from Node-Validator</td>
</tr>
<tr>
<td>941190</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941200</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941210</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941220</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941230</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941240</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941250</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>941260</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941270</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941280</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941290</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941300</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941320</td>
<td>Cross-Site Scripting (XSS) Attempt: HTML Tag Handler</td>
<td>Cross-Site Scripting (XSS) Attempt: HTML Tag Handler</td>
</tr>
<tr>
<td>941330</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941340</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>941350</td>
<td>Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE</td>
<td>Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>942100</td>
<td>SQL Injection (SQLi) Libinjection Detection</td>
<td>SQL Injection (SQLi) Attempt: SQLi Filters via libinjection.</td>
</tr>
<tr>
<td>942101</td>
<td>SQL Injection (SQLi) Libinjection</td>
<td>SQL Injection (SQLi) Attempt: Detects SQLi using libinjection.</td>
</tr>
<tr>
<td>942120</td>
<td>SQL Injection (SQLi) SQL operators</td>
<td>SQL Injection (SQLi) Attempt: SQL operators detection also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>942130</td>
<td>SQL Injection (SQLi) SQL Tautologies</td>
<td>SQL Injection (SQLi) Attempt: SQL Tautologies detection</td>
</tr>
<tr>
<td>942140</td>
<td>SQL Injection (SQLi) Detect DB Names</td>
<td>SQL Injection (SQLi) Attempt: SQLi Filters via DB Names</td>
</tr>
<tr>
<td>942150</td>
<td>SQL Injection (SQLi) SQL Function Names</td>
<td>SQL Injection (SQLi) Attempt: SQL Function Names detection also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>942160</td>
<td>SQL Injection (SQLi) PHPIDS SQLi Filters</td>
<td>SQL Injection (SQLi) Attempt: SQLi Filters via PHPIDS.</td>
</tr>
<tr>
<td>942170</td>
<td>SQL Injection (SQLi) SQL benchmark and sleep injections</td>
<td>SQL Injection (SQLi) Attempt: SQL benchmark and sleep injection detection.</td>
</tr>
<tr>
<td>942180</td>
<td>SQL Injection (SQLi) Basic SQL auth bypass</td>
<td>SQL Injection (SQLi) Attempt: Basic SQL authentication bypass detection.</td>
</tr>
<tr>
<td>942190</td>
<td>SQL Injection (SQLi) MSSQL code execution and info gathering</td>
<td>SQL Injection (SQLi) Attempt: MSSQL code execution and info gathering detection.</td>
</tr>
<tr>
<td>942200</td>
<td>SQL Injection (SQLi) MySQL comment/-space-obfuscated injections and backtick termination</td>
<td>SQL Injection (SQLi) Attempt: MySQL comment/-space-obfuscated injections and backtick termination detection.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>942210</td>
<td>SQL Injection (SQLi) chained SQL injection attempts</td>
<td>SQL Injection (SQLi) Attempt: chained SQL injection attempts detection.</td>
</tr>
<tr>
<td>942220</td>
<td>SQL Injection (SQLi) Integer overflow attacks</td>
<td>SQL Injection (SQLi) Attempt: Integer Overflow attack detection.</td>
</tr>
<tr>
<td>942230</td>
<td>SQL Injection (SQLi) Conditional SQL injections</td>
<td>SQL Injection (SQLi) Attempt: Conditional SQL injection detection.</td>
</tr>
<tr>
<td>942240</td>
<td>SQL Injection (SQLi) MYSQL charset/ MSSQL DOS</td>
<td>SQL Injection (SQLi) Attempt: MYSQL charset/ MSSQL DOS detection.</td>
</tr>
<tr>
<td>942251</td>
<td>SQL Injection (SQLi) SQL HAVING queries</td>
<td>SQL Injection (SQLi) Attempt: Detects SQL HAVING queries.</td>
</tr>
<tr>
<td>942260</td>
<td>SQL Injection (SQLi) basic SQL auth bypass</td>
<td>SQL Injection (SQLi) Attempt: basic SQL authentication bypass detection.</td>
</tr>
<tr>
<td>942270</td>
<td>SQL Injection (SQLi) Common SQLi attacks for various dbs</td>
<td>SQL Injection (SQLi) Attempt: Common attacks against msql, oracle, and other dbs detection.</td>
</tr>
<tr>
<td>942280</td>
<td>SQL Injection (SQLi) pg_sleep injection/ waitfor delay/ database shutdown</td>
<td>SQL Injection (SQLi) Attempt: pg_sleep injection/ waitfor delay attack/ database shutdown detection.</td>
</tr>
<tr>
<td>942290</td>
<td>SQL Injection (SQLi) MongoDB SQLLi</td>
<td>SQL Injection (SQLi) Attempt: MongoDB SQL injection detection.</td>
</tr>
<tr>
<td>942300</td>
<td>SQL Injection (SQLi) MySQL comments, conditions and ch(a)r injections</td>
<td>SQL Injection (SQLi) Attempt: MySQL comments, conditions and ch(a)r injections detection.</td>
</tr>
<tr>
<td>942310</td>
<td>SQL Injection (SQLi) chained SQL injection</td>
<td>SQL Injection (SQLi) Attempt: chained SQL injection detection.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>942320</td>
<td>SQL Injection (SQLi) MYSQL/PostgreSQL stored procedure and function injection</td>
<td>SQL Injection (SQLi) Attempt: MYSQL/PostgreSQL stored procedure and function injection detection.</td>
</tr>
<tr>
<td>942330</td>
<td>SQL Injection (SQLi) classic SQL injection probings</td>
<td>SQL Injection (SQLi) Attempt: classic SQL injection probings detection.</td>
</tr>
<tr>
<td>942340</td>
<td>SQL Injection (SQLi) basic SQL auth bypass attempts</td>
<td>SQL Injection (SQLi) Attempt: basic SQL authentication bypass attempts detection.</td>
</tr>
<tr>
<td>942350</td>
<td>SQL Injection (SQLi) MYSQL UDF/data structure manipulation</td>
<td>SQL Injection (SQLi) Attempt: MYSQL UDF/data structure manipulation detection.</td>
</tr>
<tr>
<td>942360</td>
<td>SQL Injection (SQLi) Concatenated SQLi and SQLLFI</td>
<td>SQL Injection (SQLi) Attempt: Concatenated SQLi and SQLLFI detection.</td>
</tr>
<tr>
<td>942361</td>
<td>SQL Injection (SQLi) basic SQL injection based on keyword alter or union</td>
<td>SQL Injection (SQLi) Attempt: basic SQL injection based on keyword alter or union detection.</td>
</tr>
<tr>
<td>942370</td>
<td>SQL Injection (SQLi) classic SQL injection probings</td>
<td>SQL Injection (SQLi) Attempt: classic SQL injection probings detection also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>942380</td>
<td>SQL Injection (SQLi) SQL injection</td>
<td>SQL Injection (SQLi) Attempt: SQL injection detection.</td>
</tr>
<tr>
<td>942390</td>
<td>SQL Injection (SQLi) SQL injection</td>
<td>SQL Injection (SQLi) Attempt: SQL injection detection.</td>
</tr>
<tr>
<td>942400</td>
<td>SQL Injection (SQLi) SQL injection</td>
<td>SQL Injection (SQLi) Attempt: SQL injection detection.</td>
</tr>
<tr>
<td>942410</td>
<td>SQL Injection (SQLi) SQL injection</td>
<td>SQL Injection (SQLi) Attempt: SQL injection detection also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>942420</td>
<td>SQL Injection (SQLi) SQL Injection Character Anomaly Usage</td>
<td>SQL Injection (SQLi) Attempt: Detects when there is an excessive use of meta-characters within a single parameter payload.</td>
</tr>
<tr>
<td>942421</td>
<td>SQL Injection (SQLi) SQL Injection Character Anomaly Usage</td>
<td>SQL Injection (SQLi) Attempt: Detects SQL Injection Character Anomaly Usage.</td>
</tr>
<tr>
<td>942430</td>
<td>SQL Injection (SQLi) Restricted SQL Character Anomaly Detection</td>
<td>SQL Injection (SQLi) Attempt: This rule attempts to gauge when there is an excessive use of meta-characters within a single parameter payload. Also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>942431</td>
<td>SQL Injection (SQLi) Restricted SQL Character Anomaly Detection</td>
<td>SQL Injection (SQLi) Attempt: Restricted SQL Character Anomaly Detection also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>942432</td>
<td>SQL Injection (SQLi) Restricted SQL Character Anomaly Detection</td>
<td>SQL Injection (SQLi) Attempt: Restricted SQL Character Anomaly Detection also detects CVE-2018-2380.</td>
</tr>
<tr>
<td>942440</td>
<td>SQL Injection (SQLi) SQL Comment Sequence</td>
<td>SQL Injection (SQLi) Attempt: Detects SQL Comment Sequence.</td>
</tr>
<tr>
<td>942450</td>
<td>SQL Injection (SQLi) SQL Hex Evasion Methods</td>
<td>SQL Injection (SQLi) Attempt: Detects SQL Hex Evasion Methods.</td>
</tr>
<tr>
<td>942460</td>
<td>SQL Injection (SQLi) Repetitive Non-Word Characters</td>
<td>SQL Injection (SQLi) Attempt: Detects when multiple (4 or more) non-word characters are repeated in sequence.</td>
</tr>
<tr>
<td>942470</td>
<td>SQL Injection (SQLi) SQL injection</td>
<td>SQL Injection (SQLi) Attempt: SQL injection detection.</td>
</tr>
<tr>
<td>942480</td>
<td>SQL Injection (SQLi) SQL injection</td>
<td>SQL Injection (SQLi) Attempt: SQL injection detection.</td>
</tr>
<tr>
<td>942490</td>
<td>SQL Injection (SQLi) classic SQL injection probings</td>
<td>SQL Injection (SQLi) Attempt: Detects classic SQL injection probings.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>942500</td>
<td>SQL Injection (SQLi) in-line comments</td>
<td>SQL Injection (SQLi) Attempt: In-line comments detection.</td>
</tr>
<tr>
<td>942510</td>
<td>SQL Injection (SQLi) SQLi bypass: backticks</td>
<td>SQL Injection (SQLi) Attempt: Detects quotes and backticks can be used to bypass SQLi detection.</td>
</tr>
<tr>
<td>942511</td>
<td>SQL Injection (SQLi) SQLi bypass: quotes</td>
<td>SQL Injection (SQLi) Attempt: Detects quotes and backticks which can be used to bypass filters.</td>
</tr>
<tr>
<td>943100</td>
<td>Session Fixation cookie in HTML</td>
<td>Detects Cookie Values in HTML which could be a session fixation attack</td>
</tr>
<tr>
<td>943110</td>
<td>Session Fixation Off-Domain Referrer in SessionID</td>
<td>Detects SessionID Parameter Name with Off-Domain Referrer</td>
</tr>
<tr>
<td>943120</td>
<td>Session Fixation No Referrer in SessionID</td>
<td>Detects SessionID Parameter Name with No Referrer</td>
</tr>
<tr>
<td>944100</td>
<td>Java attack Attempt: Apache Struts and Oracle WebLogic vulnerabilities</td>
<td>Java attack Attempt: Apache Struts and Oracle WebLogic vulnerabilities</td>
</tr>
<tr>
<td>944110, 944120</td>
<td>Java attack Attempt: Apache Struts and Oracle WebLogic vulnerabilities and detect processbuilder or runtime calls</td>
<td>Java attack Attempt: Apache Struts and Oracle WebLogic vulnerabilities, Java deserialization</td>
</tr>
<tr>
<td>944130</td>
<td>Java attack Attempt: Apache Struts and Oracle WebLogic vulnerabilities</td>
<td>Java attack Attempt: Apache Struts and Oracle WebLogic vulnerabilities</td>
</tr>
<tr>
<td>944200</td>
<td>Java attack Attempt: Detect exploitation of &quot;Java deserialization&quot; Apache Commons</td>
<td>Java attack Attempt: Detect exploitation of &quot;Java deserialization&quot; Apache Commons</td>
</tr>
<tr>
<td>944210</td>
<td>Java attack Attempt: Detecting possibe base64 text to match encoded magic bytes \xac\xed\x00\x05 with padding encoded in base64 strings are r00ABQ KztAAU Cs7QAF</td>
<td>Java attack Attempt: Detecting possibe base64 text to match encoded magic bytes \xac\xed\x00\x05 with padding encoded in base64 strings are r00ABQ KztAAU Cs7QAF</td>
</tr>
<tr>
<td>944240</td>
<td>Java attack Attempt: Remote Command Execution: Java serialization</td>
<td>Java attack Attempt: Remote Command Execution: Java serialization</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>944300</td>
<td>Java attack Attempt: Interesting keywords for possibly RCE on vulnerable classes and methods base64 encoded</td>
<td>Java attack Attempt: Interesting keywords for possibly RCE on vulnerable classes and methods base64 encoded</td>
</tr>
<tr>
<td>950001, 959070, 959071, 959072, 95908, 959073</td>
<td>Common SQL Injections</td>
<td>Detects common SQL injection attacks</td>
</tr>
<tr>
<td>950002</td>
<td>Common system command access attempt</td>
<td>Detect access attempts to common system commands, such as map, telnet, ftp, rcmd, and cmd.</td>
</tr>
<tr>
<td>950005</td>
<td>Common system files access attempt</td>
<td>Detects access attempts to common system files, such as access, passwd, groupm global.asa, httpd.conf, boot.ini, /and so on.</td>
</tr>
<tr>
<td>950006</td>
<td>Injection for common system commands</td>
<td>Detects injections for common system commands such as telnet, map, blocalgroup, ftp, rcmd, echo, cmd, chmod, passwd, and mail.</td>
</tr>
<tr>
<td>950007</td>
<td>Blind SQL injection</td>
<td>Detects common blind SQL injection attacks.</td>
</tr>
<tr>
<td>950008</td>
<td>ColdFusion Admin Functions Injection</td>
<td>Detects injection of ColdFusion undocumented admin functions.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>950009, 950003, 950000</td>
<td>Session fixation</td>
<td>Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to &quot;fix&quot; the session ID value. These techniques range from Cross-site Scripting exploits to peppering the web site with previously made HTTP requests. After a user's session ID has been fixed, the attacker will wait for that user to login. Once the user does so, the attacker uses the predefined session ID value to assume the same online identity.</td>
</tr>
<tr>
<td>950010</td>
<td>LDAP Injection</td>
<td>Detects common LDAP data constructions injections.</td>
</tr>
<tr>
<td>950011</td>
<td>SSI Injection</td>
<td>Detects common Server-Side-Include format data injections.</td>
</tr>
<tr>
<td>950012</td>
<td>HTTP Request Smuggling</td>
<td>Detects specially crafted requests that under certain circumstances could be seen by the attacked entities as two different sets of requests. This allows certain requests to be smuggled through to a second entity without the first one realizing it.</td>
</tr>
<tr>
<td>950018</td>
<td>UPDF XSS Injection</td>
<td>Detects submitted links that contains the # fragment in a query_string.</td>
</tr>
<tr>
<td>950019</td>
<td>Email Injection</td>
<td>Detects mail command Injections targeting mail servers and webmail applications that construct IMAP/SMTP statements from user-supplied input that is not properly sanitized.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>950103</td>
<td>Path/directory traversal</td>
<td>Detects path traversal attempts, also known as directory traversal or &quot;/../&quot; attacks.</td>
</tr>
<tr>
<td>950107, 950109, 950108</td>
<td>URL Encodings Validation</td>
<td>Detects URL encoding inconsistencies, encoding abuse and invalid formatting.</td>
</tr>
<tr>
<td>950110, 950921, 950922</td>
<td>Trojan, Backdoor and Webshell Access Attempts</td>
<td>Detects when an attacker attempts to access trojan, backdoor or webshell web page.</td>
</tr>
<tr>
<td>950116</td>
<td>Unicode Encoding/Decoding Validation</td>
<td>Blocks full-width Unicode encoding as decoding evasions could be possible.</td>
</tr>
<tr>
<td>950117</td>
<td>URL Contains an IP Address</td>
<td>Detects a common RFI attack, when URL contains an IP address.</td>
</tr>
<tr>
<td>950118</td>
<td>PHP include() function</td>
<td>Detects a common RFI php include() function attacks.</td>
</tr>
<tr>
<td>950119</td>
<td>Data ends with question mark(s) (?)</td>
<td>Detects a common RFI attack, when data ends with question mark(s) (?).</td>
</tr>
<tr>
<td>950120</td>
<td>Host doesn't match localhost</td>
<td>Detects a common RFI attack, when Host Doesn't Match Local Host.</td>
</tr>
<tr>
<td>950801</td>
<td>UTF Encoding Validation</td>
<td>Detects UTF encoding inconsistencies and invalid formatting.</td>
</tr>
<tr>
<td>950901</td>
<td>SQL Tautologies</td>
<td>Detects common SQL tautologies attacks.</td>
</tr>
<tr>
<td>950907</td>
<td>OS Command Injection</td>
<td>Detects OS command injection in an application to elevate privileges, execute arbitrary commands, compromise the underlying operating system and install malicious toolkits such as those to participate in botnet attacks.</td>
</tr>
<tr>
<td>950910, 950911</td>
<td>HTTP Response Splitting</td>
<td>Detects Carriage Return + Linefeed characters in the response header that could cause attacked entities to interpret it as two separate responses instead of one.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958000</td>
<td>addimport XSS attack</td>
<td>Detects usage of addimport in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958001</td>
<td>document cookie XSS attack</td>
<td>Detects usage of document.cookie in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958002</td>
<td>execscript XSS attack</td>
<td>Detects usage of execscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958003</td>
<td>fromcharcode XSS attack</td>
<td>Detects usage of fromcharcode in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958004</td>
<td>innerhtml XSS attack</td>
<td>Detects usage of innerhtml in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958005</td>
<td>cdata XSS attack</td>
<td>Detects usage of cdata in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958006</td>
<td>body background XSS attack</td>
<td>Detects usage of &lt;body background in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958007</td>
<td>onload XSS attack</td>
<td>Detects usage of onload in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958008</td>
<td>input type image XSS attack</td>
<td>Detects usage of &lt;input type image in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958009</td>
<td>import XSS attack</td>
<td>Detects usage of import in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958010</td>
<td>activexobject XSS attack</td>
<td>Detects usage of activexobject in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958011</td>
<td>background-image: XSS attack</td>
<td>Detects usage of background-image: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958012</td>
<td>copyparentfolder XSS attack</td>
<td>Detects usage of copyparentfolder in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958013</td>
<td>createtextrange XSS attack</td>
<td>Detects usage of createtextrange in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>958016</td>
<td>getparentfolder XSS attack</td>
<td>Detects usage of getparentfolder in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958017</td>
<td>getspecialfolder XSS attack</td>
<td>Detects usage of getspecialfolder in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958018</td>
<td>href javascript: XSS attack</td>
<td>Detects usage of href javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958019</td>
<td>href schell XSS attack</td>
<td>Detects usage of href schell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958020</td>
<td>href vbscript: XSS attack</td>
<td>Detects usage of href vbscript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958022</td>
<td>livescript: XSS attack</td>
<td>Detects usage of livescript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958023</td>
<td>lowsrmjavascript: XSS attack</td>
<td>Detects usage of lowsrmjavascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958024</td>
<td>lowsrmshell XSS attack</td>
<td>Detects usage of lowsrmshell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958025</td>
<td>lowsrmvbscript XSS attack</td>
<td>Detects usage of lowsrmvbscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958026</td>
<td>mocha: XSS attack</td>
<td>Detects usage of mocha: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958027</td>
<td>onabort XSS attack</td>
<td>Detects usage of onabort in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958028</td>
<td>settimeout XSS attack</td>
<td>Detects usage of settimeout in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958030</td>
<td>src http: XSS attack</td>
<td>Detects usage of src http: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958031</td>
<td>javascript: XSS attack</td>
<td>Detects usage of javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958032</td>
<td>src and shell XSS attack</td>
<td>Detects usage of src and shell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958033</td>
<td>vbscript: XSS attack</td>
<td>Detects usage of vbscript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958034</td>
<td>style bexpession XSS attack</td>
<td>Detects usage of style bexpession in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958036</td>
<td>type application x-javascript XSS attack</td>
<td>Detects usage of type application x-javascript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958037</td>
<td>type application x-vbscript XSS attack</td>
<td>Detects usage of type application x-vbscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958038</td>
<td>type text ecmascript XSS attack</td>
<td>Detects usage of type text ecmascript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958039</td>
<td>type text javascript XSS attack</td>
<td>Detects usage of type text javascript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958040</td>
<td>type text jscript XSS attack</td>
<td>Detects usage of type text jscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958041</td>
<td>type text vbscript XSS attack</td>
<td>Detects usage of type text vbscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958045</td>
<td>url javascript: XSS attack</td>
<td>Detects usage of url javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958046</td>
<td>url shell XSS attack</td>
<td>Detects usage of &lt;url shell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958047</td>
<td>url vbscript: XSS attack</td>
<td>Detects usage of url vbscript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958049</td>
<td>?meta XSS attack</td>
<td>Detects usage of ?meta in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958051</td>
<td>?script XSS attack</td>
<td>Detects usage of &lt; ?script in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958052</td>
<td>alert XSS attack</td>
<td>Detects usage of alert in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>958054</td>
<td>lowsrc and http: XSS attack</td>
<td>Detects usage of lowsrc and http: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958056</td>
<td>iframe src XSS attack</td>
<td>Detects usage of iframe src in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958057</td>
<td>?iframe XSS attack</td>
<td>Detects usage of ?iframe in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958059</td>
<td>asfunction: XSS attack</td>
<td>Detects usage of asfunction: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958295</td>
<td>Connection Header Validation</td>
<td>Detects connection header inconsistencies and invalid formatting</td>
</tr>
<tr>
<td>958404</td>
<td>onerror XSS attack</td>
<td>Detects usage of onerror in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958405</td>
<td>onblur XSS attack</td>
<td>Detects usage of onblur in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958406</td>
<td>onchange XSS attack</td>
<td>Detects usage of onchange in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958407</td>
<td>onclick XSS attack</td>
<td>Detects usage of onclick in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958408</td>
<td>ondragdrop XSS attack</td>
<td>Detects usage of ondragdrop in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958409</td>
<td>onfocus XSS attack</td>
<td>Detects usage of onfocus in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958410</td>
<td>onkeydown XSS attack</td>
<td>Detects usage of onkeydown in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958411</td>
<td>onkeypress XSS attack</td>
<td>Detects usage of onkeypress in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958412</td>
<td>onkeyup XSS attack</td>
<td>Detects usage of onkeyup in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958413</td>
<td>onload XSS attack</td>
<td>Detects usage of onload in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958414</td>
<td>onmousedown XSS attack</td>
<td>Detects usage of onmousedown in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958415</td>
<td>onmousemove XSS attack</td>
<td>Detects usage of onmousemove in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958416</td>
<td>bonmouseout XSS attack</td>
<td>Detects usage of bonmouseout in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958417</td>
<td>bonmouseover XSS attack</td>
<td>Detects usage of bonmouseover in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958418</td>
<td>onmouseup XSS attack</td>
<td>Detects usage of onmouseup in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958419</td>
<td>onmove XSS attack</td>
<td>Detects usage of onmove in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958420</td>
<td>onresize XSS attack</td>
<td>Detects usage of onresize in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958421</td>
<td>onselect XSS attack</td>
<td>Detects usage of onselect in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958422</td>
<td>onsubmit XSS attack</td>
<td>Detects usage of onsubmit in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958423</td>
<td>onunload XSS attack</td>
<td>Detects usage of onunload in request, cookies, or arguments.</td>
</tr>
<tr>
<td>959151, 958976, 958977</td>
<td>php code injection</td>
<td>Detects a common injections attack, when request contain any php code e.g. &quot;&lt;?&gt;&quot;</td>
</tr>
<tr>
<td>960000</td>
<td>File Name Validation</td>
<td>Detects multipart/form-data file name evasion attempts.</td>
</tr>
<tr>
<td>960007, 960008</td>
<td>Missing Host Header</td>
<td>Detects missing request host header.</td>
</tr>
<tr>
<td>960009, 960006</td>
<td>Missing User-Agent Header</td>
<td>Detects missing request user-agent header.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>960010</td>
<td>Restrict HTTP Content Types</td>
<td>Allows only such content types as: application/x-www-form-urlencoded, multipart/form-data, text/xml, application/xml, application/x-amf, application/json</td>
</tr>
<tr>
<td>960011</td>
<td>GET/HEAD Requests Validation</td>
<td>Detects if GET/HEAD requests contain request body, since it is not a common practice.</td>
</tr>
<tr>
<td>960012</td>
<td>Content-Length Header Validation</td>
<td>Detects if content-length header is provided with every POST request.</td>
</tr>
<tr>
<td>960013</td>
<td>Require Content-Length to be provided with every HTTP/1.1 POST request that has no Transfer-Encoding header</td>
<td>Detect HTTP/1.1 request that do not comply with HTTP 1.1 spec by having no Content-Length header when Transfer-Encoding header is also absent.</td>
</tr>
<tr>
<td>960014</td>
<td>URI Validation</td>
<td>Ensures that URI and canonical server name are matching.</td>
</tr>
<tr>
<td>960015, 960021</td>
<td>Missing Accept Header</td>
<td>Detects missing request accept header.</td>
</tr>
<tr>
<td>960016</td>
<td>Content-Length Header Validation</td>
<td>Detects if content-length HTTP header is not numeric.</td>
</tr>
<tr>
<td>960017</td>
<td>Host Header Is IP Address</td>
<td>Detects if host header is a numeric IP address as it could be an indicative of automated client access.</td>
</tr>
<tr>
<td>960020</td>
<td>Pragma Header Validation</td>
<td>Ensures that pragma, cache-control headers and HTTP protocol version supplied by the client are matching.</td>
</tr>
<tr>
<td>960022</td>
<td>Expect Header Validation</td>
<td>Ensures that expect header and HTTP protocol version supplied by the client are matching.</td>
</tr>
<tr>
<td>960024</td>
<td>Repeatative Non-Word Chars</td>
<td>Attempts to identify when four or more non-word characters are repeated in sequence.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>960032</td>
<td>Restrict HTTP Request Methods</td>
<td>Allows only request methods specified by the configurable &quot;Allowed http methods&quot; parameter.</td>
</tr>
<tr>
<td>960034</td>
<td>Restrict HTTP Protocol Versions</td>
<td>Allows only HTTP protocol versions HTTP/1.0 and HTTP/1.1.</td>
</tr>
<tr>
<td>960208</td>
<td>Values Limits</td>
<td>Detects HTTP requests with value length exceeding the configurable &quot;Max length of argument&quot; parameter.</td>
</tr>
<tr>
<td>960209</td>
<td>Arguments Limits</td>
<td>Detects HTTP requests with argument name length exceeding the 100 symbols.</td>
</tr>
<tr>
<td>960335</td>
<td>Number of Arguments Limits</td>
<td>Detects HTTP requests with number of arguments exceeding the configurable &quot;Max amount of arguments&quot; value.</td>
</tr>
<tr>
<td>960341</td>
<td>Total Arguments Limits</td>
<td>Detects HTTP requests with total length of all arguments exceeding the configurable &quot;Max total argument length&quot; parameter.</td>
</tr>
<tr>
<td>960901, 960018</td>
<td>Character Set Validation</td>
<td>Ensures that only specific character set(s) is used.</td>
</tr>
<tr>
<td>960902</td>
<td>Content-Encoding Header Validation</td>
<td>Ensures that identity is not specified in content-encoding header.</td>
</tr>
<tr>
<td>960904</td>
<td>Missing Content-Type Header</td>
<td>Detects missing content-type header or if combination of content-length and content-type headers is invalid.</td>
</tr>
<tr>
<td>960911</td>
<td>Request Line Format Validation against the HTTP RFC</td>
<td>Uses rule negation against the regex for positive security. The regex specifies the proper construction of URI request lines such as: &quot;http: &quot;/&quot;&quot; host [ &quot;:&quot; port ] [ abs_path [ &quot;?&quot; query ]]. It also outlines proper construction for CONNECT, OPTIONS and GET requests.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>960912</td>
<td>Malformed request bodies</td>
<td>Checks for Request body parsing errors.</td>
</tr>
<tr>
<td>960914</td>
<td>Strict Multipart Parsing Checks</td>
<td>By default be strict with what we accept in the multipart/form-data request body. If the rule below proves to be too strict for your environment, consider changing it to Off.</td>
</tr>
<tr>
<td>960915</td>
<td>Multipart Unmatched Boundary Check</td>
<td>Checks for signs of evasions during file upload requests.</td>
</tr>
<tr>
<td>970002</td>
<td>Statistics pages information leakage</td>
<td>Detects statistics pages information leakage.</td>
</tr>
<tr>
<td>970003</td>
<td>SQL errors information leakage</td>
<td>Detects SQL errors information leakage.</td>
</tr>
<tr>
<td>970004, 970904</td>
<td>IIS errors information leakage</td>
<td>Detects IIS errors information leakage.</td>
</tr>
<tr>
<td>970007</td>
<td>Zope information leakage</td>
<td>Detects Zope information leakage.</td>
</tr>
<tr>
<td>970008</td>
<td>ColdFusion information leakage</td>
<td>Detects ColdFusion information leakage.</td>
</tr>
<tr>
<td>970009</td>
<td>PHP information leakage</td>
<td>Detects PHP information leakage.</td>
</tr>
<tr>
<td>970010</td>
<td>ISA server existence revealed</td>
<td>Detects if ISA server existence revealed.</td>
</tr>
<tr>
<td>970011</td>
<td>File and/or directory names leakage</td>
<td>Detects file and/or directory names leakage.</td>
</tr>
<tr>
<td>970012, 970903</td>
<td>MS Office document properties leakage</td>
<td>Detects MS Office document properties leakage.</td>
</tr>
<tr>
<td>970013</td>
<td>Directory listing information leakage</td>
<td>Detects directory listing information leakage.</td>
</tr>
<tr>
<td>970014</td>
<td>ASP/JSP source code leakage</td>
<td>Detects ASP/JSP source code leakage.</td>
</tr>
<tr>
<td>970015, 970902</td>
<td>PHP source code leakage</td>
<td>Detects PHP source code leakage.</td>
</tr>
<tr>
<td>970016</td>
<td>ColdFusion source code leakage</td>
<td>Detects ColdFusion source code leakage.</td>
</tr>
<tr>
<td>970018</td>
<td>IIS default location revealed</td>
<td>Detects if IIS default location revealed.</td>
</tr>
<tr>
<td>970021</td>
<td>Weblogic information leakage</td>
<td>Detects Weblogic information leakage.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>970118</td>
<td>Microsoft OLE DB Provider Error page leakage</td>
<td>Detects Microsoft OLE DB Provider for SQL Server error page.</td>
</tr>
<tr>
<td>970901</td>
<td>5XX Status code information leakage</td>
<td>Detects if application generates 500-level status code, for example, 500 Internal Server Error, 501 Not Implemented...505 HTTP Version Not Supported.</td>
</tr>
<tr>
<td>973000, 97301, 97302</td>
<td>Common direct HTML injection</td>
<td>Detects tags that are the most common direct HTML injection points.</td>
</tr>
<tr>
<td>97306</td>
<td>Embedding javascript in style attribute</td>
<td>Detects embedding javascript in style attribute.</td>
</tr>
<tr>
<td>97307</td>
<td>Embedded Scripts Within JavaScript Fragments</td>
<td>Detects common JavaScript fragments like fromcharcode, alert, eval that can be used for attacks.</td>
</tr>
<tr>
<td>97309, 97308</td>
<td>CSS Fragments attacks</td>
<td>Detects common CSS fragments attacks like &lt;div style=&quot;background-image: url(javascript:...)&quot;&gt; or &lt;img style=&quot;x:expression(document.write(1))&quot;&gt;</td>
</tr>
<tr>
<td>97310</td>
<td>Embedded Scripts Within Alert Fragments</td>
<td>Detects attacks like alert('xss'), alert(&quot;xss&quot;), alert(/xss/).</td>
</tr>
<tr>
<td>97312</td>
<td>&quot;:!-&quot;&lt;XSS&gt;=&amp;{()} Attacks</td>
<td>Detects &quot;:!-&quot;&lt;XSS&gt;=&amp;{()} attacks.</td>
</tr>
<tr>
<td>97313</td>
<td>&amp;{alert('xss')} attacks</td>
<td>Detects &amp;{alert('xss')} attacks.</td>
</tr>
<tr>
<td>97314</td>
<td>Doctype Entity inject</td>
<td>Detects Doctype Entity inject attacks.</td>
</tr>
<tr>
<td>97331, 973315, 973330, 973327, 973326, 973346, 973345, 973324, 973323, 973322, 973348, 973321, 973320, 973318, 973317, 973347, 973335, 973334, 973333, 973344, 973332, 973329, 973328, 973316, 973325, 973319</td>
<td>Internet Explorer XSS Filters</td>
<td>Detects common IE XSS attacks.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>973336</td>
<td>Embedding Scripts Within Scripts</td>
<td>Detects script tag based XSS vectors, for example, <code>&lt;script&gt; alert(1)&lt;/script&gt;</code>.</td>
</tr>
<tr>
<td>973337, 973303</td>
<td>Embedded Scripts Within Event Handlers</td>
<td>Detects event handler based XSS vectors, for example, <code>&lt;body onload=&quot;alert(1)&quot;&gt;</code>.</td>
</tr>
<tr>
<td>973338, 973304, 973305</td>
<td>Embedded Scripts Within URI Schemes</td>
<td>Detects &quot;data&quot;, &quot;javascript&quot;, &quot;src&quot; or other URI schemes/attributes based XSS vectors, for example, <code>&lt;p style=&quot;background:url(javascript:alert(1))&quot;&gt;</code>.</td>
</tr>
<tr>
<td>981004</td>
<td>Potential Obfuscated Javascript, fromCharCode</td>
<td>Detects excessive fromCharCode Javascript in Output.</td>
</tr>
<tr>
<td>981006</td>
<td>Potential Obfuscated Javascript, Unescape</td>
<td>Detects Potential Unescape in response.</td>
</tr>
<tr>
<td>981078, 9200019, 920005, 920007, 920009, 920011, 920013, 920015, 920017</td>
<td>Credit card leakage in request</td>
<td>Detects primary credit card numbers (Visa, MasterCard, GSA SmartPay, Americal Express, Diners Club, enRoute, Discover, JCB) in user input.</td>
</tr>
<tr>
<td>981080, 920020, 920006, 920008, 920010, 920012, 920014, 920016, 920018</td>
<td>Credit card leakage in response</td>
<td>Detects primary credit card numbers (Visa, MasterCard, GSA SmartPay, Americal Express, Diners Club, enRoute, Discover, JCB) sent from site to user.</td>
</tr>
<tr>
<td>981136</td>
<td>Generic XSS attacks</td>
<td>Detects common XSS attacks embedded within non-script elements, for example, `jscript onsubmit copyparentfolder document javascript meta onchange onmove onkeydown onkeyup.activexobject onerror onmousedown ecmscript bexpression onmouseover vbscript.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>981172, 981173</td>
<td>SQL Character Anomaly Scoring</td>
<td>Attempts to gauge when there is an excessive use of meta-characters within a single parameter payload.</td>
</tr>
<tr>
<td>981177, 981000, 981001, 981003</td>
<td>IFrame Injection</td>
<td>Detects iframe injections that could execute malicious code to steal data, redirect to malware infected sites, load malware, and so on.</td>
</tr>
<tr>
<td>981227</td>
<td>Request URI Validation</td>
<td>Detects invalid URI in request.</td>
</tr>
<tr>
<td>981231</td>
<td>SQL Comment Sequences</td>
<td>Detects common SQL comment sequences, for example, DROP/ <em>comment</em>/sampletable.</td>
</tr>
<tr>
<td>981240</td>
<td>MySQL comments, conditions</td>
<td>Detects MySQL comments, conditions and ch(a)r injections.</td>
</tr>
<tr>
<td>981241</td>
<td>Conditional SQL injection attempts</td>
<td>Detects conditional SQL injection attempts.</td>
</tr>
<tr>
<td>981242, 981243</td>
<td>Classic SQL injection probings</td>
<td>Detects classic SQL injection probings.</td>
</tr>
<tr>
<td>981244, 981245, 981246</td>
<td>SQL authentication bypass attempts</td>
<td>Detects basic SQL authentication bypass attempts.</td>
</tr>
<tr>
<td>981247</td>
<td>Concatenated basic SQL injection and SQLLFI attempts</td>
<td>Detects concatenated basic SQL injection and SQLLFI attempts.</td>
</tr>
<tr>
<td>981248, 981249</td>
<td>Chained SQL injection attempts</td>
<td>Detects chained SQL injection attempts.</td>
</tr>
<tr>
<td>981250</td>
<td>SQL benchmark and sleep injection attempts</td>
<td>Detects SQL benchmark and sleep injection attempts including conditional queries.</td>
</tr>
<tr>
<td>981251</td>
<td>MySQL UDF injection</td>
<td>Detects MySQL UDF injection and other data/ structure manipulation attempts.</td>
</tr>
<tr>
<td>981252</td>
<td>MySQL charset switch and MSSQL DoS attempts</td>
<td>Detects MySQL charset switch and MSSQL DoS attempts.</td>
</tr>
<tr>
<td>981253</td>
<td>MySQL and PostgreSQL stored procedure/function injections</td>
<td>Detects MySQL and PostgreSQL stored procedure/function injections.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>981254</td>
<td>PostgreSQL pg_sleep injection</td>
<td>Detects PostgreSQL pg_sleep injection, waitfor delay attacks and database shutdown attempts.</td>
</tr>
<tr>
<td>981255</td>
<td>MSSQL code execution</td>
<td>Detects MSSQL code execution and information gathering attempts.</td>
</tr>
<tr>
<td>981256</td>
<td>MATCH AGAINST, MERGE, EXECUTE IMMEDIATE and HAVING</td>
<td>Detects MATCH AGAINST, MERGE, EXECUTE IMMEDIATE and HAVING injections.</td>
</tr>
<tr>
<td>981257</td>
<td>MySQL comment-/space-obfuscated</td>
<td>Detects MySQL comment-/space-obfuscated injections and backtick termination.</td>
</tr>
<tr>
<td>981260</td>
<td>SQL Hex Evasion Methods</td>
<td>Detects SQL hex encoding evasion attacks.</td>
</tr>
<tr>
<td>981270</td>
<td>MongoDB SQL injection</td>
<td>Detects basic MongoDB SQL injection attempts.</td>
</tr>
<tr>
<td>981272</td>
<td>SQL injection using sleep() or benchmark()</td>
<td>Detects blind SQL injection tests using sleep() or benchmark() functions.</td>
</tr>
<tr>
<td>981276</td>
<td>Common attack string for mysql, oracle</td>
<td>Detects common attack string for mysql, oracle and others</td>
</tr>
<tr>
<td>981277</td>
<td>Integer overflow attacks</td>
<td>Detects integer overflow attacks.</td>
</tr>
<tr>
<td>981300, 981301, 981302, 981303, 981304, 981305, 981306, 981307, 981308, 981309, 981310, 981311, 981312, 981313, 981314, 981315, 981316, 981317</td>
<td>SQL Keyword Anomaly Scoring</td>
<td>Detects common SQL keywords anomalies.</td>
</tr>
<tr>
<td>981318</td>
<td>String Termination/Statement Ending</td>
<td>Identifies common initial SQLi probing requests where attackers insert/append quote characters to the existing normal payload to see how the app/db responds.</td>
</tr>
<tr>
<td>981319</td>
<td>SQL Operators</td>
<td>Detects common SQL operators injection attacks.</td>
</tr>
<tr>
<td>981320</td>
<td>DB Names</td>
<td>Detects common DB names injection attacks.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1000000, 1000001, 1000002, 1000003, 1000004</td>
<td>Shellshock exploit attempt</td>
<td>Detects the ability to unintentionally execute commands in Bash. CVE-2014-6271</td>
</tr>
<tr>
<td>2100019</td>
<td>/_layouts/scriptresx.ashx sections Parameter XSS</td>
<td>Microsoft SharePoint / _layouts/scriptresx.ashx sections Parameter XSS</td>
</tr>
<tr>
<td>2100023</td>
<td>/owssrv.dll List Parameter XSS</td>
<td>Microsoft SharePoint / owssrv.dll List Parameter XSS</td>
</tr>
<tr>
<td>2100026</td>
<td>_layouts/Chart/WebUI/WizardList.aspx skey Parameter XSS</td>
<td>Microsoft SharePoint _layouts/Chart/WebUI/WizardList.aspx skey Parameter XSS</td>
</tr>
<tr>
<td>2100027</td>
<td>_layouts/themeweb.aspx XSS</td>
<td>Microsoft SharePoint _layouts/themeweb.aspx XSS</td>
</tr>
<tr>
<td>2100028</td>
<td>_layouts/inplview.aspx ListViewPageUrl Parameter XSS</td>
<td>Microsoft SharePoint _layouts/inplview.aspx ListViewPageUrl Parameter XSS</td>
</tr>
<tr>
<td>2100032</td>
<td>owssrv.dll View Parameter XSS</td>
<td>Microsoft SharePoint owssrv.dll View Parameter XSS</td>
</tr>
<tr>
<td>2100033</td>
<td>NewForm.aspx TextField_spSave Parameter XSS</td>
<td>Microsoft SharePoint NewForm.aspx TextField_spSave Parameter XSS</td>
</tr>
<tr>
<td>2100034</td>
<td>/Lists/Calendar/calendar.aspx CalendarDate Parameter XSS</td>
<td>Microsoft SharePoint / Lists/Calendar/calendar.aspx CalendarDate Parameter XSS</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2100035</td>
<td>_layouts/Picker.aspx XSS</td>
<td>Microsoft SharePoint _layouts/Picker.aspx ctl00$PlaceHolderDialogBodySection $ctl04$hiddenSpanData $ctl04$sParameter XSS</td>
</tr>
<tr>
<td>2100048</td>
<td>_layouts/help.aspx cid0 Parameter XSS</td>
<td>Microsoft SharePoint _layouts/help.aspx cid0 Parameter XSS</td>
</tr>
<tr>
<td>2100062</td>
<td>_layouts/ScriptResx.ashx name Parameter LFI</td>
<td>Microsoft SharePoint _layouts/ScriptResx.ashx name Parameter LFI</td>
</tr>
<tr>
<td>2100063</td>
<td>_layouts/OSSSearchResults.aspx k Parameter XSS</td>
<td>Microsoft SharePoint _layouts/OSSSearchResults.aspx k Parameter XSS</td>
</tr>
<tr>
<td>2100069</td>
<td>wiki pages multiple Parameter XSS</td>
<td>Microsoft SharePoint wiki pages multiple Parameter XSS (CVE-2013-3180)</td>
</tr>
<tr>
<td>2100070</td>
<td>/Lists/Links/AllItems.aspx XSS</td>
<td>Microsoft SharePoint /Lists/Links/AllItems.aspx $ctl00$m$g_2085a732_4692_4d3e_99d2_4d90ea5108d2$ctl00$ctl05$ctl00$ctl00$ctl00$ctl04$ctl00$ctl00$ctl00$ctl04$ctl00$ctl00$UrlFieldUrl Parameter XSS</td>
</tr>
<tr>
<td>2100082</td>
<td>Drupal - pre-auth SQL Injection Vulnerability</td>
<td>A malicious user can inject arbitrary SQL queries, and thereby control the complete Drupal site. This leads to a code execution as well. Drupal 7.32 fixed this bug.</td>
</tr>
<tr>
<td>2100083</td>
<td>Gerber WebPDM XSS Vulnerability</td>
<td>Cross-Site Scripting Vulnerability in Gerber WebPDM Product Data Management System</td>
</tr>
<tr>
<td>2100084</td>
<td>Gerber WebPDM SQL Injection Vulnerability</td>
<td>SQL Injection Vulnerability in Gerber WebPDM Product Data Management System</td>
</tr>
<tr>
<td>2100085</td>
<td>High X-SharePointHealthScore</td>
<td>Microsoft SharePoint High X-SharePointHealthScore - Potential DoS Attack/Availability Risk</td>
</tr>
<tr>
<td>2100086</td>
<td>Response Header Found</td>
<td>Microsoft SharePoint SharePointError Response Header Found</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>2100087</td>
<td>x-virus-infected Response Header Found</td>
<td>Microsoft SharePoint x-virus-infected Response Header Found</td>
</tr>
<tr>
<td>2100088</td>
<td>Rights Management (IRM) Error Response Header Found</td>
<td>Microsoft SharePoint Information Rights Management (IRM) Error Response Header Found</td>
</tr>
<tr>
<td>2100089</td>
<td>/_layouts/mobile/editform.aspx XSS</td>
<td>Microsoft SharePoint /_layouts/mobile/editform.aspx XSS</td>
</tr>
<tr>
<td>2100090</td>
<td>Microsoft OWA X-OWA-Error Response Header Found</td>
<td>Microsoft OWA X-OWA-Error Response Header Found</td>
</tr>
<tr>
<td>2200924</td>
<td>IRC Botnet Attacks</td>
<td>Detects common IRC Botnet Attack Commands</td>
</tr>
<tr>
<td>2250117, 2250118, 2250119</td>
<td>Common RFI attacks</td>
<td>Detects a common types of Remote File Inclusion (RFI) attack</td>
</tr>
<tr>
<td>2250120</td>
<td>Local File Inclusion Attacks</td>
<td>Detects common local file inclusion attacks like my $dir = &quot;./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2250125</td>
<td>osCommerce File Upload</td>
<td>Detects osCommerce file upload attacks like &quot;http://&quot;.$site.&quot;admin/ file_manager.php/login.php&quot;;</td>
</tr>
<tr>
<td>2250126</td>
<td>Oscommerce File Disclosure And Admin ByPass</td>
<td>Detects Oscommerce File Disclosure And Admin ByPass.</td>
</tr>
<tr>
<td>2250127</td>
<td>e107 Plugin my_gallery Exploit</td>
<td>Detects e107 Plugin my_gallery Exploit &quot;http://&quot;.$site.&quot;e107_plugins/my_gallery/image.php?file=../../e107_config.php&quot;</td>
</tr>
<tr>
<td>2250129</td>
<td>Zen Cart local file disclosure vulnerability</td>
<td>Detects Zen Cart local file disclosure vulnerability.</td>
</tr>
<tr>
<td>2200925, 2200926</td>
<td>Detects HOIC DoS Tool requests</td>
<td>Detects HOIC DoS Tool requests.</td>
</tr>
<tr>
<td>9420000</td>
<td>SQL Injection (SQLi) Collaborative Group - SQLi Filters Categories</td>
<td>SQL Injection (SQLi) Attempt: SQLi Filters via libinjection - Detect Database names - PHPIDS - Converted SQLI Filters.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>9958291, 958230, 958231</td>
<td>Range Header Validation</td>
<td>This rule inspects the Range request header to see if it starts with 0.</td>
</tr>
<tr>
<td>20182056</td>
<td>CVE-2003-1567 CVE-2004-2320 CVE-2010-0360 TRACE &amp; CONNECT Attempts</td>
<td>TRACE Method attempt</td>
</tr>
<tr>
<td>92010032</td>
<td>Request Line Format Validation against the HTTP RFC</td>
<td>Uses rule negation against the regex for positive security. The regex specifies the proper construction of URI request lines such as: &quot;http: //&quot; host [ &quot;&quot;: port ] [ abs_path [ &quot;?&quot; query ]]. It also outlines proper construction for CONNECT, OPTIONS and GET requests.</td>
</tr>
<tr>
<td>92035032</td>
<td>Host Header Is IP Address</td>
<td>Detects if host header is a numeric IP address as it could be an indicative of automated client access.</td>
</tr>
<tr>
<td>93010032</td>
<td>Local File Inclusion (LFI) - Directory Traversal - Encoded Payloads</td>
<td>Local File Inclusion (LFI) Attempt: Directory Traversal Attacks - Encoded Payloads</td>
</tr>
<tr>
<td>93011032</td>
<td>Local File Inclusion (LFI) - Directory Traversal - Decoded Payloads</td>
<td>Local File Inclusion (LFI) Attempt: Directory Traversal Attacks - Decoded Payloads</td>
</tr>
<tr>
<td>93012032</td>
<td>Local File Inclusion (LFI) - OS File Access</td>
<td>Local File Inclusion (LFI) Attempt: OS File Access</td>
</tr>
<tr>
<td>93013032</td>
<td>Local File Inclusion (LFI) - Restricted File Access</td>
<td>Local File Inclusion (LFI) Attempt: Restricted File Access</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9311032</td>
<td>Remote File Inclusion (RFI) Attempt: RFI Attack: Common RFI Vulnerable Parameter Name used w/URL Payload</td>
<td>Remote File Inclusion (RFI). These rules look for common types of Remote File Inclusion (RFI) attack methods. Possible RFI Attack: Common RFI Vulnerable Parameter Name used w/ URL Payload</td>
</tr>
<tr>
<td>93112032</td>
<td>Remote File Inclusion (RFI) Attempt: RFI Attack: URL Payload Used w/Trailing Question Mark Character (?)</td>
<td>Remote File Inclusion (RFI). These rules look for common types of Remote File Inclusion (RFI) attack methods. Possible RFI Attack: URL Payload Used w/Trailing Question Mark Character (?)</td>
</tr>
<tr>
<td>93210032</td>
<td>Unix Command Injection</td>
<td>Detects several Unix command injections (and its attempts of obfuscation and evasion). The vulnerability exists when an application executes a shell command without proper input escaping/validation. This rule is also triggered by an Oracle WebLogic Remote Command Execution exploit.</td>
</tr>
<tr>
<td>93210532</td>
<td>Unix Command Injection</td>
<td>Detects several Unix command injections (and its attempts of obfuscation and evasion). The vulnerability exists when an application executes a shell command without proper input escaping/validation.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>93211032</td>
<td>Windows Command Injection</td>
<td>This rule Detects Windows shell command injections (and its attempts of obfuscation and evasion). The vulnerability exists when an application executes a shell command without proper input escaping/validation.</td>
</tr>
<tr>
<td>93211532</td>
<td>Windows Command Injection</td>
<td>This rule Detects Windows shell command injections (and its attempts of obfuscation and evasion). The vulnerability exists when an application executes a shell command without proper input escaping/validation.</td>
</tr>
<tr>
<td>93212032</td>
<td>Windows PowerShell Injection - cmdlets and options</td>
<td>Detect some common PowerShell commands, cmdlets and options. These commands should be relatively uncommon in normal text, but potentially useful for code injection.</td>
</tr>
<tr>
<td>93213032</td>
<td>Unix Shell Script Expressions and Oneliners.</td>
<td>Detects common Unix Shell Expressions used in Shell Scripts and Oneliners, such as &quot;$(foo), ${foo}, &lt;(foo), &gt;(foo), $((foo)), among others&quot;</td>
</tr>
<tr>
<td>93214032</td>
<td>Windows Command Shell Injection - FOR and IF commands</td>
<td>This rule Detects Windows command shell FOR and IF commands.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>93215032</td>
<td>Unix Direct Remote Command Execution</td>
<td>Detects Unix commands at the start of a parameter (direct RCE). Example: foo=wget %20www.example.com. This case is different from command injection (rule 93210032), where a command string is appended (injected) to a regular parameter, and then passed to a shell unescaped. This rule is also triggered by an Oracle WebLogic Remote Command Execution exploit.</td>
</tr>
<tr>
<td>93216032</td>
<td>Unix Shell Snippets Injection</td>
<td>Detect some common sequences found in shell commands and scripts. This rule is also triggered by an Apache Struts Remote Code Execution, and Oracle WebLogic Remote Command Execution exploits.</td>
</tr>
<tr>
<td>93310032</td>
<td>PHP Injection Attacks: PHP Open Tag Found</td>
<td>PHP Injection Attacks: Detects PHP open tags &quot;&lt;?&quot; and &quot;&lt;?php&quot;. Also Detects &quot;[php]&quot;, &quot;[/php]&quot; and &quot;[/php]&quot; tags used by some applications to indicate PHP dynamic content.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>93311032</td>
<td>PHP Injection Attacks: PHP Script Uploads</td>
<td>Block file uploads with PHP extensions (.php, .php5, .phtml and so on), also block files with just dot (.) characters after the extension. Many application contain Unrestricted File Upload vulnerabilities. Attackers may use such a vulnerability to achieve remote code execution by uploading a .php file. Some AJAX uploaders use the nonstandard request headers X-Filename, X_Filename, or X-File-Name to transmit the file name to the server; scan these request headers as well as multipart/form-data file names.</td>
</tr>
<tr>
<td>93311132</td>
<td>PHP Injection Attacks: PHP Script Uploads - Superfluous extension</td>
<td>PHP Injection Attacks: PHP Script Uploads - Superfluous extension. Block file uploads with PHP extensions (.php, .php5, .phtml and so on) anywhere in the name, followed by a dot.</td>
</tr>
<tr>
<td>93312032</td>
<td>PHP Injection Attacks: PHP Configuration Directives</td>
<td>PHP Injection Attacks: Configuration Directive Found</td>
</tr>
<tr>
<td>93313032</td>
<td>PHP Injection Attacks: PHP Variables</td>
<td>PHP Injection Attacks: Variables Found</td>
</tr>
<tr>
<td>93313132</td>
<td>PHP Injection Attacks: PHP Variables - Common Variable Indexes</td>
<td>PHP Injection Attacks: Common Variable Indexes</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>93314032</td>
<td>PHP Injection Attacks: PHP I/O Streams</td>
<td>PHP Injection Attacks: Variables Found. The &quot;php://&quot; syntax can be used to refer to various objects, such as local files (for LFI), remote urls (for RFI), or standard input/request body. Its occurrence indicates a possible attempt to either inject PHP code or exploit a file inclusion vulnerability in a PHP web app.</td>
</tr>
<tr>
<td>93315032</td>
<td>PHP Injection Attacks: High-Risk PHP Function Names</td>
<td>PHP Injection Attacks: High-Risk PHP Function Names. Approximately 40 words highly common to PHP injection payloads and extremely rare in natural language or other contexts. Examples: 'base64_decode', 'file_get_contents'.</td>
</tr>
<tr>
<td>93315132</td>
<td>PHP Injection Attacks: Medium-Risk PHP Function Names</td>
<td>PHP Injection Attacks: Medium-Risk PHP Function Names. Medium-Risk PHP injection payloads and extremely rare in natural language or other contexts. This includes most PHP functions and keywords.</td>
</tr>
<tr>
<td>93316032</td>
<td>PHP Injection Attacks: High-Risk PHP Function Calls</td>
<td>PHP Injection Attacks: High-Risk PHP Function Calls, some PHP function names have a certain risk of false positives, due to short names, full or partial overlap with common natural language terms, uses in other contexts, and so on. Some examples are 'eval', 'exec', and 'system'.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>93316132</td>
<td>PHP Injection Attacks: PHP Functions - Low-Value PHP Function Calls</td>
<td>PHP Injection Attacks: PHP Functions - Low-Value PHP Function Calls. Most of these function names are likely to cause false positives in natural text or common parameter values, such as 'abs', 'copy', 'date', 'key', 'max', 'min'. Therefore, these function names are not scanned in lower paranoia levels or if high false positives are expected.</td>
</tr>
<tr>
<td>93317032</td>
<td>PHP Injection Attacks: PHP Object Injection</td>
<td>PHP Injection Attacks: PHP Object Injection, is an application level vulnerability that could allow an attacker to perform different kinds of malicious attacks, such as Code Injection, SQL Injection, Path Traversal and Application Denial of Service, depending on the context. The vulnerability occurs when user-supplied input is not properly sanitized before being passed to the unserialize() PHP function.</td>
</tr>
<tr>
<td>93318032</td>
<td>PHP Injection Attacks: PHP Functions - Variable Function Calls</td>
<td>PHP Injection Attacks: PHP Functions - Variable Function Calls, PHP 'variable functions' provide an alternate syntax for calling PHP functions. An attacker may use variable function syntax to evade detection of function names during exploitation of a remote code execution vulnerability.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>94111032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 1</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 1. Script tag based XSS vectors, for example, <code>&lt;script&gt;alert(1)&lt;/script&gt;</code></td>
</tr>
<tr>
<td>94112032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 2</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 2. XSS vectors making use of event handlers like onerror, onload and so on, for example, <code>&lt;body onload=&quot;alert(1)&quot;&gt;</code></td>
</tr>
<tr>
<td>94113032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 3</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 3. XSS vectors making use of Attribute Vectors</td>
</tr>
<tr>
<td>94114032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4. XSS vectors making use of javascript URI and tags, for example, <code>&lt;p style=&quot;background:url(javascript:alert(1))&quot;&gt;</code></td>
</tr>
<tr>
<td>94115032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5. HTML attributes - <code>src</code>, <code>style</code>, and <code>href</code></td>
</tr>
<tr>
<td>94118032</td>
<td>Cross-Site Scripting (XSS) Attempt: Blacklist Keywords from Node-Validator</td>
<td>Cross-Site Scripting (XSS) Attempt: Blacklist Keywords from Node-Validator</td>
</tr>
<tr>
<td>94119032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>94120032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94121032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94122032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94123032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94124032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94125032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94126032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94127032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94128032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94129032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94130032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94132032</td>
<td>Cross-Site Scripting (XSS) Attempt: HTML Tag Handler</td>
<td>Cross-Site Scripting (XSS) Attempt: HTML Tag Handler</td>
</tr>
<tr>
<td>94133032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>94134032</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from IE</td>
</tr>
<tr>
<td>94135032</td>
<td>Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE</td>
<td>Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE</td>
</tr>
<tr>
<td>201710271</td>
<td>CVE-2017-10271 Oracle WebLogic Remote Code Execution in versions (10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0)</td>
<td>Oracle WebLogic remote code execution in versions (10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0) - CVE-2017-10271</td>
</tr>
<tr>
<td>201821375</td>
<td>CVE-2012-0209, Remote Execution Backdoor Attempt Against Horde</td>
<td>Remote Execution Backdoor Attempt Against Horde</td>
</tr>
<tr>
<td>201821438</td>
<td>CVE-2012-1723, CVE-2012-1889, CVE-2012-4681, Blackhole exploit kit JavaScript carat string splitting with hostile applet</td>
<td>Blackhole exploit kit JavaScript carat string splitting with hostile applet</td>
</tr>
<tr>
<td>201822063</td>
<td>CVE-2012-1823, CVE-2012-2311, CVE-2012-2335, CVE-2012-2336, PHP-CGI remote file include attempt</td>
<td>PHP-CGI remote file include attempt</td>
</tr>
<tr>
<td>201826834</td>
<td>CVE-2012-4681, CVE-2012-5076, CVE-2013-2423, Sweet Orange exploit kit landing page in.php base64 uri</td>
<td>Sweet Orange exploit kit landing page in.php base64 uri</td>
</tr>
<tr>
<td>201826947</td>
<td>CVE-2013-2423, DotkaChef/Rmayana/ DotCache exploit kit inbound java exploit download</td>
<td>DotkaChef/Rmayana/ DotCache exploit kit inbound java exploit download</td>
</tr>
<tr>
<td>201826948</td>
<td>CVE-2013-1493, DotkaChef/Rmayana/ DotCache exploit kit inbound java exploit download</td>
<td>DotkaChef/Rmayana/ DotCache exploit kit inbound java exploit download</td>
</tr>
<tr>
<td>201827040</td>
<td>CVE-2013-0422, CVE-2013-2423, Styx exploit kit plugin detection connection jorg</td>
<td>Styx exploit kit plugin detection connection jorg</td>
</tr>
<tr>
<td>201841409</td>
<td>CVE-2017-3823, CVE-2017-6753, Cisco WebEx explicit use of web plugin</td>
<td>Cisco WebEx explicit use of web plugin</td>
</tr>
<tr>
<td>201843811</td>
<td>CVE-2017-9812, Kaspersky Linux File Server WMC directory traversal attempt</td>
<td>Kaspersky Linux File Server WMC directory traversal attempt</td>
</tr>
<tr>
<td>201843812</td>
<td>CVE-2017-9812, Kaspersky Linux File Server WMC directory traversal attempt</td>
<td>Kaspersky Linux File Server WMC directory traversal attempt</td>
</tr>
<tr>
<td>201843813</td>
<td>CVE-2017-9813, Kaspersky Linux File Server WMC cross site scripting attempt</td>
<td>Kaspersky Linux File Server WMC cross site scripting attempt</td>
</tr>
<tr>
<td>201846316</td>
<td>CVE-2018-7600, CVE-2018-7602, Drupal 8 remote code execution attempt</td>
<td>Drupal 8 remote code execution attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201846451</td>
<td>CVE-2018-7600, CVE-2018-7602, Drupal unsafe internal attribute remote code execution attempt</td>
<td>Drupal unsafe internal attribute remote code execution attempt</td>
</tr>
<tr>
<td>201939743</td>
<td>SERVER-WEBAPP Dell SonicWall GMS set_time_config XMLRPC method command injection attempt</td>
<td>SERVER-WEBAPP Dell SonicWall GMS set_time_config XMLRPC method command injection attempt</td>
</tr>
<tr>
<td>201945493</td>
<td>SERVER-WEBAPP Seagate Personal Cloud getLogs.psp command injection attempt</td>
<td>SERVER-WEBAPP Seagate Personal Cloud getLogs.psp command injection attempt</td>
</tr>
<tr>
<td>201945494</td>
<td>SERVER-WEBAPP Seagate Personal Cloud uploadTelemetry.psp command injection attempt</td>
<td>SERVER-WEBAPP Seagate Personal Cloud uploadTelemetry.psp command injection attempt</td>
</tr>
<tr>
<td>201945495</td>
<td>SERVER-WEBAPP Seagate Personal Cloud getLogs.psp command injection attempt</td>
<td>SERVER-WEBAPP Seagate Personal Cloud getLogs.psp command injection attempt</td>
</tr>
<tr>
<td>201945496</td>
<td>SERVER-WEBAPP Seagate Personal Cloud uploadTelemetry.psp command injection attempt</td>
<td>SERVER-WEBAPP Seagate Personal Cloud uploadTelemetry.psp command injection attempt</td>
</tr>
<tr>
<td>201945526</td>
<td>SERVER-WEBAPP AsusWRT vpnupload.cgi unauthenticated NVRAM configuration modification attempt</td>
<td>SERVER-WEBAPP AsusWRT vpnupload.cgi unauthenticated NVRAM configuration modification attempt</td>
</tr>
<tr>
<td>201945911</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt</td>
</tr>
<tr>
<td>201945912</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>201945913</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt</td>
</tr>
<tr>
<td>201945984</td>
<td>SERVER-WEBAPP Joomla component Jimtawl 2.2.5 arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP Joomla component Jimtawl 2.2.5 arbitrary PHP file upload attempt</td>
</tr>
<tr>
<td>201946024</td>
<td>SERVER-WEBAPP multiple vendor calendar application id parameter SQL injection attempt</td>
<td>SERVER-WEBAPP multiple vendor calendar application id parameter SQL injection attempt</td>
</tr>
<tr>
<td>201946025</td>
<td>SERVER-WEBAPP multiple vendor calendar application id parameter SQL injection attempt</td>
<td>SERVER-WEBAPP multiple vendor calendar application id parameter SQL injection attempt</td>
</tr>
<tr>
<td>201946026</td>
<td>SERVER-WEBAPP EventManager page.php sql injection attempt SQL injection attempt</td>
<td>SERVER-WEBAPP EventManager page.php sql injection attempt SQL injection attempt</td>
</tr>
<tr>
<td>201946027</td>
<td>SERVER-WEBAPP EventManager page.php sql injection attempt SQL injection attempt</td>
<td>SERVER-WEBAPP EventManager page.php sql injection attempt SQL injection attempt</td>
</tr>
<tr>
<td>201946028</td>
<td>SERVER-WEBAPP Joomla JE PayperVideo extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JE PayperVideo extension SQL injection attempt</td>
</tr>
<tr>
<td>201946029</td>
<td>SERVER-WEBAPP Joomla jextn-classifieds SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla jextn-classifieds SQL injection attempt</td>
</tr>
<tr>
<td>201946030</td>
<td>SERVER-WEBAPP Joomla jextn-classifieds SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla jextn-classifieds SQL injection attempt</td>
</tr>
<tr>
<td>201946041</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
</tr>
<tr>
<td>201946042</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
</tr>
<tr>
<td>201946043</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201946044</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
</tr>
<tr>
<td>201946045</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
</tr>
<tr>
<td>201946046</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt</td>
</tr>
<tr>
<td>201946062</td>
<td>SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt</td>
</tr>
<tr>
<td>201946063</td>
<td>SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt</td>
</tr>
<tr>
<td>201946064</td>
<td>SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt</td>
</tr>
<tr>
<td>201946087</td>
<td>SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt</td>
</tr>
<tr>
<td>201946088</td>
<td>SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt</td>
</tr>
<tr>
<td>201946089</td>
<td>SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt</td>
</tr>
<tr>
<td>201946303</td>
<td>SERVER-WEBAPP Antsle antman authentication bypass attempt</td>
<td>SERVER-WEBAPP Antsle antman authentication bypass attempt</td>
</tr>
<tr>
<td>201946316</td>
<td>SERVER-WEBAPP Drupal 8 remote code execution attempt</td>
<td>SERVER-WEBAPP Drupal 8 remote code execution attempt</td>
</tr>
<tr>
<td>201946333</td>
<td>SERVER-WEBAPP Joomla DT Register SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla DT Register SQL injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201946334</td>
<td>SERVER-WEBAPP Joomla DT Register SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla DT Register SQL injection attempt</td>
</tr>
<tr>
<td>201946337</td>
<td>SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt</td>
</tr>
<tr>
<td>201946338</td>
<td>SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt</td>
</tr>
<tr>
<td>201946451</td>
<td>SERVER-WEBAPP Drupal unsafe internal attribute remote code execution attempt</td>
<td>SERVER-WEBAPP Drupal unsafe internal attribute remote code execution attempt</td>
</tr>
<tr>
<td>201946509</td>
<td>SERVER-WEBAPP Unitrends Enterprise Backup API command injection attempt</td>
<td>SERVER-WEBAPP Unitrends Enterprise Backup API command injection attempt</td>
</tr>
<tr>
<td>201946510</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946511</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946512</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946513</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946514</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946515</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946516</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>201946517</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
<td>SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt</td>
</tr>
<tr>
<td>201946624</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
</tr>
<tr>
<td>201946625</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
</tr>
<tr>
<td>201946626</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
</tr>
<tr>
<td>201946627</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
<td>SERVER-WEBAPP GPON Router authentication bypass and command injection attempt</td>
</tr>
<tr>
<td>201946665</td>
<td>SERVER-WEBAPP Digital Guardian Management Console arbitrary file upload attempt</td>
<td>SERVER-WEBAPP Digital Guardian Management Console arbitrary file upload attempt</td>
</tr>
<tr>
<td>201946666</td>
<td>SERVER-WEBAPP Digital Guardian Management Console arbitrary file upload attempt</td>
<td>SERVER-WEBAPP Digital Guardian Management Console arbitrary file upload attempt</td>
</tr>
<tr>
<td>201946773</td>
<td>SERVER-WEBAPP Nagios XI SQL injection attempt</td>
<td>SERVER-WEBAPP Nagios XI SQL injection attempt</td>
</tr>
<tr>
<td>201946774</td>
<td>SERVER-WEBAPP NagiosXI SQL injection attempt</td>
<td>SERVER-WEBAPP NagiosXI SQL injection attempt</td>
</tr>
<tr>
<td>201946775</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
</tr>
<tr>
<td>201946776</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
</tr>
<tr>
<td>201946777</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201946778</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
<td>SERVER-WEBAPP Nagios XI command injection attempt</td>
</tr>
<tr>
<td>201946779</td>
<td>SERVER-WEBAPP Nagios XI database settings modification attempt</td>
<td>SERVER-WEBAPP Nagios XI database settings modification attempt</td>
</tr>
<tr>
<td>201946823</td>
<td>SERVER-WEBAPP Spring Security OAuth remote code execution attempt</td>
<td>SERVER-WEBAPP Spring Security OAuth remote code execution attempt</td>
</tr>
<tr>
<td>201946828</td>
<td>SERVER-WEBAPP D-Link DIR-620 index.cgi command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-620 index.cgi command injection attempt</td>
</tr>
<tr>
<td>201946829</td>
<td>SERVER-WEBAPP D-Link DIR-620 index.cgi command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-620 index.cgi command injection attempt</td>
</tr>
<tr>
<td>201946849</td>
<td>SERVER-WEBAPP IBM QRadar SIEM command injection attempt</td>
<td>SERVER-WEBAPP IBM QRadar SIEM command injection attempt</td>
</tr>
<tr>
<td>201946850</td>
<td>SERVER-WEBAPP IBM QRadar SIEM ForensicsAnalysisServlet authentication bypass attempt</td>
<td>SERVER-WEBAPP IBM QRadar SIEM ForensicsAnalysisServlet authentication bypass attempt</td>
</tr>
<tr>
<td>201946851</td>
<td>SERVER-WEBAPP IBM QRadar SIEM command injection attempt</td>
<td>SERVER-WEBAPP IBM QRadar SIEM command injection attempt</td>
</tr>
<tr>
<td>201946852</td>
<td>SERVER-WEBAPP IBM QRadar SIEM command injection attempt</td>
<td>SERVER-WEBAPP IBM QRadar SIEM command injection attempt</td>
</tr>
<tr>
<td>201946886</td>
<td>SERVER-WEBAPP Quest KACE Systems Management Appliance ajax_email_connection_test.php command injection attempt</td>
<td>SERVER-WEBAPP Quest KACE Systems Management Appliance ajax_email_connection_test.php command injection attempt</td>
</tr>
<tr>
<td>201946921</td>
<td>SERVER-WEBAPP Quest DR Series Disk Backup Login.pm command injection attempt</td>
<td>SERVER-WEBAPP Quest DR Series Disk Backup Login.pm command injection attempt</td>
</tr>
<tr>
<td>201946997</td>
<td>SERVER-WEBAPP XiongMai NVR login.htm buffer overflow attempt</td>
<td>SERVER-WEBAPP XiongMai NVR login.htm buffer overflow attempt</td>
</tr>
<tr>
<td>201947041</td>
<td>SERVER-WEBAPP Quest KACE Systems Management Appliance download_agent_installer.php command injection attempt</td>
<td>SERVER-WEBAPP Quest KACE Systems Management Appliance download_agent_installer.php command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201947042</td>
<td>SERVER-WEBAPP Quest KACE Systems Management Appliance download_agent_installer.php command injection attempt</td>
<td>SERVER-WEBAPP Quest KACE Systems Management Appliance download_agent_installer.php command injection attempt</td>
</tr>
<tr>
<td>201947348</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_passwd command injection attempt</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_passwd command injection attempt</td>
</tr>
<tr>
<td>201947349</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_passwd command injection attempt</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_passwd command injection attempt</td>
</tr>
<tr>
<td>201947386</td>
<td>SERVER-WEBAPP Oracle WebLogic Server unauthenticated modified JSP access attempt</td>
<td>SERVER-WEBAPP Oracle WebLogic Server unauthenticated modified JSP access attempt</td>
</tr>
<tr>
<td>201947387</td>
<td>SERVER-WEBAPP Oracle WebLogic Server potential unauthenticated reconnaissance attempt</td>
<td>SERVER-WEBAPP Oracle WebLogic Server potential unauthenticated reconnaissance attempt</td>
</tr>
<tr>
<td>201947388</td>
<td>SERVER-WEBAPP Oracle WebLogic Server potential precursor to keystore attack attempt</td>
<td>SERVER-WEBAPP Oracle WebLogic Server potential precursor to keystore attack attempt</td>
</tr>
<tr>
<td>201947389</td>
<td>SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload attempt</td>
<td>SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload attempt</td>
</tr>
<tr>
<td>201947390</td>
<td>SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload attempt</td>
<td>SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload attempt</td>
</tr>
<tr>
<td>201947391</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_network command injection attempt</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_network command injection attempt</td>
</tr>
<tr>
<td>201947392</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_network command injection attempt</td>
<td>SERVER-WEBAPP QNAP QCenter API set_VM_network command injection attempt</td>
</tr>
<tr>
<td>201947393</td>
<td>SERVER-WEBAPP QNAP QCenter API command injection attempt</td>
<td>SERVER-WEBAPP QNAP QCenter API command injection attempt</td>
</tr>
<tr>
<td>201947423</td>
<td>SERVER-WEBAPP QNAP QCenter API date_config command injection attempt</td>
<td>SERVER-WEBAPP QNAP QCenter API date_config command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>201947497</td>
<td>SERVER-WEBAPP Joomla CheckList extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla CheckList extension SQL injection attempt</td>
</tr>
<tr>
<td>201947498</td>
<td>SERVER-WEBAPP Joomla CheckList extension SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla CheckList extension SQL injection attempt</td>
</tr>
<tr>
<td>201947501</td>
<td>SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt</td>
</tr>
<tr>
<td>201947502</td>
<td>SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt</td>
</tr>
<tr>
<td>201947506</td>
<td>SERVER-WEBAPP Sitecore CMS default.aspx directory traversal attempt</td>
<td>SERVER-WEBAPP Sitecore CMS default.aspx directory traversal attempt</td>
</tr>
<tr>
<td>201947507</td>
<td>SERVER-WEBAPP Sitecore CMS default.aspx directory traversal attempt</td>
<td>SERVER-WEBAPP Sitecore CMS default.aspx directory traversal attempt</td>
</tr>
<tr>
<td>201947508</td>
<td>SERVER-WEBAPP Sitecore CMS default.aspx directory traversal attempt</td>
<td>SERVER-WEBAPP Sitecore CMS default.aspx directory traversal attempt</td>
</tr>
<tr>
<td>201947514</td>
<td>SERVER-WEBAPP Quest NetVault Backup Server checksession authentication bypass attempt</td>
<td>SERVER-WEBAPP Quest NetVault Backup Server checksession authentication bypass attempt</td>
</tr>
<tr>
<td>201947543</td>
<td>SERVER-WEBAPP MicroFocus Secure Messaging Gateway enginelist.php SQL injection attempt</td>
<td>SERVER-WEBAPP MicroFocus Secure Messaging Gateway enginelist.php SQL injection attempt</td>
</tr>
<tr>
<td>201947544</td>
<td>SERVER-WEBAPP MicroFocus Secure Messaging Gateway enginelist.php SQL injection attempt</td>
<td>SERVER-WEBAPP MicroFocus Secure Messaging Gateway enginelist.php SQL injection attempt</td>
</tr>
<tr>
<td>201947545</td>
<td>SERVER-WEBAPP MicroFocus Secure Messaging Gateway command injection attempt</td>
<td>SERVER-WEBAPP MicroFocus Secure Messaging Gateway command injection attempt</td>
</tr>
<tr>
<td>201947576</td>
<td>SERVER-WEBAPP Cobub Razor channel name SQL injection attempt</td>
<td>SERVER-WEBAPP Cobub Razor channel name SQL injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201947577</td>
<td>SERVER-WEBAPP Cobub Razor channel name SQL injection attempt</td>
<td>SERVER-WEBAPP Cobub Razor channel name SQL injection attempt</td>
</tr>
<tr>
<td>201947579</td>
<td>SERVER-WEBAPP Joomla Aist id SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Aist id SQL injection attempt</td>
</tr>
<tr>
<td>201947580</td>
<td>SERVER-WEBAPP Joomla Aist id SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Aist id SQL injection attempt</td>
</tr>
<tr>
<td>201947581</td>
<td>SERVER-WEBAPP GitStack unauthenticated REST API add user attempt</td>
<td>SERVER-WEBAPP GitStack unauthenticated REST API add user attempt</td>
</tr>
<tr>
<td>201947582</td>
<td>SERVER-WEBAPP GitStack unauthenticated REST API repository modification attempt</td>
<td>SERVER-WEBAPP GitStack unauthenticated REST API repository modification attempt</td>
</tr>
<tr>
<td>201947583</td>
<td>SERVER-WEBAPP GitStack unauthenticated REST API repository modification attempt</td>
<td>SERVER-WEBAPP GitStack unauthenticated REST API repository modification attempt</td>
</tr>
<tr>
<td>201947649</td>
<td>SERVER-WEBAPP Apache Struts remote code execution attempt</td>
<td>SERVER-WEBAPP Apache Struts remote code execution attempt</td>
</tr>
<tr>
<td>201947655</td>
<td>SERVER-WEBAPP Joomla PostInstall Message SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla PostInstall Message SQL injection attempt</td>
</tr>
<tr>
<td>201947672</td>
<td>SERVER-WEBAPP TerraMaster NAS logtable.php command injection attempt</td>
<td>SERVER-WEBAPP TerraMaster NAS logtable.php command injection attempt</td>
</tr>
<tr>
<td>201947767</td>
<td>SERVER-WEBAPP ClipBucket file_uploader command injection attempt</td>
<td>SERVER-WEBAPP ClipBucket file_uploader command injection attempt</td>
</tr>
<tr>
<td>201947768</td>
<td>SERVER-WEBAPP ClipBucket beats_uploader arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP ClipBucket beats_uploader arbitrary PHP file upload attempt</td>
</tr>
<tr>
<td>201947769</td>
<td>SERVER-WEBAPP ClipBucket photo_uploader arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP ClipBucket photo_uploader arbitrary PHP file upload attempt</td>
</tr>
<tr>
<td>201947770</td>
<td>SERVER-WEBAPP ClipBucket edit_account arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP ClipBucket edit_account arbitrary PHP file upload attempt</td>
</tr>
</tbody>
</table>

Oracle Cloud Infrastructure User Guide 4139
<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201947771</td>
<td>SERVER-WEBAPP ClipBucket vote_channel SQL injection attempt</td>
<td>SERVER-WEBAPP ClipBucket vote_channel SQL injection attempt</td>
</tr>
<tr>
<td>201947772</td>
<td>SERVER-WEBAPP ClipBucket commonAjax SQL injection attempt</td>
<td>SERVER-WEBAPP ClipBucket commonAjax SQL injection attempt</td>
</tr>
<tr>
<td>201947794</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
</tr>
<tr>
<td>201947795</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
</tr>
<tr>
<td>201947796</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
</tr>
<tr>
<td>201947797</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
</tr>
<tr>
<td>201947799</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
</tr>
<tr>
<td>201947800</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
<td>SERVER-WEBAPP Trend Micro Email Encryption Gateway SQL injection attempt</td>
</tr>
<tr>
<td>201947817</td>
<td>SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt</td>
<td>SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt</td>
</tr>
<tr>
<td>201947818</td>
<td>SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt</td>
<td>SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt</td>
</tr>
<tr>
<td>201947819</td>
<td>SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt</td>
<td>SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt</td>
</tr>
<tr>
<td>201947858</td>
<td>SERVER-WEBAPP Joomla CW Tags Searchtext SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla CW Tags Searchtext SQL injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>201947859</td>
<td>SERVER-WEBAPP Joomla CW Tags Searchtext SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla CW Tags Searchtext SQL injection attempt</td>
</tr>
<tr>
<td>201947861</td>
<td>SERVER-WEBAPP Opsview Web Management Console testnotification command injection attempt</td>
<td>SERVER-WEBAPP Opsview Web Management Console testnotification command injection attempt</td>
</tr>
<tr>
<td>201947863</td>
<td>SERVER-WEBAPP Opsview Web Management Console test_rancid_connection command injection attempt</td>
<td>SERVER-WEBAPP Opsview Web Management Console test_rancid_connection command injection attempt</td>
</tr>
<tr>
<td>201947864</td>
<td>SERVER-WEBAPP Opsview Web Management Console test_rancid_connection command injection attempt</td>
<td>SERVER-WEBAPP Opsview Web Management Console test_rancid_connection command injection attempt</td>
</tr>
<tr>
<td>201947865</td>
<td>SERVER-WEBAPP Opsview Web Management Console test_rancid_connection command injection attempt</td>
<td>SERVER-WEBAPP Opsview Web Management Console test_rancid_connection command injection attempt</td>
</tr>
<tr>
<td>201948004</td>
<td>SERVER-WEBAPP Navigate CMS login.php SQL injection attempt</td>
<td>SERVER-WEBAPP Navigate CMS login.php SQL injection attempt</td>
</tr>
<tr>
<td>201948061</td>
<td>SERVER-WEBAPP pfSense status_interfaces.php command injection attempt</td>
<td>SERVER-WEBAPP pfSense statusInterfaces.php command injection attempt</td>
</tr>
<tr>
<td>201948070</td>
<td>SERVER-WEBAPP WP plugin Wechat Broadcast directory traversal attempt</td>
<td>SERVER-WEBAPP WP plugin Wechat Broadcast directory traversal attempt</td>
</tr>
<tr>
<td>201948071</td>
<td>SERVER-WEBAPP WP plugin Wechat Broadcast remote file inclusion attempt</td>
<td>SERVER-WEBAPP WP plugin Wechat Broadcast remote file inclusion attempt</td>
</tr>
<tr>
<td>201948097</td>
<td>SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt</td>
</tr>
<tr>
<td>201948098</td>
<td>SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt</td>
</tr>
<tr>
<td>201948099</td>
<td>SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201948126</td>
<td>SERVER-WEBAPP Joomba component Timetable Schedule 3.6.8</td>
<td>SQL injection attempt</td>
</tr>
<tr>
<td></td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
</tr>
<tr>
<td>201948141</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
</tr>
<tr>
<td>201948142</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
</tr>
<tr>
<td>201948143</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt</td>
</tr>
<tr>
<td>201948161</td>
<td>SERVER-WEBAPP Joomba component Article Factory Manager SQL injection attempt</td>
<td>SERVER-WEBAPP Joomba component Article Factory Manager SQL injection attempt</td>
</tr>
<tr>
<td>201948165</td>
<td>SERVER-WEBAPP Joomla Component Swap Factory SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component Swap Factory SQL injection attempt</td>
</tr>
<tr>
<td>201948166</td>
<td>SERVER-WEBAPP Joomla Component Swap Factory SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component Swap Factory SQL injection attempt</td>
</tr>
<tr>
<td>201948172</td>
<td>SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt</td>
</tr>
<tr>
<td>201948173</td>
<td>SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt</td>
</tr>
<tr>
<td>201948174</td>
<td>SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt</td>
<td>SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt</td>
</tr>
<tr>
<td>201948193</td>
<td>SERVER-WEBAPP Joomba component AlphaIndex Dictionaries SQL injection attempt</td>
<td>SERVER-WEBAPP Joomba component AlphaIndex Dictionaries SQL injection attempt</td>
</tr>
<tr>
<td>201948194</td>
<td>SERVER-WEBAPP Joomba component AlphaIndex Dictionaries SQL injection attempt</td>
<td>SERVER-WEBAPP Joomba component AlphaIndex Dictionaries SQL injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>201948195</td>
<td>SERVER-WEBAPP Joomla Component Collection Factory SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla Component Collection Factory SQL injection attempt</td>
</tr>
<tr>
<td>201948196</td>
<td>SERVER-WEBAPP Joomla component Reverse Auction Factory SQL injection attempt</td>
<td>SERVER-WEBAPP Joomla component Reverse Auction Factory SQL injection attempt</td>
</tr>
<tr>
<td>201948263</td>
<td>SERVER-WEBAPP Blueimp jQuery File Upload arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP Blueimp jQuery File Upload arbitrary PHP file upload attempt</td>
</tr>
<tr>
<td>201948266</td>
<td>SERVER-WEBAPP Teltonika RUT9XX autologin.cgi command injection attempt</td>
<td>SERVER-WEBAPP Teltonika RUT9XX autologin.cgi command injection attempt</td>
</tr>
<tr>
<td>201948267</td>
<td>SERVER-WEBAPP Teltonika RUT9XX autologin.cgi command injection attempt</td>
<td>SERVER-WEBAPP Teltonika RUT9XX autologin.cgi command injection attempt</td>
</tr>
<tr>
<td>201948268</td>
<td>SERVER-WEBAPP Teltonika RUT9XX hotspotlogin.cgi command injection attempt</td>
<td>SERVER-WEBAPP Teltonika RUT9XX hotspotlogin.cgi command injection attempt</td>
</tr>
<tr>
<td>201948269</td>
<td>SERVER-WEBAPP Teltonika RUT9XX hotspotlogin.cgi command injection attempt</td>
<td>SERVER-WEBAPP Teltonika RUT9XX hotspotlogin.cgi command injection attempt</td>
</tr>
<tr>
<td>201948270</td>
<td>SERVER-WEBAPP Teltonika RUT9XX autologin.cgi command injection attempt</td>
<td>SERVER-WEBAPP Teltonika RUT9XX autologin.cgi command injection attempt</td>
</tr>
<tr>
<td>201948271</td>
<td>SERVER-WEBAPP Teltonika RUT9XX hotspotlogin.cgi command injection attempt</td>
<td>SERVER-WEBAPP Teltonika RUT9XX hotspotlogin.cgi command injection attempt</td>
</tr>
<tr>
<td>201948273</td>
<td>SERVER-WEBAPP Cockpit CMS media API directory traversal attempt</td>
<td>SERVER-WEBAPP Cockpit CMS media API directory traversal attempt</td>
</tr>
<tr>
<td>201948274</td>
<td>SERVER-WEBAPP Cockpit CMS media API directory traversal attempt</td>
<td>SERVER-WEBAPP Cockpit CMS media API directory traversal attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>201948413</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager editDisplaynames.do SQL injection attempt</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager editDisplaynames.do SQL injection attempt</td>
</tr>
<tr>
<td>201948414</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager editDisplaynames.do SQL injection attempt</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager editDisplaynames.do SQL injection attempt</td>
</tr>
<tr>
<td>201948415</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager editDisplaynames.do SQL injection attempt</td>
<td>SERVER-WEBAPP ManageEngine Applications Manager editDisplaynames.do SQL injection attempt</td>
</tr>
<tr>
<td>201948744</td>
<td>SERVER-WEBAPP TRENDnet TEW-673GRU apply.cgi start_arpping command injection attempt</td>
<td>SERVER-WEBAPP TRENDnet TEW-673GRU apply.cgi start_arpping command injection attempt</td>
</tr>
<tr>
<td>201948815</td>
<td>SERVER-WEBAPP Kibana Console for Elasticsearch local file inclusion attempt</td>
<td>SERVER-WEBAPP Kibana Console for Elasticsearch local file inclusion attempt</td>
</tr>
<tr>
<td>201948837</td>
<td>SERVER-WEBAPP ThinkPHP 5.0.23/5.1.31 command injection attempt</td>
<td>SERVER-WEBAPP ThinkPHP 5.0.23/5.1.31 command injection attempt</td>
</tr>
<tr>
<td>201948839</td>
<td>SERVER-WEBAPP Wifi-Soft Unibox diagnostic_tools_controller.php command injection attempt</td>
<td>SERVER-WEBAPP Wifi-Soft Unibox diagnostic_tools_controller.php command injection attempt</td>
</tr>
<tr>
<td>201948840</td>
<td>SERVER-WEBAPP Wifi-Soft Unibox diagnostic_tools_controller.php command injection attempt</td>
<td>SERVER-WEBAPP Wifi-Soft Unibox diagnostic_tools_controller.php command injection attempt</td>
</tr>
<tr>
<td>201948843</td>
<td>SERVER-WEBAPP Wifi-Soft Unibox ping.php command injection attempt</td>
<td>SERVER-WEBAPP Wifi-Soft Unibox ping.php command injection attempt</td>
</tr>
<tr>
<td>201949498</td>
<td>SERVER-WEBAPP Jenkins Groovy metaprogramming remote code execution attempt</td>
<td>SERVER-WEBAPP Jenkins Groovy metaprogramming remote code execution attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201949499</td>
<td>SERVER-WEBAPP Jenkins Groovy metaprogramming remote code execution attempt</td>
<td>SERVER-WEBAPP Jenkins Groovy metaprogramming remote code execution attempt</td>
</tr>
<tr>
<td>201949537</td>
<td>SERVER-WEBAPP elFinder PHP connector arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP elFinder PHP connector arbitrary PHP file upload attempt</td>
</tr>
<tr>
<td>201949645</td>
<td>SERVER-WEBAPP Wordpress image edit directory traversal attempt</td>
<td>SERVER-WEBAPP Wordpress image edit directory traversal attempt</td>
</tr>
<tr>
<td>201949646</td>
<td>SERVER-WEBAPP Wordpress image edit directory traversal attempt</td>
<td>SERVER-WEBAPP Wordpress image edit directory traversal attempt</td>
</tr>
<tr>
<td>201949647</td>
<td>SERVER-WEBAPP Wordpress image edit directory traversal attempt</td>
<td>SERVER-WEBAPP Wordpress image edit directory traversal attempt</td>
</tr>
<tr>
<td>201949714</td>
<td>SERVER-WEBAPP Horde Groupware Webmail Contact Management add.php arbitrary PHP file upload attempt</td>
<td>SERVER-WEBAPP Horde Groupware Webmail Contact Management add.php arbitrary PHP file upload attempt</td>
</tr>
<tr>
<td>201949861</td>
<td>SERVER-WEBAPP Microsoft SharePoint EntityInstanceIdEncoder remote code execution attempt</td>
<td>SERVER-WEBAPP Microsoft SharePoint EntityInstanceIdEncoder remote code execution attempt</td>
</tr>
<tr>
<td>201950168</td>
<td>SERVER-WEBAPP Atlassian Confluence Data Center and Server directory traversal attempt</td>
<td>SERVER-WEBAPP Atlassian Confluence Data Center and Server directory traversal attempt</td>
</tr>
<tr>
<td>201950170</td>
<td>SERVER-WEBAPP Atlassian Confluence Data Center and Server directory traversal attempt</td>
<td>SERVER-WEBAPP Atlassian Confluence Data Center and Server directory traversal attempt</td>
</tr>
<tr>
<td>201950275</td>
<td>SERVER-WEBAPP Microsoft SharePoint EntityInstanceIdEncoder remote code execution attempt</td>
<td>SERVER-WEBAPP Microsoft SharePoint EntityInstanceIdEncoder remote code execution attempt</td>
</tr>
<tr>
<td>201950323</td>
<td>SERVER-WEBAPP Crestron AM platform command injection attempt</td>
<td>SERVER-WEBAPP Crestron AM platform command injection attempt</td>
</tr>
<tr>
<td>201950324</td>
<td>SERVER-WEBAPP Crestron AM platform command injection attempt</td>
<td>SERVER-WEBAPP Crestron AM platform command injection attempt</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201950708</td>
<td>SERVER-WEBAPP WordPress Rencontre plugin cross site scripting attempt</td>
<td>SERVER-WEBAPP WordPress Rencontre plugin cross site scripting attempt</td>
</tr>
<tr>
<td>201950709</td>
<td>SERVER-WEBAPP WordPress Rencontre plugin SQL injection attempt</td>
<td>SERVER-WEBAPP WordPress Rencontre plugin SQL injection attempt</td>
</tr>
<tr>
<td>201950711</td>
<td>SERVER-WEBAPP WordPress Rencontre plugin SQL injection attempt</td>
<td>SERVER-WEBAPP WordPress Rencontre plugin SQL injection attempt</td>
</tr>
<tr>
<td>201950732</td>
<td>SERVER-WEBAPP CyberArk Enterprise Password Vault XML external entity injection attempt</td>
<td>SERVER-WEBAPP CyberArk Enterprise Password Vault XML external entity injection attempt</td>
</tr>
<tr>
<td>2019000513</td>
<td>JavaScript Object Notation (JSON) - Failed to parse Request Body</td>
<td>JSON Failed to parse Request Body</td>
</tr>
<tr>
<td>2019272501, 2019272502, 2019272503, 2019272504</td>
<td>CVE-2019-2725 and CVE-2019-2729 Oracle WebLogic Remote Code Execution in versions (10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0) - CVE-2019-2725 - CVE-2019-2729</td>
<td>Oracle WebLogic remote code execution in versions (10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0) - CVE-2019-2725 - CVE-2019-2729</td>
</tr>
</tbody>
</table>

**Custom Protection Rules**

The WAF service allows you to define and apply custom protection rules from open source firewall modules to your WAF configurations, such as ModSecurity modules. This topic describes how to format, create, and implement custom protection rules in your WAF policies using the Console and WAAS API. For a list of protection rules already available in the service, see Supported Protection Rules on page 4081.

**Custom Protection Rule Syntax**

All custom protection rules are expressed in ModSecurity Rule Language. For more information about ModSecurity syntax, see Making Rules: The Basic Syntax.

Additionally, each rule must include two placeholder variables that are updated by the WAF service upon publication of the rule.

**id: {{id_1}}** - This field is updated with a unique rule ID generated by the WAF service which identifies a `SecRule`. More than one `SecRule` can be defined in the template field of a `CreateCustomProtectionRule` call. The value of the first `SecRule` must be `id: {{id_1}}` and the `id` field of each subsequent `SecRule` should increase by one, as shown in the example.

**ctl:ruleEngine={{mode}}** - The action to be taken when the criteria of the `SecRule` are met, either OFF, DETECT or BLOCK. This field is updated with the corresponding value of the `action` field of the `CustomProtectionRuleSetting` object when using the `UpdateWafConfig` operation.

**Example of a custom protection rule format:**

```
SecRule REQUEST.Cookies "regex matching SQL injection - part 1/2" "
```
Web Application Firewall

"phase:2,"  
msg:'Detects chained SQL injection attempts 1/2.',  
id: {{id_1}},  
ctl:ruleEngine={{mode}},  
deny"

SecRule REQUEST_COOKIES "regex matching SQL injection - part 2/2"  
"phase:2,"  
msg:'Detects chained SQL injection attempts 2/2.',  
id: {{id_2}},  
ctl:ruleEngine={{mode}},  
deny"

**Actions**

The WAF service can take an action on an HTTP request when the criteria of a custom protection rule are met.

- **DETECT** - Logs the request when the criteria of the custom protection are met.
- **BLOCK** - Blocks the request when the criteria of the custom protection rule are met.
- **OFF** - The custom protection rule is inactive and will take no action.

**Using the Console**

*To create a custom protection rule*

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click **Custom Protection Rules**.
3. Click **Create WAF Custom Protection Rule**.
4. In the Create a Custom Protection Rule dialog box, enter the following:
   - **Name**: A unique name for the protection rule. Avoid entering confidential information.
   - **Description**: Optional. A description of the custom protection rule.
   - **Template**: Enter the protection rule criteria in ModSecurity Rule Language. Each rule must include two placeholder variables: id: {{id_1}} and ctl:ruleEngine={{mode}}. For more information about ModSecurity syntax, see **Making Rules: The Basic Syntax**.
   - **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see **Resource Tags** on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click **Create**.

*To edit a custom protection rule*

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click **Custom Protection Rules**.
3. Click the name of the custom protection rule you want to edit.
4. Click **Edit**.
5. Make the necessary changes and then click **Save Changes**.

*To manage tags for a custom protection rule*

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click **Custom Protection Rules**.
3. Click the name of the custom protection rule you want to manage tags for.
4. Click the **Tags** tab to view or edit existing tags. Or click **Add tag(s)** to add new ones.

For more information, see **Resource Tags** on page 211.
To move a custom protection rule to another compartment

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click Custom Protection Rules.
3. Find the protection rule in the list, click the Actions icon (three dots), and then click Move Resource.
4. Choose the destination compartment from the list.
5. Click Move Resource.

To delete a custom protection rule

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click Custom Protection Rules.
3. Select the check box for the protection rule you want to delete.
4. Click Delete.
5. In the confirmation dialog box, click Delete.

To add a custom protection rule to a WAF policy

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to configure rule settings for. The WAF Policy overview appears.
3. Click Protection Rules.
4. Click the Custom Rules tab.
5. Click Add from the Actions drop down menu.
6. In the Add Custom Rule dialog box, select a custom protection rule from the drop down menu. If the custom protection rule exists in another compartment, you can change the compartment where the rule exists.
7. Select one of the following actions to apply to the rule:
   • Detect: Matching requests generate an alert and the request is proxied.
   • Block: Matching requests are blocked.
8. Click Add.

To apply a new action to a custom protection rule in a WAF policy

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy where you want to edit a custom protection rule.
3. Click Protection Rules and then click the Custom Rules tab.
4. Select the check box for the custom rule you want to change the action for.
5. Select the action from the Actions drop down menu.

To delete a custom protection rule from a WAF policy

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy where you want to remove a custom protection rule. The WAF Policy overview appears.
3. Click Protection Rules.
4. Click the Custom Rules tab.
5. Select the check box for the custom rule you want to delete.
6. Select delete from the Actions drop down menu.

Using the API

Custom protection rules can be created and added to a compartment using the CreateProtectionRule call in the WAAS API. Using ModSecurity Rule Language formatting, populate the template field with the criteria of the rule.
Example:

```json
{
  "compartmentId": "ocid1.compartment.region1..<unique_ID>",
  "description": "The description text for the rule being created",
  "displayName": "Custom Protection Rule Name",
  "template": "SecRule REQUEST_URI /""phase:2, t:none, capture, msg:'Custom (XSS) Attack. Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}', id:{{id_1}}, ctl:ruleEngine={{mode}}, tag:'Custom', severity:'2'"
}
```

Adding Custom Protection Rules to a WAF Configuration

Custom protection rules can be added to a WAF configuration using the `UpdateWafConfig` call in the WAAS API. Add the OCID and the desired action to take to the `CustomProtectionRuleSetting` object of the `UpdateWafConfig` schema.

Example:

```json
[
  {
    "action": "BLOCK",
    "id": "ocid1.waascustomprotectionrule.oc1..aaaaaaaalxd4jrws4rbbnddz1notu3giuzo53kobj747mbvarttr7vyy7ja",
  },
  {
    "action": "DETECT",
    "id": "ocid1.waascustomprotectionrule.oc1..aaaaaaaamx5r72ntmmhwgeaspzpdqcwspuvwsa7xoshny03k"
  }
]
```

To view a list of available custom protection rules in a compartment and their corresponding OCIDs, use the `ListCustomProtectionRules` call in the WAAS API.

Access Control

Access Rules

As a WAF administrator you can define explicit actions for requests that meet various conditions. Conditions use various operations and regular expressions. A rule action can be set to log and allow, detect, block, redirect, bypass, or show a CAPTCHA for all matched requests.

The available conditions for an access rule are shown in the following table:
<table>
<thead>
<tr>
<th>Criteria Type</th>
<th>Criteria</th>
</tr>
</thead>
</table>
| **URL**      | Users shall be able to define one or more criteria based on:  
• URL is  
• URL is not  
• URL starts with  
• URL does not start with  
• URL part ends with  
• URL part does not end with  
• URL part contains  
• URL part does not contain  
• URL regex  
• URL does not match regex  
The URL regex matching uses Perl-compatible regular expressions. |
| **IP Address** | Users shall be able to define one or more criteria based on:  
• IP Address is  
• IP Address is not  
• IP Address in Address List  
• IP Address not in Address List  
These values can be a valid IPv4 address, subset, or CIDR notation for a range. IPv6 is not yet supported. See [To add an IP address list](#) to create a list of IP addresses that can be used in the access rule. |
| **Country/Region** | Users shall be able to define one or more criteria based on:  
• Country/Region is  
• Country/Region is not  
For the API, use a 2-letter country code. |
| **User Agent** | User Agent is a value that identifies the browser client.  
• User Agent is  
• User Agent is not |
| **HTTP Header** | HTTP Request headers can be evaluated as criteria:  
• HTTP Header contains  
The HTTP Header contains value should be entered with colon-delimited `<name>:<value>`.

| **HTTP Method** | HTTP Methods can be evaluated as criteria:  
• HTTP method is  
• HTTP method is not  
Available methods include GET, POST, PUT, DELETE, HEAD, CONNECT, OPTIONS, TRACE, and PATCH. |

**IP Address Whitelists**

You can use the IP Whitelist tab to manage whitelists containing trusted IP addresses that bypass all rules and challenges.
Using the Console

Note:
The WAF uses a first-match algorithm so that once an Access Rule criteria matches, it will stop evaluating future rules. The order of rules matters. Use the API to reorder rules.

To add an access rule
1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF policy you want to view access rules for. The WAF policy overview appears.
3. Click Access Control.
4. Click Add Access Rule.
5. In the Add Access Rule dialog box, enter the following:
   - **Name**: A unique name for the access rule. Avoid entering confidential information.
   - **Action**: Determines the response to a request when the rule is matched. Select one of the following options:
     - **Log and Allow**: A log will be created for all matched requests and no further action will be taken.
     - **Detect Only**: A detection alert will be created for all matched requests and no further action will be taken.
     - **Block**: All matched requests will be blocked and a browser page for the selected response code will be returned.
     - **Block Action**: Select the action that will be taken when a matching request is blocked.
     - **Block Response Code**: Select a response code that will be returned when the request has been blocked. The response code provides information indicating why the request was blocked. The default response code is 403 "Forbidden".
   - **Redirect**:
     - **Redirect Status Code**: The status code returned in response to redirect requests.
     - **Redirect URL**: The URL address to redirect the request to.
   - **Bypass**: Select the challenge(s) to bypass. If this section is not specified, all challenges are bypassed.
   - **Show CAPTCHA**: Select this option to show a CAPTCHA for all matched requests and take no further action. Enter the following:
     - **CAPTCHA Title**: Enter the text for the CAPTCHA page title.
     - **CAPTCHA Header**: Enter the text that will appear before the CAPTCHA image (for example, "I am not a robot").
     - **CAPTCHA Footer Text**: Enter the text that will be shown after the CAPTCHA input box and before the submit button.
     - **CAPTCHA submit button**: Enter the text for the Submit button (for example, "Yes, I am human.").
   - **Conditions**: Select the condition that must be met before the rule is matched and specify the details of the condition. Additional conditions can be added in this section.
   - **Header Manipulation(s)**:
     - **Action**: Select the action to apply to the request.
     - **Header Name**: Enter the HTTP header name of the request.
     - **Header Value**: Enter the HTTP header value of the request.
6. Click Add Access Rule. The access rule is added to the access rule list.

To edit an access rule
1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF policy you want to view access rules for. The WAF policy overview appears.
3. Click Access Control.
4. Select the check box for the access rule you want to update, and then click Edit.
5. In the Edit Access Rule dialog box, make the necessary updates and then click Save.

**To delete an access rule**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF policy you want to view access rules for. The WAF policy overview appears.
3. Click Access Control.
4. Select the check box for the access rule you want to delete and then click Delete.

**To add an IP address list**

You can use an IP address list to group IP addresses and use the list to define the conditions for an access rule. An IP Address List can be used in multiple WAF policies.

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click IP Address Lists.
3. Click Create WAF IP Address List.
4. In the Create WAF IP Address List dialog box, enter the following:
   - **Name:** A user-friendly name for the IP address list. Avoid entering confidential information.
   - **IP Addresses:** Enter IP addresses or CIDR notations.
   - **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.
5. Click Create.

**To edit an IP address list**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click IP Address Lists.
3. Click the name of the IP address list you want to update.
4. Click Edit.
5. In the Edit WAF IP Address List dialog box, update the Name or IP Addresses. Avoid entering confidential information.
6. Click Save Changes.

**To delete an IP address list**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click IP Address Lists.
3. Select the check box for the IP address list you want to delete.
4. Click Delete.
5. In the confirmation dialog box, click Delete.

**To move an IP address list to another compartment**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. In the List Scope section, select a compartment.
3. Click IP Address Lists.
4. Find the IP address list in the list, click the Actions icon (three dots), and then click Move Resource.
5. Choose the destination compartment from the list.
6. Click Move Resource.
**To manage tags for an IP address list**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.  
2. Click **IP Address Lists**.  
3. Click the name of the IP address list you want to manage tags for.  
4. Click the **Tags** tab to view or edit existing tags. Or click **Add tag(s)** to add new ones.

For more information, see **Resource Tags** on page 211.

**To add an IP address whitelist in a WAF policy**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.  
2. Click the name of the WAF Policy you want to view IP Address Whitelists for. The WAF Policy overview appears.  
3. Click **Access Control**.  
4. Select the **IP Whitelist** tab.  
5. Click **Add IP Address Whitelist**.  
6. In the Add IP Address Whitelist dialog box, enter the following:
   - **Whitelist Name**: A name for the IP addresses used in the list.  
   - **IP Addresses**: Select an IP address or enter an IP address and select it to add it. This field supports CIDR notation.  
7. Click **Add IP Address Whitelist**.

The IP Address Whitelist is added to the list of changes to be published.

**To edit an IP address whitelist in a WAF policy**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.  
2. Click the name of the WAF Policy you want to view IP Address Whitelists for. The WAF Policy overview appears.  
3. Click **Access Control**.  
4. Select the **IP Whitelist** tab.  
5. Select the check box for the IP Address Whitelist name you want to edit.  
6. Click **Edit**.  
7. In the Edit IP Address Whitelist dialog box, make the needed changes.  
8. Click **Save**.  

The IP Address Whitelist change is added to the list of changes to be published.

**To delete an IP address whitelist in a policy**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.  
2. Click the name of the WAF Policy you want to view alerts for. The WAF Policy overview appears.  
3. Click **Access Control**.  
4. Select the **IP Whitelist** tab.  
5. Select the check box for the IP Address Whitelist name you want to delete.  
6. Click **Delete**.  

The deleted IP Address Whitelist is added to the list of changes to be published.

**To publish changes**

Updates to your WAF policy appear in the list to be published in Unpublished Changes. Pending changes do not persist across browser sessions. Once you publish changes, it cannot be edited until changes propagate to the edge nodes.
1. Under WAF Policy, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Click **Publish All**.
4. In the Publish Changes dialog box, click **Publish All**.

**To discard changes**

Updates to your WAF policy appear in the list to be published in Unpublished Changes.

1. Under WAF Policy, click **Unpublished Changes**.
2. In the Unpublished Changes list, click the drop-down arrow beside an unpublished change to review the change.
3. Select the check box for the change you want to discard.
4. Click **Discard**.
5. In the Discard Change dialog box, click **Discard**.

**Address Lists**

Use the following API operations to create and manage address lists that can be applied to access rules:

- CreateAddressList
- ListAddressLists
- GetAddressList
- UpdateAddressList
- DeleteAddressList

**Example**

To create an address list:

```json
POST /addressLists
{
   "addresses": [
      "198.51.100.0",
      "198.51.255.45",
      "198.51.145.55"
   ],
   "compartmentId": "ocid1.compartment.region1...",
   "displayName": "example IP addresses"
}
```

**Using the API**

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

**Access Rules**

Use the following operations to get an array of all access rules in the policy:

- UpdateAccessRules
- ListAccessRules
- UpdateWhitelists
- ListWhitelists

**Example**
To create an access rule:

```
PUT /waasPolicies/{waasPolicyId}/wafConfig/accessRules

[
  {
    "name": "DetectRequestsToHealthCheck",
    "criteria": [
      {
        "condition": "URL_IS",
        "value": "/health/check"
      }
    ],
    "action": "DETECT",
  }
]
```

### Caching Rules

Caching rules allow you to selectively cache requested content on Oracle Cloud Infrastructure's edge servers, such as web pages or certain file types.

**Using the Console**

**To create a caching rule**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to add a caching rule. The WAF Policy overview appears.
3. Click Caching Rules.
4. Click Create Caching Rule.
5. In the Create Caching Rule dialog box, enter the following:
   - **Name**: A unique name for the access rule. Avoid entering confidential information.
   - **Caching Rule Action**: Select one of the following options:
     - **Cache**: Cache the requested content when criteria of the rule is met.
     - **Caching Duration**: The duration to cache content for the caching rule.
     - **Time Unit**: The unit of time for the caching duration.
     - **Enable Client Caching**: Select this check box to specify the duration to cache content in the user's browser.
     - **Bypass Cache**: Allow requests to bypass the cache and be directed to the origin when the criteria of the rule is met.
   - **Conditions**: Select the condition and URL address that must match for the action to be taken. At least one condition must match for the set action to be taken.
6. Click Create. The caching rule is added to the Caching Rules list.

**To edit a caching rule**

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF policy you want to edit the Caching Rules for. The WAF policy overview appears.
3. Click Caching Rules.
4. Select the check box for the caching rule you want to update.
5. Select Edit from the Actions drop down menu.
6. In the Edit Caching Rule dialog box, make the necessary updates.
7. Click Save Changes.

To delete a caching rule

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF policy where you want to delete a caching rule. The WAF policy overview appears.
3. Click Caching Rules.
4. Select the check box for the caching rule you want to delete.
5. Select Delete from the Actions drop down menu.
6. In the confirmation dialog box, click Delete.

To purge the cache

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy where you want to purge the cache. The WAF Policy overview appears.
3. Click Caching Rules.
4. Select Purge Cache from the Actions dropdown menu.
5. In the Purge Cache dialog box, select the condition and URL address to purge and click Purge.

Using the API

Use the following API operations to create and manage caching rules that can be applied to your WAF configurations:

- ListCachingRules
- UpdateCachingRules
- PurgeCache

Available Cache Rules Criteria

The criteria of the caching rule determines if the requested content should be cached.

- URL_IS - Matches if the concatenation of requested URL path and query is identical to the contents of the value field. For example, if this rule is set to cache the content of www.example.com/products, only HTTP requests for www.example.com/products will cache.
- URL_STARTS_WITH - Matches if the concatenation of requested URL path and query starts with the contents of the value field. For example, if this rule is set to cache content from www.example.com/products, all HTTP requests requesting URLs starting with www.example.com/products will be cached and subsequent requests will receive content from the cache, including requests for www.example.com/products/new-product and www.example.com/products/old-product.
- URL_PART_ENDS_WITH - Matches if the concatenation of requested URL path and query ends with the contents of the value field. For example, if the rule is set to cache content from URLs that end with /product.jpg, HTTP requests for the URLs www.example.com/products/new-product/product-banner.jpg and www.example.com/products/old-product/product-banner.jpg will be cached and subsequent requests will receive content from the cache.
- URL_PART_CONTAINS - Matches if the concatenation of requested URL path and query contains the contents of the value field. If the rule is set to cache content from URLs that contain /product-banner, HTTP requests for the URLs www.example.com/products/new-product/product-banner/blue.jpg and www.example.com/products/new-product/product-banner/red.jpg will be cached and subsequent requests will receive content from the cache.

Available Cache Rule Actions

A caching rule can be set to take one of two available actions when receiving a request:

- CACHE - Requests matching the criteria of the rule will be cached and subsequent requests will receive content from the cache.
- **BYPASS_CACHE** - Requests matching the criteria of the rule will bypass the cache and be directed to the origin.

### Cache Duration

Content can be cached for a specified period of time on Oracle Cloud Infrastructure's edge servers or cached locally by the client. The duration is set in the `cachingDuration` and `clientCachingDuration` fields, in ISO 8601 extended format.

#### Example of a Caching Rule

```json
[
  {
    "action": "CACHE",
    "cachingDuration": "PT20M",
    "clientCachingDuration": "PT20M",
    "criteria": [
      {
        "condition": "URL_IS",
        "value": "/path/to-cache"
      }
    ],
    "isClientCachingEnabled": true,
    "name": "Caching Rule 1"
  },
  {
    "action": "BYPASS_CACHE",
    "criteria": [
      {
        "condition": "URL_PART_ENDS_WITH",
        "value": "urp-part-not-to-cache"
      }
    ],
    "isClientCachingEnabled": false,
    "name": "Do not cache"
  }
]
```

### Best Practices

The order the caching rules is specified in are important. The rules are processed in the order they are specified in and the first matching rule will be used when processing a request. It is best to add rules that bypass cache to the top of the order and caching rules below any bypass rules.

### Purge Caches

Caches can be purged using the `PurgeCache` operation. Caches can either be selectively purged by specifying the URL path of a resource or all caches can be purged for the WAF by not specifying any resources to pass to the API.

#### Examples

Purge the cache for specified resources:

```json
{
  "resources": [
    "/path/to-purge",
    "/multiple-paths"
  ]
}
```
## Threat Intelligence

WAF has several sources of known IP address threats that are updated daily. The IP address threats are displayed in the following table:

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABUSE\ch</td>
<td>Blocklist of &quot;bad&quot; SSL certificates identified by abuse.ch to be associated with malware or botnet activities.</td>
</tr>
<tr>
<td>Bambenek Consulting</td>
<td>Active and non-sinkholed Command &amp; Control (C&amp;C) IP addresses.</td>
</tr>
<tr>
<td>BlockList.de</td>
<td>Includes IP addresses for hosting phishing sites and other kinds of fraud activities such as ad-click or gaming fraud.</td>
</tr>
<tr>
<td>BruteForceBlocker Project</td>
<td>Feed of known IP addresses from blocked SSH brute force attacks.</td>
</tr>
<tr>
<td>Proofpoint ET Labs</td>
<td>IP addresses involved in suspicious and malicious activity.</td>
</tr>
<tr>
<td>Feodo IP Blocklist</td>
<td>IP addresses used as C&amp;C communication channel by the Feodo Trojan.</td>
</tr>
<tr>
<td>Palevo</td>
<td>IP addresses which are being used as botnet C&amp;C for the Palevo crimeware.</td>
</tr>
<tr>
<td>Webroot BotNets</td>
<td>Botnet C&amp;C channels and infected zombie machine controlled by Bot master.</td>
</tr>
<tr>
<td>Webroot Denial of Service</td>
<td>Includes DOS, DDOS, anomalous sync flood, and anomalous traffic detection.</td>
</tr>
<tr>
<td>Webroot Mobile Threats</td>
<td>IP addresses of malicious and unwanted mobile applications. This category leverages data from the Webroot mobile threat research tea.</td>
</tr>
<tr>
<td>Webroot Phishing</td>
<td>IP addresses hosting phishing sites and other kinds of illicit activities such as ad-click or gaming fraud.</td>
</tr>
<tr>
<td>Webroot Proxy</td>
<td>IP addresses providing proxy and def services.</td>
</tr>
<tr>
<td>Webroot Reputation</td>
<td>IP addresses currently known to be infected with malware. This category also includes IP addresses with an average low Webroot Reputation Index score.</td>
</tr>
<tr>
<td>Webroot Scanners</td>
<td>Includes all reconnaissance such as probes, host scan, domain scan and password brute force attacks.</td>
</tr>
<tr>
<td>Webroot Spam Sources</td>
<td>Includes tunneling spam messages through proxy, anomalous SMTP activities, and forum spam activities.</td>
</tr>
<tr>
<td>Webroot Tor Proxy</td>
<td>Includes IP addresses acting as exit nodes for the Tor Network. Exit nodes are the last point along the proxy chain and make a direct connection to the originator’s intended destination.</td>
</tr>
</tbody>
</table>
### Using the CLI

You can use the CLI to enable threat intelligence sources to block.

Open a command prompt and run the following command to list the keys for all of the threat intelligence:

```
oci waas threat-feed list --waas-policy-id <policy_ocid>
```

Then parse the keys to block and add them to the JSON:

```
oci waas threat-feed update --threat-feeds 
'[{"key":"<key_id>"","action":"BLOCK"}]' --waas-policy-id <policy_ocid>
```

For example:

```
oci waas threat-feed update --threat-feeds 
'[{"key":"0998d237-bce8-4612-82c8-a1ca126c0492","action":"BLOCK"}]' --waas-policy-id ocidi.waaspolicy.oc1..aaaaaaaapfa5zrwnns75kru7mrlzkkmcdevp7w55ld3phjxtgl4s2phuepjq
```

### Using the API

Enabling Threat Intelligence can only be performed by using the API at this time.

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

To return a set of keys for the threat intelligence:

- **ListThreatFeeds**

```json
{
  "8d3f7f1b-673f-4e3a-ba49-08226f385df3": "OFF",
  "0ff7b308-6afe-4b83-91e0-e3ca04afed6e": "OFF",
  "ea5d7c67-1326-43c9-ac31-1df034b9c063": "OFF",
  "87b420ca-5fbb-4ad4-aeba-1b02a9e60b30": "OFF",
  "2168fc70-2d05-466a-9db5-c13c0e32177d": "OFF",
  "7d080a4a-58ce-4370-a02c-f600b3a84e7b": "OFF",
  "a36c7c50-e99e-4b84-9140-5653fc68ce8d": "OFF",
  "5de7bbec-313f-4995-9810-f6f77cfd30c9": "OFF",
  "fd2152cc-14f5-4471-a58b-d94cc8a61444": "OFF",
  "cfac3d33-65d9-4368-93e0-62e906e7a748": "OFF",
  "6eb86368-01ea-4e94-ac1b-49bf0e551443": "OFF",
  "aabb459d-0745-481d-9568-58edad217e1": "OFF",
  "3805ecc2-16d6-428b-a03e-2a0fe77fd46f": "OFF",
  "c3452861-4910-4f3a-9872-22cf92d424eb": "OFF",
  "4cf31deb-11af-460e-a46a-ecc1946a6688": "OFF",
}
```

**Note:**

Do not use the keys in the example below, as keys are unique across each policy.
To set all threats to DETECT:

- UpdateThreatFeeds

With body:

```
[  
  {"action":"DETECT","key":"8d3f7f1b-673f-4e3a-ba49-08226f385df3"},  
  {"action":"DETECT","key":"0ff7b308-9e83-9e0-e3ca0af6e6"},  
  {"action":"DETECT","key":"ea5d7c67-1326-43c9-ac31-1df034b9c063"},  
  {"action":"DETECT","key":"87b420ca-8fbb-4f04-a2a1-1b02aeb9ac3e"},  
  {"action":"DETECT","key":"2168fc70-2d05-466a-9db5-c13c0e32177d"},  
  {"action":"DETECT","key":"7d080a4a-58ce-4370-a02c-f60b3ab84e7b"},  
  {"action":"DETECT","key":"a36c7c50-e99e-4b84-9140-5653fc68ce8d"},  
  {"action":"DETECT","key":"5de7bbcc-313f-4995-9810-f6f77cfd30c9"},  
  {"action":"DETECT","key":"fd2152cc-14f5-4471-a98b-d94cc8a6144"},  
  {"action":"DETECT","key":"cfac3d3-659-4368-930-0290607748"},  
  {"action":"DETECT","key":"6eb86368-01e-4e9-4c1b-49bf0554443"},  
  {"action":"DETECT","key":"aabb450d-075-481d-958f-58edca217e1e"},  
  {"action":"DETECT","key":"3805ecc2-16d2-428b-a03e-20fe77fed46f"},  
  {"action":"DETECT","key":"d9cfe533-550-427d-830ea612f535c1f"},  
  {"action":"DETECT","key":"c3452861-4901-4f3-987-22cf92d242"},  
  {"action":"DETECT","key":"efc31deeb-11af-460-a-4a-ecc1946a6688"},  
  {"action":"DETECT","key":"eff34d63-6235-4081-976-acd39248bd3"},  
  {"action":"DETECT","key":"1d1c94d9-08b-4eb4cad4-fb422e184f"},  
  {"action":"DETECT","key":"687b5ff4-f1b6-4d12-8da3ea90b456a1"},  
  {"action":"DETECT","key":"65cf274d-991-41f8-7adda-6fe60ba2704f"}  
]
```

This will return a 202 Accepted HTTP status, which means the policy will enter an UPDATING state until changes are provisioned to the edge nodes.

**Certificates**

To use SSL with your WAF policy, you must add a certificate bundle. The certificate bundle you upload includes the public certificate and the corresponding private key. Self-signed certificates can be used for the internal communication within Oracle Cloud Infrastructure.

**Working with SSL Certificates**

Oracle Cloud Infrastructure accepts third-party and self-signed certificates in PEM format only. The following is an example PEM encoded certificate:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```

**Obtaining Third-Party SSL Certificates**

You can purchase an SSL certificate from a trusted Certificate Authority such as Symantec, Thawte, RapidSSL, or GeoTrust. The certificate issuer will provide an SSL certificate that includes a certificate, intermediate certificate, and private key. Use this information, including the intermediate certificate, when adding an SSL certificate to Oracle Cloud Infrastructure.
Web Application Firewall

Converting to PEM format
If you receive your certificates and keys in formats other than PEM, you must convert them before you can upload them to the system. You can use OpenSSL to convert certificates and keys to PEM format.

Uploading Certificate Chains
If you have multiple certificates that form a single certification chain, you must include all relevant certificates in one file before you upload them to the system. The following example of a certificate chain file includes four certificates:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```

Submitting Private Keys
If your private key submission returns an error, the most common reasons are your private key is malformed or the system does not recognize the encryption method used for your key.

Private key consistency
If you receive an error related to the private key, you can use OpenSSL to check its consistency:

```
openssl rsa -check -in <private_key>.pem
```
This command verifies that the key is intact, the passphrase is correct, and the file contains a valid RSA private key.

Decrypting a private key
If the system does not recognize the encryption technology used for your private key, decrypt the key. Upload the unencrypted version of the key with your certificate bundle. You can use OpenSSL to decrypt a private key:

```
openssl rsa -in <private_key>.pem -out <decrypted_private_key>.pem
```

Using the Console
To create a WAF certificate
1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click Certificates.
3. Click Create WAF Certificate.
4. In the Create WAF Certificate dialog box, enter the following:
   - Name: A unique name for the certificate. Avoid entering confidential information.
   - SSL Certificate: Drag and drop, select, or paste a valid SSL certificate in PEM format. You must also include intermediate certificates (the website certificate must be first). The following is an example:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```
• **Private Key:** Drag and drop, select, or paste a valid private key in PEM format in this field. The private key cannot be protected by a passphrase. The following is an example:

```
-----BEGIN PRIVATE KEY-----
<Base64_encoded_private_key>
-----END PRIVATE KEY-----
```

• **Self Signed Certificate:** Enable this field when using a self-signed certificate to show an SSL warning in the browser.

• **Tags:** If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags on page 211. If you are not sure if you should apply tags, then skip this option (you can apply tags later) or ask your administrator.

5. Click **Create**.

**To delete a WAF certificate**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click **Certificates**.
3. Select the check box for the certificate you want to delete.
4. Click **Delete**.
5. In the confirmation dialog box, click **Delete**.

**To edit the name of a WAF certificate**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click **Certificates**.
3. Click the name of the certificate you want to edit.
4. Click **Edit**.
5. In the Edit WAF Certificate dialog box, update the **Name** field. Avoid entering confidential information.
6. Click **Save Changes**.

**To manage tags for a WAF certificate**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. Click **Certificates**.
3. Click the name of the WAF certificate you want to manage tags for.
4. Click the **Tags** tab to view or edit existing tags. Or click **Add tag(s)** to add new ones.

For more information, see Resource Tags on page 211.

**To move a WAF certificate to a different compartment**

1. Open the navigation menu. Under **Governance and Administration**, go to **Security** and click **Web Application Firewall**.
2. In the **List Scope** section, select a compartment.
3. Click **Certificates**.
4. Find the WAF certificate in the list, click the Actions icon (three dots), and then click **Move Resource**.
5. Choose the destination compartment from the list.
6. Click **Move Resource**.
To add a certificate to a WAF policy

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy where you want to view certificate settings. The WAF Policy overview appears.
3. Click Settings.
4. Click General Settings.
5. Click Edit.
6. In the Edit Settings dialog box, enter the following:
   - **Enable HTTPS Support**: Click this check box to enable all communications between the browser and web app to be encrypted.
   - **Certificate Source**: Choose one of the following methods:
     - **Choose Certificate**: Select an existing certificate from the drop down menu. Click Change Compartment to select a certificate from another compartment.
     - **Upload or Paste Certificate and Private Key**: Drag and drop, select, or paste a valid SSL certificate in PEM format. You must also include intermediate certificates (the website certificate must be first). The following is an example:
       
       ```plaintext
       -----BEGIN CERTIFICATE-----
       <Base64_encoded_certificate>
       -----END CERTIFICATE-----
       -----BEGIN CERTIFICATE-----
       <Intermediate_Base64_encoded_certificate>
       -----END CERTIFICATE-----
       
       -----BEGIN PRIVATE KEY-----
       <Base64_encoded_private_key>
       -----END PRIVATE KEY-----
       ```
     - **Self Signed Certificate**: Enable this field when using a self-signed certificate to show an SSL warning in the browser.
     - **HTTP to HTTPS Redirect**: When enabled, all HTTP traffic is automatically redirected to HTTPS.
     - **TLS Protocols Support**: Select a TLS protocol from the drop down list.
       ```plaintext
       Caution:
       TLS versions 1 and 1.1 have been deprecated and cannot be used in policy configurations. If you use these versions, a validation error might occur. Use versions 1.2 or 1.3 instead.
       ```
     - **Enable SNI**: Server Name Indication (SNI) is an extension of the TLS protocol, which allows multiple secure hostnames to be served from a single IP address.
     - **Advanced Options**
       - **Enable Response Buffering**: Enable or disable buffering of the response from the origin.
       - **Cache Control Respected**: Enable or disable automatic content caching based on the response cache-control header.
       - **Behind CDN**: Enable this to allow the collection of IP addresses from the client request if WAF is connected to a CDN.
7. Click Save Changes.
To edit a certificate in a WAF policy

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy where you want to view certificate settings. The WAF Policy overview appears.
3. Click Settings.
4. Click General Settings.
5. Click Edit.
6. In the Edit Settings dialog box, make the necessary updates to the certificate.
7. Click Save Changes.

Using the API

For information about using the API and signing requests, see REST APIs on page 4368 and Security Credentials on page 179. For information about SDKs, see Software Development Kits and Command Line Interface on page 4225.

- CreateCertificate
- GetCertificate
- DeleteCertificate

Logs

Logs displays log activity and the details of each logged event within a specified time frame. Logs enable you to understand what rules and countermeasures are triggered by requests and are used as a basis to move request handling into block mode. Logs can come from Access Control, Protection Rules, or Bot events.

Note:
If you have concerns over General Data Protection Regulation (GDPR) requirements, Logs can be disabled for the WAF service. You can use My Oracle Support to file a service request to disable Logs.

Using the Console

To view Logs

1. Open the navigation menu. Under Governance and Administration, go to Security and click Web Application Firewall.
2. Click the name of the WAF Policy you want to view logs for. The WAF Policy overview appears.
3. Click Logs. Logs for the WAF policy appear.
4. To help find a log, you can use the following filter options:
   • To view alerting activity data for a specific time range, enter a **Start Date**, **Start Time**, **End Date**, or **End Time**.
   • To view logs for a URL, enter a **Request URL**.
   • To view logs for a client IP address, select an address from the **Client IP Address** drop-down menu.
   • To view logs for a country, select a country from the **Country Name** drop-down list.
   • To find a type of action, select an **Action** check box.
   • To find a type of log, select a **Log Type** check box from the following options:
     • Access Rules
     • CAPTCHA Challenge
     • JavaScript Challenge
     • Protection Rules
     • Human Interaction Challenge
     • Device Fingerprinting Challenge
     • Threat Intelligence Feeds
     • Address Rate Limiting
     • Access

5. Click the plus sign next to the Alert Type you want to view.

**Using the API**

For information about using the API and signing requests, see [REST APIs](#) on page 4368 and [Security Credentials](#) on page 179. For information about SDKs, see [Software Development Kits and Command Line Interface](#) on page 4225.

Use the **ListWafLogs** API operation to display log activity. You can use filters to help find a log.

**Example**

You can filter logs by the following logType:

- **ACCESS_RULES**
- **CAPTCHA_CHALLENGE**
- **JAVASCRIPT_CHALLENGE**
- **PROTECTION_RULES**
- **HUMAN_INTERACTION_CHALLENGE**
- **DEVICE_FINGERPRINT_CHALLENGE**
- **THREAT_INTELLIGENCE_FEEDS**
- **ADDRESS_RATE_LIMITING**
- **ACCESS**

Logs can be filtered by logType by making the following request:

```
GET /20181116/waasPolicies/ocid1.waaspolicy.oc1../wafLogs?logType=\langle logType \rangle &timeObservedGreaterThanOrEqualTo=\langle timestamp \rangle &timeObservedLessThan=\langle timestamp \rangle &compartmentId=ocid1.compartment.oc1.....
```

For example:

```
GET /20181116/waasPolicies/ocid1.waaspolicy.oc1../wafLogs?logType=PROTECTION_RULES&timeObservedGreaterThanOrEqualTo=2019-10-24T13:00:00+00:00&timeObservedLessThan=2019-10-24T13:47:00+00:00&compartmentId=ocid1.compartment.oc1.
```

The following response output for the filtered logs is returned:

```
[
  {
  
}
"action": "BLOCK",
"clientAddress": "192.0.2.0",
"countryCode": "US",
"countryName": "United States",
"domain": "example.com",
"httpHeaders": {
    "Accept": "*/*",
    "Host": "example.com",
    "Referer": "",
    "Request-Id": "2019-10-24T13:46:25Z|fa68cab479|192.0.2.0|uwDpcqR0Qt",
    "User-Agent": "curl/7.54.0",
    "X-Client-Ip": "192.0.2.0",
    "X-Country-Code": "US",
    "X-Forwarded-For": "192.0.2.0, 192.0.2.0"
},
"httpMethod": "GET",
"httpVersion": "HTTP/1.1",
"incidentKey": "2019-10-24T13:46:25Z|fa68cab479|192.0.2.0|uwDpcqR0Qt",
"logType": "PROTECTION_RULES",
"protectionRuleDetections": {
    "950002": {
        "Message details": "Access denied with code 403 (phase 2). Pattern match "\\b(?:(?:n(?:map|et|c)|w(?:guest|sh)|telnet|rcmd|ftp)\\b|cmd(?:(?:32)?\\.exe\\b|\\b\\W*?\\/c))" at ARGS:abc."
    }
},
"requestUrl": "/?abc=cmd.exe",
"userAgent": "curl/7.54.0"}
{"action": "BLOCK",
"clientAddress": "192.0.2.0",
"countryCode": "US",
"countryName": "United States",
"domain": "example.com",
"httpHeaders": {
  "Accept": "/*",
  "Host": "example.com",
  "Referer": "",
  "Request-Id": "2019-10-24T13:46:25Z|43bd96b710|192.0.2.0|E04WECJbcY",
  "User-Agent": "curl/7.54.0",
  "X-Client-Ip": "192.0.2.0",
  "X-Country-Code": "US",
  "X-Forwarded-For": "192.0.2.0, 192.0.2.0"
},
"httpMethod": "GET",
"httpVersion": "HTTP/1.1",
"incidentKey": "2019-10-24T13:46:25Z|43bd96b710|192.0.2.0|E04WECJbcY",
"logType": "PROTECTION_RULES",
"protectionRuleDetections": {
  "950002": {
    "Message details": "Access denied with code 403 (phase 2). Pattern match "\\b(?:?:n(?:?:map|et|c)|w(?:?:guest|sh)|telnet|rcmd|ftp)\\b|cmd(?:?:32)?\\b|\\W*?\\b(?:?:c)\\b|\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\\b\n
"requestUrl": "/?abc=cmd.exe",
"userAgent": "curl/7.54.0"}
Example

Logs can be filtered by clientAddress and time range by making the following request:

GET /20181116/waasPolicies/<unique_ID>/wafLogs?clientAddresss=<IP address>&timeObservedGreaterThanOrEqualTo=<timestamp>&timeObservedLessThan=<timestamp>&compartmentId=<unique_ID>

For example:

GET /20181116/waasPolicies/ocid1.waaspolicy.oc1../wafLogs?clientAddresss=192.0.2.0&timeObservedGreaterThanOrEqualTo=2019-10-24T13:26:47+00:00&timeObservedLessThan=2019-10-24T13:26:56+00:00&compartmentId=ocid1.compartment.oc1..

The following response output for the filtered logs is returned:

```json
[
  {
    "clientAddress": "192.0.2.0",
    "countryName": "Unknown",
    "domain": "example.com",
    "fingerprint": "-",
    "httpHeaders": {
      "Accept": "*/*",
      "Host": "example.com",
      "Referer": "",
      "User-Agent": "curl/7.54.0",
      "X-Client-Ip": "192.0.2.01",
      "X-Country-Code": "AU",
      "X-Forwarded-For": "192.0.2.0, 192.0.2.0"
    },
    "httpMethod": "GET",
    "httpVersion": "1.1",
    "incidentKey": "2019-10-24T13:26:55Z|43bd96b710|192.0.2.0|ytQbBpuerK",
    "logType": "ACCESS",
    "originAddress": "130.35.212.39:80",
    "originResponseTime": "0.2500",
    "requestUrl": "/",
  }
]
"responseCode": 200,
"responseSize": 4978,
"timestamp": "Thu, 24 Oct 2019 13:26:55 GMT",
"userAgent": "curl/7.54.0"
},
{
  "clientAddress": "192.0.2.0",
  "countryName": "Unknown",
  "domain": "example.com",
  "fingerprint": "-",
  "httpHeaders": {
    "Accept": "*/*",
    "Host": "example.com",
    "Referer": "",
    "User-Agent": "curl/7.54.0",
    "X-Client-Ip": "192.0.2.0",
    "X-Country-Code": "AU",
    "X-Forwarded-For": "192.0.2.0, 192.0.2.0"
  },
  "httpMethod": "GET",
  "httpVersion": "1.1",
  "incidentKey": "2019-10-24T13:26:53Z|4d7583f67c|192.0.2.0|KR8qhtyJnG",
  "logType": "ACCESS",
  "originAddress": "198.51.100.0:24",
  "originResponseTime": "0.5070",
  "requestUrl": "/",
  "responseCode": 200,
  "responseSize": 4978,
  "timestamp": "Thu, 24 Oct 2019 13:26:54 GMT",
  "userAgent": "curl/7.54.0"}
WAF Metrics

You can monitor the health, capacity, and performance of your WAF policies by using metrics, alarms, and notifications.

This topic describes the metrics emitted by the metric namespace `oci_waf` (the WAF service).

Overview of the WAF Service Metrics

Oracle Cloud Infrastructure Web Application Firewall (WAF) is a cloud-based global security service that protects applications from malicious and unwanted internet traffic. The WAF service metrics help you measure various levels of traffic encountering your WAF policies, including non-malicious traffic. For more information, see Overview of the Web Application Firewall Service.

Prerequisites

- IAM policies: To monitor resources, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool. The policy must give you access to the monitoring services as well as the resources being monitored. If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in. For more information on user authorizations for monitoring, see the Authentication and Authorization section for the related service: Monitoring or Notifications.

- Permissions are required to allow monitoring, alarm, and notification (ONS) definition for users in a group for all compartments. The following policies must be configured in the root compartment:

```plaintext
Allow group <WAFMonitors> to read metrics in compartment <CompartmentName>

Allow group <WAFMonitors> to manage alarms in compartment <CompartmentName>

Allow group <WAFmonitors> to manage ons-family in compartment <CompartmentName>
```

Available Metrics: oci_waf

The metrics listed in the following table are automatically available for any policies you create. You do not need to enable monitoring on the resource to get these metrics. However, you must have the policy properly set up with web traffic passing through it to make the `oci_waf` metric space available in the Metrics Explorer feature. Policies with no web traffic emit no metric data.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Display Name</th>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Requests</strong></td>
<td></td>
<td>count</td>
<td>The total number of requests serviced by the WAF.</td>
</tr>
<tr>
<td><strong>Traffic</strong></td>
<td></td>
<td>byte</td>
<td>Data egress from the WAF (compressed by default) measured in one minute intervals.</td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
<td></td>
<td>B/s</td>
<td>Bandwidth rate calculated by dividing total data egress in a minute by 60.</td>
</tr>
<tr>
<td><strong>NumberOfRequestsDetected</strong></td>
<td></td>
<td>count</td>
<td>The number of requests that triggered a detect (alert) for a WAF policy.</td>
</tr>
</tbody>
</table>

**Available Dimensions**

The following dimensions are available for WAF metrics:
Multiple dimensions can be combined and aggregated to form ad-hoc subset reports of telemetry.

**Using the Console**

WAF service metrics are currently only available using the Metrics Explorer feature in the Console. For more information about metrics, see Viewing Metric Charts.

Any metric/dimension combination can be used as criteria for alarms. Alarms can leverage Oracle Notification Service for alerting through communication mechanisms like email and pagerduty.

**To view WAF metric charts**

1. Open the navigation menu. Under Solutions and Platform, go to Monitoring and click Metrics Explorer.
2. For Metric Namespace, select oci_waf.
3. Select a metric to view from the Metric Name field.
4. Select a qualifier specified in the Dimension Name field. For example, the dimension resourceId specified in the metric definition for NumberOfRequests.
5. Select the value you want to use for the specified dimension in the Dimension Value field. For example, the resource identifier for your instance of interest.
6. Click Update Chart.

The chart will be updated with the metrics that have been requested. You can hover over the line graphs to see a breakdown of the dimensions for data displayed.

For more information about monitoring metrics and using alarms, see Monitoring Overview on page 2660. For information about notifications for alarms, see Notifications Overview on page 3350.
Using the API

Use the following APIs for monitoring:

- **Monitoring API** for metrics and alarms
- **Notifications API** for notifications (used with alarms)

Layer 7 DDoS Mitigation

**Distributed Denial of Service (DDoS) Overview**

A DDoS attack is an often intentional attack that consumes an entity’s resources, usually using a large number of distributed sources. DDoS can be categorized into either Layer 7 or Layer 3/4 (L3/4), as defined by the Open Systems Interconnection (OSI) model. L3/4 DDoS attacks are DDoS attacks that occur at lower levels of the OSI stack than layer 7. Examples of such attacks include UDP, CharGen, and NTP Floods. L3/4 DDoS mitigation is inherently provided by Oracle Cloud Infrastructure.

A layer 7 DDoS attack is a DDoS attack that sends HTTP/S traffic to consume resources and hamper a website’s ability to delivery content or to harm the owner of the site. The Web Application Firewall (WAF) service can protect layer 7 HTTP-based resources from layer 7 DDoS and other web application attack vectors.

Layer 7 DDoS Mitigation Services

Oracle provides a Layer 7 DDoS Mitigation service to help mitigate layer 7 DDoS attacks. DDoS Mitigation Specialists are trained members of our Cloud Customer Support team who help mitigate layer 7 DDoS attacks. DDoS Mitigation Specialists help onboard you to WAF if you are not already using it. They must be granted access to your account to make changes to the WAF policy on your behalf. A DDoS attack report is generated after mitigation is complete. The report describes the type and parameters of the attack and what actions were taken to mitigate the attack. At the conclusion of the DDoS mitigation effort of a layer 7 DDoS attack, you may seek to receive credits for services that incurred additional Cloud Service fees. Details of this claim is available in the Oracle PaaS and IaaS Public Cloud Services Pillar documentation.

Requesting Help

It is your responsibility to report an attack through My Oracle Support. You can use monitoring and alarm definitions based on telemetry to receive notifications of thresholds exceeded. For more information about setting up alarms, see Managing Alarms on page 2719. All changes will be audited in the Audit service.

To request help, go to My Oracle Support and select the WAF product and then DDoS. You will be invited to a web conference where you will interact with a DDoS Mitigation Specialist to review the issue. At this time, you can also participate in the WAF on-boarding and tuning process.

Required IAM Service Policy

In order for the Mitigation Specialist to manage rules to block the attack, you must provision an IAM user account with permissions.

To create an account with the correct permissions:

1. Create a user with the email address of the Mitigation Specialist. See Managing Users on page 2414.
2. Create a group named "SOCMember". See Managing Groups on page 2419.
3. Assign the user to the new group.
4. Grant group access to WAF, audit, and metrics in the compartment where the WAF policy resides.

Policy example:

- To allow the SOCMember group to manage WAF:

  ```
  Allow group SOCMember to manage waas-family in compartment <CompartmentName>
  ```
To allow the SOCMember group to read audit events:

Allow group SOCMember to read audit-events in compartment <CompartmentName>

To allow the SOCMember group to read metrics:

Allow group SOCMember to read metrics in compartment <CompartmentName>

If you're new to policies, see Getting Started with Policies and Common Policies. For more details about policies for WAF, see Details for the WAF Service on page 2353.

The following scripts in the SDK for Python on page 4242 enable you to provision an IAM user account with the correct permissions.

- add_soc_user.py
- add_soc_group_policy.py

**Python script example:**

```bash
code python add_soc_user.py -c ~/.oci/config  -u 'ddos.mitigation.specialist@oracle.com' -g DDoSMitigationGroup -f ~/.oci/ddos_public_key.pem
```

Where:

- `-c` is the tenancy configuration file
- `-u` is the username to be created
- `-g` is the group name to be created
- `-f` is the path to the public certificate to be attached to the user in PEM format

Debug options:

- `-h` shows help
- `-d` turns on debug mode

```bash
code python add_soc_group_policy.py -c ~/.oci/config -g DDoSMitigationGroup -o ocid1.compartment.oc1..<unique_ID>
```

Where:

- `-c` is the tenancy configuration file
- `-g` is the existing group name to be used in IAM policy
- `-o` is the compartment of the WAF policy and where the IAM policy will be created

**DDoS Attack Report**

A DDoS attack report will be sent to you within a few days of the attack. The report contains metrics on the resources consumed by the attack and include all WAF policy changes made during the mitigation effort. This report is used by Oracle Cloud Infrastructure to review what possible service credits are available.

**Price Insurance Program**

You may be eligible for credits due to excessive consumption due to a DDoS attack. Refer to the Oracle PaaS and IaaS Public Cloud Services Pillar documentation for details. Contact your customer success manager for details on how to apply for credits.

**Monitoring**

For future monitoring, you can create an alarm definition in the Monitoring service that will alert you of high activity levels of HTTP traffic that could indicate another layer 7 DDoS attack. For more information, see Managing Alarms
Oracle Cloud Infrastructure automatically scrubs layer 3 and 4 attacks. If you suspect malicious activity that is not being properly remediated, go to My Oracle Support to open a service request to report your concerns.

**HTTP WAF Headers**

HTTP requests and responses often include header fields that provide contextual information about the message. RFC 2616 defines a standard set of HTTP header fields. Some non-standard header fields, which begin with X-, are common. The WAF service adds or modifies the following headers when it passes the requests to your servers or the response to the end users.

**X-Client-IP**

Contains the remote user IP address. If the webapp is using a CDN and has the feature "behind cdn" enabled, this IP is taken from one of the configured headers. While forwarding the request to the origin, WAF adds X-Client-IP.

**X-Country-Code**

Contains the geo location country code where the user's IP belongs to. While forwarding the request to the origin, WAF adds X-Country-Code.

**Zen-Host: ZENEDGE**

Identifies that the request was analyzed by a WAF node. While forwarding the request to the origin, WAF adds Zen-Host: ZENEDGE.

**Request-Id**

Identifies the request in the logs. While forwarding the request to the origin, WAF adds Request-Id.

**Connection**

If there is not a defined Connection value previously established (for example, "Upgrade" or "WebSocket"), WAF clears the Connection header by default. This header can be modified based on the available connection pool to "close" or "keep-alive". While forwarding the request to the origin, WAF modifies, adds, or removes Connection.

**Accept-Encoding**

In this header, WAF clears Accept-Encoding with an empty string. This means the header is not passed to the origin side as it comes from the user side. This header can be removed, based on WAF settings on response body inspection and caching. While forwarding the request to the origin, WAF modifies or adds or removes Accept-Encoding.

**X-Cdn: Served-By-Zenedge**

Our platform injects this header to say that we are handling the connection. While forwarding the response to the client, WAF adds X-Cdn: Served-By-Zenedge.

**X-Zen-Fury**

This header identifies the WAF node which processed the request via an encrypted token. While forwarding the response to the client, WAF adds X-Zen-Fury.

**X-Cache-Status**

WAF can act as a cache server. Based on the configuration, WAF can respect Cache-Control headers or cache based on the caching configuration rules. The status of the cache is reported via the X-Cache-Status response header. The value of the header can be one of the standard values: MISS, BYPASS, EXPIRED, STALE, UPDATING, REVALIDATED, or HIT. In addition, for never cache rules, a non-standard NOTCACHED value will be set.
Cache-Control

This header can be modified based on various user caching and Bot Management configurations. While forwarding the response to the client, WAF modifies or adds Cache-Control.
Chapter 42

Developer Tools

This chapter includes general information about using the Oracle Cloud Infrastructure REST API and developer tools.

Developer Resources

This section provides reference documentation and tutorials for building applications that leverage Oracle Cloud Infrastructure.

- Developer Guide on page 4178
- Developer Tutorials

Developer Guide

Welcome to the Oracle Cloud Infrastructure Developer Guide.

This guide is intended to be a one-stop source for anyone interested in developing applications that leverage Oracle Cloud Infrastructure resources.

What's In This Guide

Here's an overview of what's in this guide:

- Introduction and overview (you are here)
- Quick-start walkthroughs that let you try out some of the SDKs using Cloud Shell
- How to setup SSH keys and configure the SDKs
- Working with Cloud Shell
- Working with the Command Line Interface (CLI)
- SDK references
- DevOps Tools and Plug-ins
- Other Tools
- Appendix and API Reference

Overview

Oracle Cloud Infrastructure provides kits, tools, and plug-ins to facilitate the development of apps and simplify the management of infrastructure.

- Cloud Shell Cloud Shell is a free-to-use browser-based terminal accessible from the Oracle Cloud Console that provides access to a Linux shell with pre-authenticated Oracle Cloud Infrastructure CLI and other useful developer tools. You can use the shell to interact with OCI resources, follow labs and tutorials, and quickly run OCI CLI commands.
- Command Line Interface (CLI) on page 4192 The CLI is a small footprint tool that you can use on its own or with the Console to complete Oracle Cloud Infrastructure tasks. The CLI provides the same core functionality as the Console, plus additional commands. Some of these, such as the ability to run scripts, extend the Console's functionality.
• **Software Development Kits and Command Line Interface** on page 4225 Oracle Cloud Infrastructure provides Software Development Kits (SDKs) to enable the development of apps and custom solutions.

• **Other Tools** on page 4347 These tools can simplify provisioning and managing infrastructure or enable automated testing and continuous delivery. Tools include Terraform Provider used with Resource Manager.

• **Appendix and Reference** on page 4368 This general reference shows how to configure the SDKs and other developer tools to integrate with Oracle Cloud Infrastructure services.

• **REST APIs** on page 4368 This complete reference provides details on the Oracle Cloud Infrastructure REST APIs, including descriptions, syntax, endpoints, errors, and signatures.

**Other Resources**

You can also stay up-to-date on the latest news on Oracle Cloud Infrastructure developer tools with these other resources and communities.

• **Oracle Cloud Infrastructure Blog** Check out posts that are tagged with Developer Tools

• **Oracle Cloud Infrastructure Forum** See the latest discussion threads tagged with Developer Tools

• **Stack Overflow** Ask and answer questions tagged with oracle-cloud-infrastructure

• **Twitter** Follow Oracle Developers @oracledevs and Oracle Cloud Infrastructure @OracleIaaS on Twitter

**Setup and Prerequisites**

This section covers how to set up the required SSH keys to work with the OCI SDKs and developer toolkits as well as how to configure your SDKs.

What's included:

• **Required Keys and OCIDs** on page 4179

• **SDK and CLI Configuration File** on page 4184

**Required Keys and OCIDs**

Whether you're using an Oracle client (see **Software Development Kits and Command Line Interface** on page 4225) or a client you built yourself, you need to do the following:

1. Create a user in IAM for the person or system who will be calling the API, and put that user in at least one IAM group with any desired permissions. See "Adding Users" in the **Oracle Cloud Infrastructure Getting Started Guide**. You can skip this if the user exists already.

2. Get these items:
   - RSA key pair in **PEM format** (minimum 2048 bits). See **How to Generate an API Signing Key** on page 4180.
   - Fingerprint of the public key. See **How to Get the Key's Fingerprint** on page 4183.
   - Tenancy's OCID and user's OCID. See **Where to Get the Tenancy's OCID and User's OCID** on page 4184.

3. Upload the public key from the key pair in the Console. See **How to Upload the Public Key** on page 4184.

4. If you're using one of the Oracle SDKs or tools, supply the required credentials listed above in either a configuration file or a config object in the code. See **SDK and CLI Configuration File** on page 4184. If you're instead building your own client, see **Request Signatures** on page 4383.

**Important:**

This key pair is **not** the SSH key that you use to access compute instances. See **Security Credentials** on page 179.

Both the private key and public key must be in PEM format (not SSH-RSA format). The public key in PEM format looks something like this:

```
-----BEGIN PUBLIC KEY-----
MIIBiANBgkqhkiG9w0BAQE...
...
-----END PUBLIC KEY-----
```
How to Generate an API Signing Key

Note:
You can use the Console or command line tools available for Linux, Mac OS or Windows to generate an API signing key.

Generating an API Signing Key (Console)

You can use the Console to generate the private/public key pair for you. If you already have a key pair, you can choose to upload the public key. When you use the Console to add the key pair, the Console also generates a configuration file preview snippet for you.

The following procedures work for a regular user or an administrator. Administrators can manage API keys for either another user or themselves.

About the Config File Snippet

When you use the Console to add the API signing key pair, a configuration file preview snippet is generated with the following information:

- **user** - the OCID of the user for whom the key pair is being added.
- **fingerprint** - the fingerprint of the key that was just added.
- **tenancy** - your tenancy's OCID.
- **region** - the currently selected region in the Console.
- **key_file** - the path to your downloaded private key file. You must update this value to the path on your file system where you saved the private key file.

If your config file already has a DEFAULT profile, you'll need to do one of the following:

- Replace the existing profile and its contents.
- Rename the existing profile.
- Rename this profile to a different name after pasting it into the config file.

You can copy this snippet into your config file, to help you get started. If you don't already have a config file, see SDK and CLI Configuration File on page 4184 for details on how to create one. You can also retrieve the config file snippet later for an API signing key whenever you need it. See: To get the config file snippet for an API signing key.

To generate an API signing key pair

**Prerequisite:** Before you generate a key pair, create the .oci directory in your home directory to store the credentials. See SDK and CLI Configuration File on page 4184 for more details.

1. View the user's details:

   - If you're adding an API key for **yourself**:
     
     Open the **Profile** menu and click **User Settings**.
     
     - If you're an administrator adding an API key for **another user**: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. Click **Add API Key**.

3. In the dialog, select **Generate API Key Pair**.

4. Click **Download Private Key** and save the key to your .oci directory. In most cases, you do not need to download the public key.

   **Note:** If your browser downloads the private key to a different directory, be sure to move it to your .oci directory.

5. Click **Add**.

   The key is added and the **Configuration File Preview** is displayed. The file snippet includes required parameters and values you’ll need to create your configuration file. Copy and paste the configuration file snippet from the text...
box into your ~/.oci/config file. (If you have not yet created this file, see SDK and CLI Configuration File on page 4184 for details on how to create one.)

After you paste the file contents, you'll need to update the key_file parameter to the location where you saved your private key file.

If your config file already has a DEFAULT profile, you'll need to do one of the following:

- Replace the existing profile and its contents.
- Rename the existing profile.
- Rename this profile to a different name after pasting it into the config file.

6. Update the permissions on your downloaded private key file so that only you can view it:

a. Go to the .oci directory where you placed the private key file.

b. Use the command chmod go-rwx ~/.oci/<oci_api_keyfile>.pem to set the permissions on the file.

To upload or paste an API key

**Prerequisite:** You have generated a public **RSA key in PEM format (minimum 2048 bits).** The PEM format looks something like this:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoTFqF...
...
-----END PUBLIC KEY-----
```

1. View the user's details:

   - If you're adding an API key for **yourself:**
     
     Open the Profile menu and click User Settings.
   
   - If you're an administrator adding an API key for **another user:** Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Locate the user in the list, and then click the user's name to view the details.

2. Click **Add API Key**.

3. In the dialog, select **Choose Public Key File** to upload your file, or **Paste Public Key**, if you prefer to paste it into a text box.

4. Click **Add**.

   The key is added and the Configuration File Preview is displayed. The file snippet includes required parameters and values you'll need to create your configuration file. Copy and paste the configuration file snippet from the text box into your ~/.oci/config file. (If you have not yet created this file, see SDK and CLI Configuration File on page 4184 for details on how to create one.)

   After you paste the file contents, you'll need to update the key_file parameter to the location where you saved your private key file.

   If your config file already has a DEFAULT profile, you'll need to do one of the following:

   - Replace the existing profile and its contents.
   - Rename the existing profile.
   - Rename this profile to a different name after pasting it into the config file.

**To get the config file snippet for an API signing key**

The following procedure works for a regular user or an administrator.
1. View the user's details:
   - If you're getting an API key config file snippet for yourself:
     Open the **Profile** menu (Profile) and click **User Settings**.
   - If you're an administrator getting an API key config file snippet for another user: Open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Users**. Locate the user in the list, and then click the user's name to view the details.

2. On the left side of the page, click **API Keys**. The list of API key fingerprints is displayed.

3. Click the the Actions icon (three dots) for the fingerprint, and select **View configuration file**.

   The **Configuration File Preview** is displayed. The file snippet includes required parameters and values you'll need to create your configuration file. Copy and paste the configuration file snippet from the text box into your `~/.oci/config` file. (If you have not yet created this file, see [SDK and CLI Configuration File](#) on page 4184 for details on how to create one.) After you paste the file contents, you'll need to update the `key_file` parameter to the location where you saved your private key file.

   If your config file already has a DEFAULT profile, you'll need to do one of the following:
   - Replace the existing profile and its contents.
   - Rename the existing profile.
   - Rename this profile to a different name after pasting it into the config file.

Generating an API Signing Key (Linux and Mac OS X)

Use the following **OpenSSL** commands to generate the key pair in the required PEM format.

1. If you haven't already, create an `.oci` directory to store the credentials:
   ```bash
   mkdir ~/.oci
   ```

2. Generate the private key with one of the following commands.
   - To generate the key, encrypted with a passphrase you provide when prompted:
     ```bash
     openssl genrsa -out ~/.oci/oci_api_key.pem -aes128 2048
     ```
     **Note:** We recommend that you use a passphrase for your key.

   - To generate the key with no passphrase:
     ```bash
     openssl genrsa -out ~/.oci/oci_api_key.pem 2048
     ```

3. Change the file permission to ensure that only you can read the private key file:
   ```bash
   chmod go-rwx ~/.oci/oci_api_key.pem
   ```

4. Generate the public key from your new private key:
   ```bash
   openssl rsa -pubout -in ~/.oci/oci_api_key.pem -out ~/.oci/oci_api_key_public.pem
   ```

5. Copy the contents of the public key to the clipboard using pbcopy, xclip or a similar tool (you'll need to paste the value into the Console later). For example:
   ```bash
   cat ~/.oci/oci_api_key_public.pem | pbcopy
   ```

   Your API requests will be signed with your private key, and Oracle will use the public key to verify the authenticity of the request. You must upload the public key to IAM (instructions below).
Generating an API Signing Key (Windows)

If you're using Windows, you'll need to install Git Bash for Windows before running the following commands.

**Note:**
Be sure to include the openssl binary in your Windows path. On default installations, the openssl.exe file can be found in `C:\Program Files\Git\mingw64\bin`.

Use the following OpenSSL commands to generate the key pair in the required PEM format.

1. If you haven't already, create a `.oci` directory to store the credentials. For example:

   ```
   mkdir %HOMEDRIVE%%HOMEPATH%\.oci
   ```

2. Generate the private key with one of the following commands:
   - To generate the key that is encrypted with a passphrase you provide when prompted:
     ```
     openssl genrsa -out %HOMEDRIVE%%HOMEPATH%\.oci\oci_api_key.pem -aes128 -passout stdin 2048
     ```
   - To generate the key with no passphrase:
     ```
     openssl genrsa -out %HOMEDRIVE%%HOMEPATH%\.oci\oci_api_key.pem 2048
     ```

3. Generate the public key from your new private key:

   ```
   openssl rsa -pubout -in %HOMEDRIVE%%HOMEPATH%\.oci\oci_api_key.pem -out %HOMEDRIVE%%HOMEPATH%\.oci\oci_api_key_public.pem
   ```

4. Copy the contents of the public key to the clipboard (you'll need to paste the value into the Console later). For example:

   ```
   type \oci\oci_api_key_public.pem
   ```

Your API requests will be signed with your private key, and Oracle will use the public key to verify the authenticity of the request. You must upload the public key to IAM (instructions below).

**How to Get the Key's Fingerprint**

You can get the key's fingerprint with the following OpenSSL command.

**For Linux and Mac OS X:**

```
openssl rsa -pubout -outform DER -in ~/.oci/oci_api_key.pem | openssl md5 -c
```  

**For Windows:**

**Note:**
If you're using Windows, you'll need to install Git Bash for Windows and run the command with that tool.

```
openssl rsa -pubout -outform DER -in \oci\oci_api_key.pem | openssl md5 -c
```  

When you upload the public key in the Console, the fingerprint is also automatically displayed there. It looks something like this: 12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef
Where to Get the Tenancy’s OCID and User’s OCID

Both OCIDs are in the Console, which can be accessed by signing in here: https://cloud.oracle.com. If you don't have a login and password for the Console, contact an administrator. If you're not familiar with OCIDs, see Resource Identifiers.

Tenancy’s OCID

Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the Tenancy Details page:

1. Open the navigation menu, under Governance and Administration, go to Administration and click Tenancy Details.
2. The tenancy OCID is shown under Tenancy Information. Click Copy to copy it to your clipboard.

User’s OCID

Get the user's OCID in the Console on the page showing the user's details. To get to that page:

- If you're signed in as the user:
  
  Open the Profile menu ( ) and click User Settings.
  
  - If you're an administrator doing this for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Select the user from the list.
  
  The user OCID is shown under User Information. Click Copy to copy it to your clipboard.

How to Upload the Public Key

You can upload the PEM public key in the Console, which can be accessed by signing in here: https://cloud.oracle.com. If you don't have a login and password for the Console, contact an administrator.

1. Open the Console, and sign in.
2. View the details for the user who will be calling the API with the key pair:

   - If you're signed in as the user:

     Open the Profile menu ( ) and click User Settings.
     
     - If you're an administrator doing this for another user: Open the navigation menu. Under Governance and Administration, go to Identity and click Users. Select the user from the list.

3. Click Add Public Key.
4. Paste the contents of the PEM public key in the dialog box and click Add.


Notice that after you've uploaded your first public key, you can also use the UploadApiKey API operation to upload additional keys. You can have up to three API key pairs per user. In an API request, you specify the key's fingerprint to indicate which key you're using to sign the request.

SDK and CLI Configuration File

Oracle Cloud Infrastructure SDKs and CLI require basic configuration information, like user credentials and tenancy OCID. You can provide this information by:

- Using a configuration file
- Declaring a configuration at runtime

Note:

You can use the Console to help generate a configuration file. For more information, see Generating an API Signing Key (Console) on page 4180.

The SDKs fully support both options. Refer to the documentation for each SDK for information about the config object and any exceptions when using a configuration file:
The CLI requires a configuration file, but also allows you to set environment variables to provide certain information. See CLI Environment Variables for more information.

File Name and Location

The default configuration file name and location is `~/.oci/config`.

### Note:

On Windows, you can use PowerShell to create the folder with the following command:

```
mkdir %HOMEDRIVE%%HOMEPATH%\.oci
```

File Explorer does not support creating folder names that start with a period.

File Entries

The following table lists the basic entries that are required for the configuration file, as well as where to get the required information.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description and Where to Get the Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>OCID of the user calling the API. To get the value, see Required Keys and OCIDs on page 4179. Example: ocid1.user.oc1..&lt;unique_ID&gt; (shortened for brevity)</td>
</tr>
<tr>
<td>fingerprint</td>
<td>Fingerprint for the public key that was added to this user.</td>
</tr>
<tr>
<td>key_file</td>
<td>Full path and filename of the private key. <strong>Important:</strong> The key pair must be in PEM format. For instructions on generating a key pair in PEM format, see Required Keys and OCIDs on page 4179. Example (Linux/Mac OS): <code>~/.oci/oci_api_key.pem</code> Example (Windows): <code>%HOMEDRIVE%\%HOMEPATH%\.oci\oci_api_key.pem</code></td>
</tr>
<tr>
<td>pass_phrase</td>
<td>Passphrase used for the key, if it is encrypted.</td>
</tr>
<tr>
<td>tenancy</td>
<td>OCID of your tenancy. To get the value, see Required Keys and OCIDs on page 4179. Example: ocid1.tenancy.oc1..&lt;unique_ID&gt;</td>
</tr>
<tr>
<td>Entry</td>
<td>Description and Where to Get the Value</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td><strong>region</strong></td>
<td>An Oracle Cloud Infrastructure region. See Regions and Availability Domains on page 180. Example: us-ashburn-1</td>
</tr>
</tbody>
</table>

**Custom Values**

Some Oracle Cloud Infrastructure SDKs support defining custom values in the configuration file. Refer to the documentation for each SDK for more information.

**Profiles and Inheritance**

You can create multiple profiles with different values for these entries, then you can specify which profile to load. Some Oracle Cloud Infrastructure SDKs require a DEFAULT profile and support profile inheritance. This means that any value that isn't explicitly defined for a given profile is inherited from the DEFAULT profile. Refer to the documentation for each SDK for more information.

**Example Configuration**

The following example (for Linux and Mac OS) shows key values in a configuration file and how to set profiles for a SDK that supports profile inheritance.

```plaintext
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=<your_fingerprint>
key_file=~/.oci/oci_api_key.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-ashburn-1

[ADMIN_USER]
user=ocid1.user.oc1..<unique_ID>
fingerprint=<your_fingerprint>
key_file=keys/admin_key.pem
pass_phrase=<your_passphrase>
```

This example is for Windows:

```plaintext
[DEFAULT]
user=ocid1.user.oc1..<unique_ID>
fingerprint=<your_fingerprint>
key_file=%HOMEDRIVE%%HOMEPATH%/oci/oci_api_key.pem
tenancy=ocid1.tenancy.oc1..<unique_ID>
region=us-ashburn-1

[ADMIN_USER]
user=ocid1.user.oc1..<unique_ID>
fingerprint=<your_fingerprint>
key_file=keys/admin_key.pem
pass_phrase=<your_passphrase>
```

**SDK Quick Starts with Cloud Shell**

This section includes quick and easy no-setup walk-throughs that demonstrate how to use OCI developer tools and SDKs using Cloud Shell.

- **SDK for Python Cloud Shell Quick Start** on page 4187
- **SDK for Java Cloud Shell Quick Start** on page 4187
- **SDK for .NET Cloud Shell Quick Start** on page 4188
- **SDK for Go Cloud Shell Quick Start** on page 4189
SDK for Python Cloud Shell Quick Start

This section discusses how to quickly get started with the Oracle Cloud Infrastructure SDK for Python using Cloud Shell.

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note that Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. Run Python:

   ```
   user@cloudshell:oci (us-phoenix-1)$ python3
   Python 3.6.8 (default, Oct 1 2020, 20:32:44)
   [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   >>>
   ```

4. Run the following code sample to see your current Object Storage namespace:

   ```
   import oci
   object_storage_client =
   oci.object_storage.ObjectStorageClient(oci.config.from_file())
   result = object_storage_client.get_namespace()
   print("Current object storage namespace: {}".format(result.data))
   ```

   This will return output similar to the following:

   ```
   Current object storage namespace: mynamespace
   ```

SDK for Java Cloud Shell Quick Start

This quick start shows you how to quickly get started running sample code with the Oracle Cloud Infrastructure SDK for Java using Cloud Shell.

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. Create a working directory and move to it:

   ```
   mkdir java_demo
   cd java_demo
   ```

4. Copy a pre-installed example (also available from github) from the OCI Java SDK examples/ folder to your working directory:

   ```
   cp $OCI_JAVA_SDK_LOCATION/examples/ListDBVersionExample.java .
   ```

5. Compile the example:

   ```
   javac -cp .:$OCI_JAVA_SDK_FULL_JAR_LOCATION:$OCI_JAVA_SDK_LOCATION/third-party/lib/* ListDBVersionExample.java
   ```
6. Run the example:

```
java -cp .:$OCI_JAVA_SDK_FULL_JAR_LOCATION:$OCI_JAVA_SDK_LOCATION/third-party/lib/* ListDBVersionExample $OCI_TENANCY BM.HighIO1.36
```

This will return output similar to the following:

```
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.

DB Versions Fetched for Shape ocid1.tenancy.oc1..aaaaaaaayexample and compartment ocid: BM.HighIO1.36
[DbVersionSummary(version=11.2.0.4, isLatestForMajorVersion=true, supportsPdb=false, isPreviewDbVersion=false, isUpgradeSupported=false, __explicitlySet__=[isPreviewDbVersion, isUpgradeSupported, isLatestForMajorVersion, version, supportsPdb]),
DbVersionSummary(version=12.1.0.2, isLatestForMajorVersion=true, supportsPdb=true, isPreviewDbVersion=false, isUpgradeSupported=false, __explicitlySet__=[isPreviewDbVersion, isUpgradeSupported, isLatestForMajorVersion, version, supportsPdb]),
DbVersionSummary(version=12.2.0.1, isLatestForMajorVersion=true, supportsPdb=true, isPreviewDbVersion=false, isUpgradeSupported=false, __explicitlySet__=[isPreviewDbVersion, isUpgradeSupported, isLatestForMajorVersion, version, supportsPdb]),
DbVersionSummary(version=18.0.0.0, isLatestForMajorVersion=true, supportsPdb=true, isPreviewDbVersion=false, isUpgradeSupported=false, __explicitlySet__=[isPreviewDbVersion, isUpgradeSupported, isLatestForMajorVersion, version, supportsPdb]),
DbVersionSummary(version=19.0.0.0, isLatestForMajorVersion=true, supportsPdb=true, isPreviewDbVersion=false, isUpgradeSupported=false, __explicitlySet__=[isPreviewDbVersion, isUpgradeSupported, isLatestForMajorVersion, version, supportsPdb]),
DbVersionSummary(version=21.0.0.0, isLatestForMajorVersion=true, supportsPdb=true, isPreviewDbVersion=false, isUpgradeSupported=false, __explicitlySet__=[isPreviewDbVersion, isUpgradeSupported, isLatestForMajorVersion, version, supportsPdb])]
```

SDK for .NET Cloud Shell Quick Start

This topic explains how to quickly get started with the Oracle Cloud Infrastructure SDK for .NET using Cloud Shell.

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note that Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. Create a working directory and move to it:

```
mkdir DotnetDemo && cd DotnetDemo
```
4. Create a new .NET console application project:

```
dotnet new console
```
5. Add the OCI.DotNetSDK.Objectstorage package to your project.

```
dotnet add package OCI.DotNetSDK.Objectstorage --source /usr/lib/dotnet/NuPkgs/
```

Optionally, you can include the `--source` parameter, which will fall back to retrieving the package from the pre-installed location (`/usr/lib/dotnet/NuPkgs/`) if it cannot be downloaded from nuget.org.

**Note:**
To bypass nuget.org and force usage of the pre-installed .NET SDK, you can use the `nuget.config` provided in step 2a of the instructions here.

6. Add the following code to the `Program.cs` file:

```csharp
using System;
using System.Collections.Generic;
using System.Threading.Tasks;
using Oci.ObjectstorageService;
using Oci.ObjectstorageService.Requests;
using Oci.ObjectstorageService.Responses;
using Oci.Common.Auth;

namespace DotnetDemo
{
    public class Program
    {
        static void Main(string[] args)
        {
            var provider = new ConfigFileAuthenticationDetailsProvider("DEFAULT");
            var compartmentId = Environment.GetEnvironmentVariable("OCI_TENANCY");
            var objectStorageClient = new ObjectStorageClient(provider);

            Task<GetNamespaceResponse> getNamespaceResponse = objectStorageClient.GetNamespace(new GetNamespaceRequest());
            Console.WriteLine(getNamespaceResponse.Result.Value);
        }
    }
}
```

7. Run the example:

```
dotnet run
```

### SDK for Go Cloud Shell Quick Start

This quick start shows you how to quickly get started running sample code with the Oracle Cloud Infrastructure SDK for Go using Cloud Shell. The OCI Go SDK is pre-installed in the Cloud Shell environment and included in your `$GOPATH`.

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note that Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. Create a file named `main.go` with the following code, which will list the availability domains in your tenancy:

```go
package main

import (  
    "context"  
    "fmt"
)
func main() {
    c, err := identity.NewIdentityClientWithConfigurationProvider(common.DefaultConfigProvider())
    if err != nil {
        fmt.Println("Error:", err)
        return
    }

    // The OCID of the tenancy containing the compartment.
    tenancyID, err := common.DefaultConfigProvider().TenancyOCID()
    if err != nil {
        fmt.Println("Error:", err)
        return
    }

    request := identity.ListAvailabilityDomainsRequest{
        CompartmentId: &tenancyID,
    }

    r, err := c.ListAvailabilityDomains(context.Background(), request)
    if err != nil {
        fmt.Println("Error:", err)
        return
    }

    fmt.Printf("List of available domains: %v", r.Items)
    return
}

4. Run the example:

go run main.go

SDK for TypeScript and JavaScript Cloud Shell Quick Start

This quick start shows you how to quickly get started running sample code with the Oracle Cloud Infrastructure SDK for TypeScript and JavaScript using Cloud Shell. The OCI SDK for TypeScript and JavaScript SDK is pre-installed globally through npm.

JavaScript Example

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note that Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. Create a file named `region_subscriptions_example.js` with the following example code, which lists the subscribed regions for your current tenancy:

```javascript
const identity = require("oci-sdk/node_modules/oci-identity");
const common = require("oci-sdk/node_modules/oci-common");
const provider = new common.ConfigFileAuthenticationDetailsProvider();
const compartmentId = provider.getTenantId() || "";

let identityClient;

async function getSubscriptionRegions(tenancyId) {
    const regions = await identityClient.listRegionSubscriptions({
        tenancyId: tenancyId
    });
```
return regions.items.map(region => {
    return region.regionName;
});
}

(async () => {
    identityClient = await new identity.IdentityClient({
        authenticationDetailsProvider: provider
    });

    const regions = await getSubscriptionRegions(compartmentId);
    console.log("Currently subscribed to the following region(s): ",
    regions)
})();

4. Run the example:

    node region_subscriptions_example.js

**TypeScript Example**

This TypeScript example will list the subscribed regions for the current tenancy.

1. Create an empty project named ts_demo and link the global installation of oci-sdk library using the following commands:

    # create a new project folder and move into it
    mkdir ts_demo
    cd ts_demo

    # initialize a new javascript/typescript project
    npm init --y

    # link the global installation of oci-sdk to the current project
    npm link oci-sdk
    npm link @types/node

2. Create a file named `region_subscriptions_example.ts` inside your ts_demo project with the following code:

    import * as identity from "oci-sdk/node_modules/oci-identity";
    import common = require("oci-sdk/node_modules/oci-common");

    const provider: common.ConfigFileAuthenticationDetailsProvider = new common.ConfigFileAuthenticationDetailsProvider();

    const compartmentId = provider.getTenantId();

    let identityClient: identity.IdentityClient;

    export async function getSubscriptionRegions(tenancyId: string) {
        const listRegionSubscriptionsRequest:
            identity.requests.ListRegionSubscriptionsRequest = {
            tenancyId: tenancyId
        };

        const regions = await identityClient.listRegionSubscriptions(listRegionSubscriptionsRequest);
        return regions.items.map(region => {
            return region.regionName;
        });
    }

    (async () => {
    ...
identityClient = await new identity.IdentityClient({ authenticationDetailsProvider: provider });
const regions = await getSubscriptionRegions(compartmentId);
console.log("Currently subscribed to the following region(s): ", regions);
})();

3. Compile the example:

```bash
# use the TypeScript compiler to compile the example
tsc region_subscriptions_example.ts
```

4. Run the example:

```bash
# run the example using node
node region_subscriptions_example.js
```

SDK for Ruby Cloud Shell Quick Start

This quick start shows you how to quickly get started running sample code with the Oracle Cloud Infrastructure SDK for Ruby using Cloud Shell. The OCI SDK for Ruby is installed in the cloud shell environment and automatically added to your GEM_PATH.

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note that Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. Create a file named `list_users_example.rb` with the following code, which lists the users in your tenancy:

```ruby
require 'oci'
api = OCI::Identity::IdentityClient.new()
response = api.list_users(OCI.config.tenancy)
response.data.each { |user| puts user.name }
```

4. Run the example:

```bash
ruby list_users_example.rb
```

OCI Modules for PowerShell Cloud Shell Quick Start

This topic discusses how to quickly get started with the Oracle Cloud Infrastructure Modules for PowerShell using Cloud Shell.

1. Login to the Console.
2. Click the Cloud Shell icon in the Console header. Note that Cloud Shell will execute commands against the region selected in the Console's Region selection menu when Cloud Shell was started.
3. From the Cloud Shell session's command prompt, start the PowerShell environment:

```bash
user@cloudshell:oci (us-phoenix-1)$ pwsh
```
4. Run the following command to list the users in your current tenancy:

```bash
oci iam user list
```

Command Line Interface (CLI)

The CLI is a small-footprint tool that you can use on its own or with the Console to complete Oracle Cloud Infrastructure tasks. The CLI provides the same core functionality as the Console, plus additional commands. Some of these, such as the ability to run scripts, extend Console functionality.
This CLI and sample is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

The CLI is built on the Oracle Cloud Infrastructure SDK for Python and runs on Mac, Windows, or Linux. The Python code makes calls to Oracle Cloud Infrastructure APIs to provide the functionality implemented for the various services. These are REST APIs that use HTTPS requests and responses. For more information, see About the API.

**Installation:** See Quickstart on page 4195.

**Reference:** For help with a specific command, you can enter `help <command>` on the command line or view the Command Line Reference. This reference is derived from the APIs and help text in the Python source code.

**Requirements**

To install and use the CLI, you must have:

- An Oracle Cloud Infrastructure account.
- A user created in that account, in a group with a policy that grants the desired permissions. This account user can be you, another person, or a system that calls the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users. For a list of other typical Oracle Cloud Infrastructure policies, see Common Policies.
- A keypair used for signing API requests, with the public key uploaded to Oracle. Only the user calling the API should possess the private key. See Configuring the CLI.

**Note:**
To use the CLI without a keypair, you can use token-based authentication. For more information, see Token-based Authentication for the CLI on page 4200.

- A supported version of Python on a supported operating system.
- If you require FIPS-compliance, see Using FIPS-validated Libraries on page 4206.

**Supported Python Versions and Operating Systems**

The CLI supports Python versions 3.6 and later running on MacOS, Windows, or a supported Linux distribution:

- Oracle Linux 6.10, Oracle Linux 7.7 and 7.8, and Oracle Linux 8.0
- Oracle Autonomous Linux 7.8
- CentOS 7.0 and CentOS 8.x
- Ubuntu 16.04, Ubuntu 18.04, and Ubuntu 20.04

**Note:**
Newer versions of Python may not be immediately supported. The CLI might work on unlisted operating systems, but we do not test them for compatibility.

If you use the CLI installer and do not have Python on your machine, the installer offers to automatically install Python for you. If you already have Python installed on your machine, you can use the `python --version` command to find out which version is installed.

**Services Supported**

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
• Blockchain Platform
• Budgets
• Cloud Guard
• Compute Instance Agent (Oracle Cloud Agent)
• Container Engine for Kubernetes
• Content and Experience
• Core Services (Networking, Compute, Block Volume)
• Data Catalog
• Data Flow
• Data Integration
• Data Safe
• Data Science
• Data Transfer
• Database
• Database Management
• Digital Assistant
• DNS
• Email Delivery
• Events
• Functions
• File Storage
• Golden Gate
• Health Checks
• IAM
• Integration
• Key Management (for the Vault service)
• Limits
• Load Balancing
• Logging
• Logging Analytics
• Logging Search
• Logging Ingestion
• Management Agent Cloud
• Management Dashboard
• Marketplace
• Monitoring
• MySQL Database
• NoSQL Database Cloud
• Notifications
• Object Storage
• OCI Registry
• Organizations
• Operations Insights
• Optimizer
• OS Management
• Quotas
• Resource Manager
• Search
• Secret Management (for the Vault service)
• Secret Retrieval (for the Vault service)
• Service Connector Hub
• Streaming
• Support Management
• Usage
• VMWare Solution
• Web Application Acceleration and Security
• Work Requests (Compute, Database)

Contact Us

Contributions
Got a fix for a bug or a new feature you’d like to contribute? The SDK is open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the CLI is released, subscribe to the Atom feed.

Questions or Feedback
• GitHub Issues: To file bugs and feature requests only
• Developer Tools section of the Oracle Cloud forums
• My Oracle Support

Quickstart
Using the installer script and the setup command is the fastest way to get up and running with the CLI.

Installing the CLI
The installer script automatically installs the CLI and its dependencies, Python and virtualenv. Before running the installer, be sure you meet the Requirements on page 4193.

**Note:**
Oracle Autonomous Linux 7 and Cloud Shell have the CLI pre-installed.

Linux and Unix (Including Oracle Linux 8)
1. Open a terminal.
2. To run the installer script, run the following command.

   ```bash
   ```

   **Note:**
   To run a 'silent' install that accepts all default values with no prompts, use the `--accept-all-defaults` parameter.


Oracle Linux 7
If you're using Oracle Linux 7, you can use yum to install the CLI.

To use yum to install the CLI:

   ```bash
   sudo yum install python36-oci-cli
   ```
The CLI will be installed to the Python site packages:

- /usr/lib/python3.6/site-packages/oci_cli
- /usr/lib/python3.6/site-packages/services

Documentation and examples will be installed in the /usr/share/doc/python36-oci-cli-<version>/ directory.

To uninstall the CLI:

```
sudo yum remove python36-oci-cli
```

**Mac OS X**

You can use Homebrew to install, upgrade, and uninstall the CLI on Mac OS.

To install the CLI on Mac OS X with Homebrew:

```
brew update && brew install oci-cli
```

To upgrade your CLI install on Mac OS X using Homebrew:

```
brew update && brew upgrade oci-cli
```

To uninstall the CLI on Mac OS X using Homebrew:

```
brew uninstall oci-cli
```

**Windows**

1. Open the PowerShell console using the Run as Administrator option.
2. The installer enables auto-complete by installing and running a script. To allow this script to run, you must enable the RemoteSigned execution policy.

   To configure the remote execution policy for PowerShell, run the following command.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

3. Download the installer script:

   ```
   ```

4. Run the installer script with or without prompts:

   a. To run the installer script with prompts, run the following command:

   ```
   ```

   ...and respond to the Installation Script Prompts on page 4196.

   b. To run the installer script without prompting the user, accepting the default settings, run the following command:

   ```
   install.ps1 -AcceptAllDefaults
   ```

**Installation Script Prompts**

The installation script prompts you for the following information.
• If you do not have a compatible version of Python installed:
  • Windows and Linux: You are prompted to provide a location for installing the binaries and executables. The script will install Python for you.
  • MacOS: You are notified that your version of Python is incompatible. You must upgrade before you can proceed with the installation. The script will not install Python for you.
  • When prompted to upgrade the CLI to the newest version, respond with Y to overwrite an existing installation.
  • When prompted to update your PATH, respond with Y to be able to invoke the CLI without providing the full path to the executable. This will add oci.exe to your PATH.

Setting up the Config File

Before using the CLI, you must create a config file that contains the required credentials for working with Oracle Cloud Infrastructure. You can create this file using a setup dialog or manually using a text editor.

Use the Setup Dialog

To have the CLI walk you through the first-time setup process, use the `oci setup config` command. The command prompts you for the information required for the config file and the API public/private keys. The setup dialog generates an API key pair and creates the config file.

For more information about how to find the required information, see:

- Where to Get the Tenancy's OCID and User's OCID on page 4184
- Regions and Availability Domains on page 180

Manual Setup

If you want to set up the API public/private keys yourself and write your own config file, see SDK and Tool Configuration.

Tip:

Use the `oci setup keys` command to generate a key pair to include in the config file.

Next Steps

- For details on starting a session, see Starting a CLI Session on page 4207.
- Getting Started with the Command Line Interface provides an end-to-end walk-through of using the CLI to launch an instance.

Manual Installation

Instead of using the installer script as described in the Quickstart on page 4195, you can manually install the CLI and its dependencies. Before proceeding, be sure you meet the Requirements on page 4193.

Step 1: Installing Python

Python installation instructions vary for each operating system that the CLI supports.

Note:

The CLI supports only the Python versions listed in the CLI Requirements.

Windows

Install a supported version of Python from the Python Windows downloads page. During installation, choose to add Python to the PATH and/or environment variables (depending on the prompt).

Oracle Linux

Some versions of Oracle Linux come with incompatible versions of Python, and might require additional components to install the CLI. Before installing the CLI, run the following commands on a new Oracle Linux image.
Tip:
Oracle Autonomous Linux 7 comes with the CLI pre-installed.

Oracle Linux 7 and Oracle Linux 8

```
sudo yum -y update
sudo yum -y groupinstall "Development Tools"
sudo yum -y install gcc wget openssl-devel bzip2-devel libffi-devel
wget https://www.python.org/ftp/python/3.8.3/Python-3.8.3.tgz
tar xvf Python-3.8.3.tgz
cd Python-3.8*/
./configure --enable-optimizations
sudo make altinstall
```

Oracle Linux 6

```
sudo yum -y update
sudo yum -y groupinstall "Development Tools"
sudo yum -y install gcc wget openssl-devel bzip2-devel libffi-devel
wget https://www.python.org/ftp/python/3.6.3/Python-3.6.3.tgz
tar xvf Python-3.6.3.tgz
cd Python-3.6*/
./configure --enable-optimizations
sudo make altinstall
```

CentOS

Before you install the CLI, run the following commands on a new CentOS image.

CentOS 7, CentOS 8

```
sudo yum -y update
sudo yum -y groupinstall "Development Tools"
sudo yum -y install gcc wget openssl-devel bzip2-devel libffi-devel
wget https://www.python.org/ftp/python/3.8.3/Python-3.8.3.tgz
tar xvf Python-3.8.3.tgz
cd Python-3.8*/
./configure --enable-optimizations
sudo make altinstall
```

Ubuntu

Before you install the CLI, run the following commands on a new Ubuntu image.

Ubuntu 16, Ubuntu 18, and Ubuntu 20

```
sudo apt update
sudo apt install build-essential zlib1g-dev libncurses5-dev libgdbm-dev
libnss3-dev libssl1-dev libreadline-dev libffi-dev libsqlite3-dev wget
libbz2-dev
wget https://www.python.org/ftp/python/3.8.3/Python-3.8.3.tgz
tar -xf Python-3.8.3.tgz
cd Python-3.8.3
./configure --enable-optimizations
sudo make altinstall
```

Mac OS X

Mac OS X comes with Python pre-installed.
To install the latest version of Python on Mac OS X, see the official Python documentation.

**Step 2: Creating and Configuring a Virtual Environment**

The venv Python module is a virtual environment builder that lets you create isolated Python environments. We recommend installing the CLI in a virtual environment.

**Installing and Activating your Virtual Environment**

After Python is installed, set up a virtual environment for your operating system using the following steps.

**Windows**

1. Navigate to the directory in which you would like to create the virtual environment.
2. Create the virtual environment by running the following command:
   ```
   python -m venv oracle-cli
   ```
3. Activate the virtual environment by running the following command:
   ```
   oracle-cli/Scripts/activate
   ```

**Linux and Mac**

1. Navigate to the directory in which you would like to create the virtual environment.
2. Create the virtual environment by running one of the following commands, depending on the version of Python installed:
   ```
   python3.8 -m venv oracle-cli
   ```
   ```
   python3.6 -m venv oracle-cli
   ```
3. Activate the virtual environment by running the following command:
   ```
   source oracle-cli/bin/activate
   ```

**Step 3: Installing the Command Line Interface**

You can download the CLI from GitHub or install the package from Python Package Index (PyPI).

To install using the GitHub download:

- Download and unzip `oci-cli.zip`.
- Run the following command.
  ```
  pip install oci-cli-*-py2.py3-none-any.whl
  ```

To install using PyPI, run the following command:

```
pip install oci-cli
```

For information on how to start a CLI session, see Starting a CLI Session on page 4207.

**Installing Without a Virtual Environment**

We do not recommend installing the CLI in your system-wide Python and suggest that instead you install the CLI using the installer or virtual environment.

In cases where you are trying to install the CLI in your system-wide Python using the latest pip version, you might encounter conflicts with some `distutils` installed packages. Following is an example error message when this occurs:

```
sudo pip install oci-cli
```
Cannot uninstall 'requests'. It is a distutils installed project and thus we cannot accurately determine which files belong to it which would lead to only a partial uninstall.

Another option is to install the CLI for the user using the following command, although this approach is not supported:

```
pip install --user oci-cli
```

**Token-based Authentication for the CLI**

Token-based authentication for the CLI allows customers to authenticate their session interactively, then use the CLI for a single session without an API signing key. This enables customers using an identity provider that is not SCIM-supported to use a federated user account with the CLI and SDKs.

**Requirements**

The requirements are the same as those listed for the CLI in Requirements on page 4193, except that instead of a SSH keypair, you need a web browser for the authentication process.

**Starting a Token-based CLI Session**

To use token-based authentication for the CLI on a computer with a web browser:

1. In the CLI, run the following command. This will launch a web browser.

   ```
   oci session authenticate
   ```

2. In the browser, enter your user credentials. This authentication information is saved to the .config file.

**Validating a Token**

To verify that a token is valid, run the following command:

```
oci session validate --config-file <path_to_config_file> --profile <profile_name> --auth security_token
```

You should receive a message showing the expiration date for the session. If you receive an error, check your profile settings.

**Refreshing a Token**

The default token TTL is set to 1 hour before it expires and can be refreshed within the validity period up to 24 hours. To refresh the token, run the following command:

```
oci session refresh --profile <profile_name>
```

**Starting a Token-based CLI Session without a Browser**

To use token-based authentication for the CLI on a computer without a web browser, you must export a session from a web-enabled computer, then import it to the computer without a web browser.

**Exporting from Source Computer**

On the source computer with the browser:

1. In the CLI, run the following command:

   ```
   oci session authenticate
   ```

2. Enter the user credentials you wish to use on the target computer.
3. To export a zip file, run the following command:

```
oci session export --profile <profile_name> --output-file <output_filename>
```

To verify the export, see Validating a Token on page 4200.

**Importing to Target Computer**

On the target computer without the browser, run the following command in the CLI:

```
oci session import --session-archive <path_to_exported_zip>
```

You can test the import by running the following:

```
oci iam region list --config-file <path_to_config_file> --profile <profile_name> --auth security_token
```

It should return a list of regions. Successful execution of this command verifies that the token authentication is working as expected.

**Running Scripts on a Computer without a Browser**

After importing the authentication to the target computer, you can run the CLI and SDKs by using the following settings.

**For CLI**

To run scripts on the CLI, append the following suffix:

```
--config-file <path_to_config_file> --profile <profile_name> --auth security_token
```

**For SDKs**

To run SDKs on the target computer, you must read in the token file, then use it to initialize the SecurityTokenSigner.

After creating a token file as shown in Starting a Token-based CLI Session on page 4200, use the following process.

**Note:**

These code samples demonstrate how to accomplish this using the Oracle Cloud Infrastructure SDK for Python. For other SDKs, follow the same process, but adjust the syntax accordingly.

1. Read the token file from the `security_token_file` parameter of the `.config` file.

```
config = oci.config.from_file(profile_name='TokenDemo')
token_file = config['security_token_file']
token = None
with open(token_file, 'r') as f:
    token = f.read()
```

2. Read the private key specified by the `.config` file.

```
private_key = oci.signer.load_private_key_from_file(config['key_file'])
```

3. Create the initial SDK client which targets the user-specified region.

```
signer = oci.auth.signers.SecurityTokenSigner(token, private_key)
```
4. Make the identity request.

```python
result = client.list_region_subscriptions(config['tenancy'])
```

**Configuring the CLI**

You can use these optional configurations to extend CLI functionality. The CLI supports using a file for CLI-specific configurations. You can:

- Specify a default profile.
- Set default values for command options so you don't have to type them into the command line.
- Define aliases for commands. For example, using "ls" as an alias for list.
- Define aliases for options. For example, using "--ad" as an alias for --availability-domain.
- Define named queries that are passed to the --query option instead of typing a JMESPath expression on the command line.

The CLI also supports the use of environment variables to specify defaults for some options. See **CLI Environment Variables** for more information.

**CLI Configuration File**

The default location and file name for the CLI-specific configuration file is `~/.oci/oci_cli_rc`, but you can use the `OCI_CLI_RC_FILE` environment variable to modify where the CLI looks for a configuration file and its default values upon startup.

You can also explicitly specify a CLI configuration file with the `--cli-rc-file` option or with the legacy `--defaults-file` option. For example:

```bash
# Uses the file from ~/.oci/oci_cli_rc
# or OCI_CLI_RC_FILE environment variable
oci os bucket list

# Uses a custom file
oci os bucket list --cli-rc-file path/to/my/cli/rc/file
```

To set up an `oci_cli_rc` file, run the following command:

```bash
oci setup oci-cli-rc --file path/to/target/file
```

This command creates the file you specify that includes examples of default command aliases, parameter aliases, and named queries.

**Note:**

If you are using Windows, you should use backslash as the directory separator in pathnames, instead of the forward slash.

**Specifying a Default Profile**

Specify a default profile in the `OCI_CLI_SETTINGS` section of the CLI configuration file. The next example shows how to specify a default profile named IAD. The CLI looks for a profile named IAD in your `~/.oci/config` file, or any other file that you specify using the `--config-file` option or the `OCI_CLI_CONFIG_FILE` environment variable.

```ini
[OCI_CLI_SETTINGS]
default_profile=IAD
```

You can also specify a default profile by using the `--profile` option or by setting the `OCI_CLI_PROFILE` environment variable.
If a default profile value has been specified in multiple locations, the order of precedence is:

1. The value specified in the `--profile` option.
2. The value specified in the `OCI_CLI_PROFILE` environment variable.
3. The value specified in the `default_profile` field in the `OCI_CLI_SETTINGS` section of the CLI configuration file.

**Specifying Default Values**

The CLI supports using default values so that you don't have to keep typing every value into the command line. For example, instead of typing in a `--compartment-id` on each launch instance command or having to keep specifying the `--namespace` when using Object Storage commands. You can specify this information in a default values file.

Default values can be applied at different levels, from general to specific:

- Globally, across all the CLI commands.
- To a particular service, such as Compute or Object Storage.
- To a specific group, such as commands related to exporting images.
- To a specific command.

Default values are treated hierarchically, with specific values having a higher order of precedence than general values. For example, if there is a globally defined value for `compartment-id` and a specific `compartment-id` defined for the `compute instance launch` command, the CLI uses the value for the `compute instance launch` instead of the global default.

**Command Value Priority**

If a value is provided on the command line also exists in `--cli-rc-file`, the value from the command line has priority. For a command with options that take multiple values, the values are taken entirely from the command line or from `--cli-rc-file`. The 2 sources aren't merged.

**Defaults Value File Syntax**

The `--cli-rc-file` file can be divided into different sections with one or more keys per section.

**Sections**

In the next example, the file has two sections, with a key in each section. To specify which section to use, you use the `--profile` option in the CLI.

```
[DEFAULT]
compartment-id = ocid1.compartment.oc1..<unique_ID_1>
[ANOTHER_SECTION]
compartment-id = ocid1.compartment.oc1..<unique_ID_2>
```

**Keys**

Keys are named after command line options, but do not use a leading double hyphen (`--`). For example, the key for `--image-id` is `image-id`. You can specify keys for single values, multiple values, and flags.

- **Keys for Single Values.** The next example shows how to specify key values at different levels, and with different scope.

```
[DEFAULT]
# Defines a global default for bucket-name
bucket-name = my-global-default-bucket-name

# Defines a default for bucket-name, which applies to all 'compute' commands
compute.bucket-name = bucket-name-for-image-import-export
```
# Defines a default for bucket-name, which applies to all 'os object' commands (e.g., os object get)

```
os.object.bucket-name = bucket-name-for-object-commands
```

# Defines a default for bucket-name, for the 'os object multipart list' command

```
os.object.multipart.list.bucket-name = bucket-name-for-multipart-list
```

- **Keys for Multiple Values.** Some options, such as `--include` and `--exclude` on the `oci os object bulk-upload` command can be specified more than once. For example:

```
oci os object bulk-upload -ns my-namespace -bn my-bucket --src-dir my-directory --include *.txt --include *.png
```

The next example shows how you would enter the `--include` values in the `--cli-rc-file` file

```
[DEFAULT]
os.object.bulk-upload.include = *.txt
  *.png
```

In the previous example, one value is given for each line and each line must be indented underneath its key. You can use tabs or spaces and the amount of indentation doesn't matter. You can also put a value on the same line as the key, add more values on the following lines, and use a path statement for a value. For example:

```
[DEFAULT]
os.object.bulk-upload.include = *.pdf
  *.txt
  *.png
  my-subfolder/*.tiff
```

- **Keys for Flags.** Some command options are flags, like `--force`, which uses a Boolean value. To set a flag for the `--force` option, use the following command.

```
os.object.delete.force=true
```

### Specifying Command Aliases

Specify named queries in the `OCI_CLI_COMMAND_ALIASES` section of the CLI configuration file. There are two types of aliases, global aliases and command sequence aliases. The following example shows each type of alias.

```
[OCI_CLI_COMMAND_ALIASES]
# This is a global alias that lets you use "ls" instead of "list" for any
# list command in the CLI.
#
ls = list

# Command examples:
# oci os object ls or oci os compute ls

# This is a command sequence alias that lets you use "oci os object rm"
# instead of "oci os object delete".
# <alias> = <dot-separated sequence of groups and sub-groups>.<command or
group to alias>
# rm = os.object.delete
# Command example:
```
If you want to define default values for options in your CLI configuration file, you can use the alias names you have defined. For example, if you have `-ls` as an alias for `--list`, you can define a default for an availability domain when listing instances by using the following command.

```
[DEFAULT]
compute.instance.ls.compartment-id=ocid1.compartment.oc1..<unique_ID>
```

**Specifying Option Aliases**

Specify option aliases in the `OCI_CLI_PARAM_ALIASES` section of the CLI configuration file. Option aliases are applied globally. The following example shows some aliases for command options.

```
[OCI_CLI_PARAM_ALIASES]
# Option aliases either start with a double hyphen (--) or are a single
# hyphen (-) followed by a # single letter. For example: --example-alias, -e
#
--ad = --availability-domain
--dn = --display-name
--egress-rules = --egress-security-rules
--ingress-rules = --ingress-security-rules
```

If you want to define default values for options in your CLI configuration file, you can use the alias names you have defined. For example, if you have `-ad` as an alias for `--availability-domain`, you can define a default for an availability domain when listing instances by using the following command.

```
[DEFAULT]
compute.instance.list.ad=xyx:PHX-AD-1
```

**Specifying Named Queries**

If you use the `--query` parameter to filter or manipulate output, you can define named queries instead of using a JMESPath expression on the command line.

Specify named queries in the `OCI_CLI_CANNED_QUERIES` section of the CLI configuration file.

**Examples of Named Queries**

```
[OCI_CLI_CANNED_QUERIES]
# For list results, this gets the ID and display-name of each item in the
# list.
# Note that when the names of attributes have dashes in them they need to
# be surrounded
# with double quotes. This query knows to look for a list because of the
# [*] syntax
get_id_and_display_name_from_list=data[*].{id: id, "display-name": "display-
name"}

get_id_and_display_name_from_single_result=data.{id: id, "display-name":
"display-name"}

# Retrieves a comma separated string, for example:
# ocid1.instance.oc1.phx.xyz....,cli_test_instance_675195,RUNNING
#
get_id_display_name_and.lifecycle_state_from_single_result.as_csv=data.{id,
"display-name", "lifecycle-state"} | join(\',\', @)

# Retrieves comma separated strings from a list of results
get_id_display_name_and_lifecycle_state_from_list_as_csv=data[*].[join(`,`, [id, "display-name", "lifecycle-state"])][[]]

# Filters where the display name contains some text
#
# filter_by_display_name_contains_text=data[?contains("display-name", `your_text_here`)]

# Filters where the display name contains some text and pull out certain attributes(id and time-created)
#
# filter_by_display_name_contains_text_and_get_attributes=data[?contains("display-name", `your_text_here`)].{id: id, timeCreated: "time-created"}

# Get the top 5 results from a list operation
#
# get_top_5_results=data[:5]

# Get the last 2 results from a list operation
#
# get_last_2_results=data[-2:]}

You can reference any of these queries using this syntax: query://<query name>.

For example, to get id and display name from a list, run the following command.

```
oci compute instance list -c $C --query query://get_id_and_display_name_from_list
```

**Enabling Auto-complete**

If you used the CLI installer, you don't have to configure auto-complete because it's enabled automatically.

To enable auto-complete (tab completion) for a manual CLI installation, run the following command.

```
oci setup autocomplete
```

To enable auto-complete on a session by session basis, run the following command.

```
eval "$_OCI_COMPLETE=source oci"
```

**Note:**

**Support for Auto-complete on Windows**

Auto-complete on Windows is only supported if you're using PowerShell. A script runs to enable this feature. However, you must change the PowerShell execution policy to RemoteSigned. To configure this policy, run the following command at the PowerShell command line.

```
Set-ExecutionPolicy RemoteSigned
```

**Using FIPS-validated Libraries**

The CLI can be configured to use FIPS-validated libraries on Linux. The CLI is built on the Oracle Cloud Infrastructure SDK for Python and leverages operating system level cryptographic libraries.
Configuring the Environment

1. Verify the installed version of OpenSSL is FIPS-compliant. Run the following command:

   openssl version

   If "fips" is not part of the version name, you should upgrade OpenSSL to a FIPS-compliant version. You can download the latest versions of OpenSSL at: https://www.openssl.org/source/

2. Determine the location of the FIPS-compliant version of libcrypto:

   ls -l /usr/lib64/libcrypto*

3. Set the environment variable OCI_CLI_FIPS_LIBCRYPTO_FILE to the location of libcrypto:

   export OCI_CLI_FIPS_LIBCRYPTO_FILE=/path/to/libcrypto.x.x.x

   If you do not want to run this command at the start of every session, you can add it to your .bashrc or .bash_profile file.

   You can confirm that the environment variable is set properly with this command:

   set | grep OCI_CLI_FIPS_LIBCRYPTO_FILE

   You can now proceed to the standard installation process outlined in Quickstart on page 4195

Verifying the Configuration

To verify that the CLI is using the library that you specified during Configuring the CLI on page 4202, execute the following commands in Python. Be sure to do so in the same environment that the CLI uses.

   import ssl
   ssl.FIPS_mode()

   This should return 1, indicating that SSL is using the library specified by the OCI_CLI_FIPS_LIBCRYPTO_FILE environment variable.

Using the CLI

This topic describes how to use the CLI to access Oracle Cloud Infrastructure and carry out service-related tasks. This topic assumes that you have configured the CLI and are ready to start using it.

Tip:

Getting Started with the Command Line Interface provides an end-to-end walk-through of using the CLI to launch an instance.

Starting a CLI Session

MacOS, Linux, and Unix

To start a CLI session, run the following commands.

1. Open a terminal.
2. Change the working directory.

   cd myvirtualspaces/virtualenvs/cli-testing/bin

3. Run the activate batch file.

   source activate
To stop using the CLI, run the following command in a terminal.

```
deactivate
```

**Windows**

To start a CLI session, run the following commands.

1. Open the Command Prompt using the **Run as administrator** option.
2. Change the working directory.

```
cd myvirtualspaces/virtualenvs/cli-testing/Scripts
```
3. Run the activate batch file.

```
activate
```

To stop using the CLI, run the following command from the command line.

```
deactivate
```

**Command Line Syntax**

Most commands must specify a service, followed by a resource type and then an action. The basic command line syntax is:

```
oci <service> <type> <action> <options>
```

For example, this syntax is applied as follows:

- **compute** is the `<service>`
- **instance** is the resource `<type>`
- **launch** is the `<action>`, and
- the rest of the command string consists of `<options>`.

The following command to launch an instance shows a typical command line construct.

```
oci compute instance launch --availability-domain "EMIr:PHX-AD-1" --compute.id oci1.compartment.ocl..aaaaaaaaa13gzi jdli eqeyq35nz5zx1i26astxxhgo12pgeyqdr gnx7jhwa
--shape "VM.Standard1.1" --display-name "Instance 1 for sandbox" --image-id
oci1.image.ocl.phx.aaaaaaaaajutj4qjxihp14mboabsa27mrpusygv6gurp47kat5z7vljmq3puq
--subnet-id
oci1.subnet.ocl.phx.aaaaaaaaaypsr25bzjmjyn6xgwcrgxd3dbhiha6lodzus3gafscirbhj5bpa
```

In the previous example, you can provide a friendly name for the instance using the **--display-name** option.

Avoid entering confidential information.

**Basic Examples**

This section provides examples of basic operations using the CLI.

**Note:**

Using Environment Variables for OCIDs

Several of the CLI examples use environment variables for OCIDs, such as:

- `$T` for a tenancy OCID
- `$C` for a compartment OCID
For example:

T=ocid1.tenancy.oc1..aaaaaaaaba3pv6wm2ytdrwrz32uzr4h25vkcr4jqaee5f15p2b2qst
C=ocid1.compartment.oc1..aaaaaaarahifmvrvuqtye5q66rck6copzqck3ukc5f1drwpp2

To get a namespace, run the following command.

```
oci os ns get
```

To list compartments, run the following command.

```
oci iam compartment list --tenancy-id $T
```

To get a list of buckets, run the following command.

```
oci os bucket list --namespace mynamespace --compartment-id $C
```

To list users and limit the output, run the following command.

```
oci iam user list --compartment-id $T --limit 5
```

To add a user to a group, run the following command.

```
oci iam group add-user --user-id ocid1.user.oc1..aaabcaaaxkkhhtmghvqqq7rgvzwuj3drwmt1sgz6bfo7y4uc5sprzli377q --group-id ocid1.group.oc1..aaabcaaa66plootq6uwwxhfdw2lsdqtegeb6l4pjsv5eeuenxrauujj35b7b
```

**Getting Help with Commands**

You can get help for any command using `--help`, `-h`, or `-?`. For example:

```
oci --help
```

```
oci os bucket -h
```

```
oci os bucket create -?
```

**Viewing all the CLI Help**

You can view the command line help.

**Determining the Installed Version of the CLI**

To get the installed version of the CLI, run the following command.

```
oci --version
```

**Using Dates and Times in CLI Commands**

The CLI supports the following accepted date formats.

- UTC with milliseconds
  
  Format: `YYYY-MM-DDTHH:mm:ss.sssTZD`, Example: `2017-09-15T20:30:00.123Z`

- UTC without milliseconds
  
  Format: `YYYY-MM-DDTHH:mm:sssTZD`, Example: `2017-09-15T20:30:00Z`
- UTC with minute precision
  Format: YYYY-MM-DDTHH:mmTZD, Example: 2017-09-15T20:30Z

- Timezone with milliseconds
  Format: YYYY-MM-DDTHH:mm:ss.sssTZD, Example: 2017-09-15T12:30:00.456-08:00

- Timezone without milliseconds
  Format: YYYY-MM-DDTHH:mm:ssTZD, Example: 2017-09-15T12:30:00-08:00

- Timezone with offset with minute precision
  Format: YYYY-MM-DDTHH:mmTZD, Example: 2017-09-15T12:35-08:00

- Date Only (This date will be taken as midnight UTC of that day)
  Format: YYYY-MM-DD, Example: 2017-09-15

- Epoch seconds
  Example: 1412195400

**Note:**
In our datetime formats, the T can be replaced with a space.
For example, both "2017-09-15 20:30:00.123Z" and 2017-09-15T20:30:00.123Z are acceptable. (Note that if you do not include the T, you must wrap the value in quotes.) We also support time zones with and without the colon. Both +10:00 and +1000 are acceptable.

**Managing CLI Input and Output**
The CLI provides several options for managing command input and output.

**Passing Complex Input**
Complex input, such as arrays and objects with more than one value, are passed in JSON format and can be provided as a string at the command line, as a file, or as a command line string and as a file.

**MacOS, Linux, or Unix**
The following command shows how to pass two values for the --metadata object.

```
oci os bucket create -ns mynamespace --name mybucket --metadata 
"{"key1":"value1","key2":"value2"}" --compartment-id
ocid1.compartment.oc1..aaaaaaaarhifmrsvqyve5g6rcz6cpzqck3ukc5f1drwpp2jojdcypxfga
```

**Windows**
On Windows, to pass complex input to the CLI as a JSON string, you must enclose the entire block in double quotes. Inside the block, each double quote for the key and value strings must be escaped with a backslash (\) character.

The following command shows how to pass two values for the --metadata object on Windows.

```
oci os bucket create -ns mynamespace --name mybucket --metadata 
"{"key1":"value1","key2":"value2"}" --compartment-id
ocid1.compartment.oc1..aaaaaaaarhifmrsvqyve5g6rcz6cpzqck3ukc5f1drwpp2jojdcypxfga
```
Note:

JSON Errors

The error message "Parameter '<PARAMETER NAME>' must be in JSON format." indicates that the value you passed for the parameter with name "PARAMETER NAME" was not valid JSON. This error is typically a result of the JSON string not being escaped correctly.

For more information about using JSON strings, see Advanced JSON Options

Format Output as a Table

By default, all responses to a command are returned in JSON format. For example, a response like the following is returned when you issue the command to get a list of regions.

```json
{
  "data": [
    {
      "key": "FRA",
      "name": "eu-frankfurt-1"
    },
    {
      "key": "IAD",
      "name": "us-ashburn-1"
    },
    {
      "key": "ICN",
      "name": "ap-seoul-1"
    },
    {
      "key": "PHX",
      "name": "us-phoenix-1"
    },
    {
      "key": "LHR",
      "name": "uk-london-1"
    },
    {
      "key": "NRT",
      "name": "ap-tokyo-1"
    },
    {
      "key": "YYZ",
      "name": "ca-toronto-1"
    }
  ]
}
```

In some cases, readability can become an issue, which is easily resolved by formatting a response as a table. To get a response to a command formatted as a table, run the following command.

```
oci iam region list --output table
```

The following sample list of regions is returned as a two column table.

```
+-----+----------------+
| key | name            |
+-----+----------------+
| FRA | eu-frankfurt-1  |
| IAD | us-ashburn-1    |
```

Filter Output

You can filter output using the JMESPath query option for JSON. Filtering is very useful when dealing with large amounts of output. For example, run the following command with the output table option to get a list of images.

```bash
oci compute image list -c
ocid1.compartment.oc1..aaaaaaaapxgklgmujxjzx2ypptfjrcieq7rrrob2u2zbesh3wlafsgthhqtea
--output table
```

The image information is returned in table format, but too much data is returned, which overflows the width of the terminal. In addition, you might not need all the information that's returned.

```
<table>
<thead>
<tr>
<th>base-image-id</th>
<th>compartment-id</th>
<th>create-image-allowed</th>
<th>display-name</th>
<th>id</th>
<th>lifecycle-state</th>
<th>operating-system</th>
<th>operating-system-version</th>
<th>time-created</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle-Linux-7.4-2017.09.29-0</td>
<td>None</td>
<td>None</td>
<td>True</td>
<td>Oracle-Linux-7.4-2017.09.29-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaaa32xpzlbrdnocjtzv2tvxcofjfc55vdcmpxdlbohmtt7encpiana</td>
<td>AVAILABLE</td>
<td>Oracle Linux</td>
<td></td>
</tr>
<tr>
<td>Oracle-Linux-7.4-2017.08.25-1</td>
<td>None</td>
<td>None</td>
<td>True</td>
<td>Oracle-Linux-7.4-2017.08.25-1</td>
<td>ocid1.image.oc1.phx.aaaaaaaaajan2cd2g65tphibaegiz41bs422rdc73okcu7dt2uya6p5szywsa</td>
<td>AVAILABLE</td>
<td>Oracle Linux</td>
<td></td>
</tr>
<tr>
<td>Oracle-Linux-7.4-2017.08.25-0</td>
<td>None</td>
<td>None</td>
<td>True</td>
<td>Oracle-Linux-7.4-2017.08.25-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaaa32xpzlbrdnocjtzv2tvxcofjfc55vdcmpxdlbohmtt7encpiana</td>
<td>AVAILABLE</td>
<td>Oracle Linux</td>
<td></td>
</tr>
</tbody>
</table>
```
You can limit the amount of data returned by combining the `--query` option with `--output table` to get the information you want from a command.

To get filtered image information returned in a table format, run the following command.

```bash
oci compute image list -c
ocidl.compartment.oc1..aaaaaaaapxgklgmujxjzx2ypptfjrcieq7rrob2u2zbesh3wlafsgthhqtea
--output table --query "data [*].{ImageName:"display-name", OCID:id}"
```

The previous command returns the following image information, formatted as a two column table.

<table>
<thead>
<tr>
<th>ImageName</th>
<th>OCID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows-Server-2012-R2-Standard-Edition-VM-2017.04.03-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaa53cliasgqvmutf1wqkafeb0b2y4wjebeci5szc4eus5yy2e2b7ua</td>
</tr>
<tr>
<td>Oracle-Linux-7.4-2017.09.29-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaa32xpx2brrdrknqctzv2tvxc0fjc55vdcmpxdlbohmtt7encpana</td>
</tr>
<tr>
<td>Oracle-Linux-7.4-2017.08.25-1</td>
<td>ocid1.image.oc1.phx.aaaaaaaajan2cd2g65tphaiegliz4l6s422rdc73okcu7d2uya6p5szywsa</td>
</tr>
<tr>
<td>Oracle-Linux-7.4-2017.08.25-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaaabf12bmaygtu4riw3vcuowl15cqwzdqzwmdqneobybcfcn2pgyc6a</td>
</tr>
<tr>
<td>Oracle-Linux-7.4-2017.07.17-1</td>
<td>ocid1.image.oc1.phx.aaaaaaaa7jvfm572d4ehcgh3iijapvhr525voie133ispumygi3k17mph55ha</td>
</tr>
<tr>
<td>Oracle-Linux-7.3-2017.07.17-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaa5y6p3riqthxzov7fdngi4tsteganmao54nq3pyxu3hxucuzmoa</td>
</tr>
<tr>
<td>Oracle-Linux-6.9-2017.09.29-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaa2dp23dmn6mj53zeyap5bdvqtq7xfmr5kg5xulr1dbjzdavaaoj6a</td>
</tr>
<tr>
<td>Oracle-Linux-6.9-2017.08.25-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaav1wctg2mx6c4q44gwvbix6g7xqkowe3tbwbjnfbybwmexpnq</td>
</tr>
<tr>
<td>Oracle-Linux-6.9-2017.07.17-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaa3s4v5eamndtyghb4b2mhokbkwjwzb3eowyy5cebmrxsoxvoopixa</td>
</tr>
<tr>
<td>CentOS-7-2017.09.14-0</td>
<td>ocid1.image.oc1.phx.aaaaaaaaa0uqvtzhqplzyuesb5tctig6grwoavnfnikkwvuyunu7z646z72ahcq</td>
</tr>
</tbody>
</table>
For more information about the JMESPath query language for JSON, see [JMESPath](https://docs.oracle.com/en-us/m-metal/oci/developer_tools/index.html).

**Advanced JSON Options**

You can get the correct JSON format for command options and commands.

- For a command option, use `--generate-param-json-input` and specify the command option that you want to get the JSON for. To generate the JSON for creating or updating a security rule, run the following command.

  ```bash
  oci network security-list create --generate-param-json-input ingress-security-rules
  ```

- For an entire command, use `--generate-full-command-json-input`. To generate the JSON for launching an instance, run the following command.

  ```bash
  oci compute instance launch --generate-full-command-json-input
  ```

**Order of Precedence for JSON Input**

The CLI supports combining arguments on the command line with file input. However, if the same values are provided in a file and on the command line, the command line takes precedence.

**Using a JSON File for Complex Input**

You can pass complex input from a file by referencing it from the command line. For Windows users, this removes the requirement of having to escape JSON text. You provide a path to the file using the `file://` prefix.

**Path Types**

Using `testfile.json` as an example, the following types of paths are supported.

- Relative paths from the same directory, for example: `file://testfile.json` and `file://relative/path/to/testfile.json`
- Absolute paths on Linux, MacOS or Unix, for example: `file:///absolute/path/to/testfile.json`
- Full file paths on Windows, for example: `file://C:\path\to\testfile.json`

**Note:**

File Path Expansions

File path expansions, such as `~` and `./`, are supported. On Windows, the `~` expression expands to your user directory, which is stored in the...
%USERPROFILE% environment variable. Using environment variables in paths is also supported.

**File Locations**

The following file locations are supported.

- Your home directory.
  ```bash
  oci os bucket create -ns mynamespace --name mybucket --compartment-id ocid1.compartment.oc1..aaaaaaaarhifmvrvuqtye5q66rck6copzqck3ukc5f1drwpp2jojdcypxfga --metadata file://~/testfile.json
  ```

- The current directory.
  ```bash
  oci os bucket create -ns mynamespace --name mybucket --compartment-id ocid1.compartment.oc1..aaaaaaaarhifmvrvuqtye5q66rck6copzqck3ukc5f1drwpp2jojdcypxfga --metadata file://testfile.json
  ```

- The /tmp directory (Linux, Unix, or MacOS).
  ```bash
  oci os bucket create -ns mynamespace --name mybucket --compartment-id ocid1.compartment.oc1..aaaaaaaarhifmvrvuqtye5q66rck6copzqck3ukc5f1drwpp2jojdcypxfga --metadata file:///tmp/testfile.json
  ```

- The C:\temp directory (Windows).
  ```bash
  oci os bucket create -ns mynamespace --name mybucket --compartment-id ocid1.compartment.oc1..aaaaaaaarhifmvrvuqtye5q66rck6copzqck3ukc5f1drwpp2jojdcypxfga --metadata file://C:\temp\testfile.json
  ```

**Examples of Using a JSON File as Input**

The examples in this section use JSON that's generated for a command option and an entire command. The JSON is saved in a file, edited, and then used as command line input.

**Use File Input for a Command Option**

This end-to-end example shows how to generate the JSON for a security list id option used to create a subnet. The JSON is saved in a file, edited, and then used as command line input.

Response from the Command

```
[
  {
    "icmpOptions": {
      "code": 0,
      "type": 0
    },
    "isStateless": true,
    "protocol": "string",
    "source": "string",
    "tcpOptions": {
      "destinationPortRange": {
        "max": 0,
        "min": 0
      },
      "sourcePortRange": {
        "max": 0,
        "min": 0
      }
    }
  },
  {
    "icmpOptions": {
      "code": 0,
      "type": 0
    },
    "isStateless": true,
    "protocol": "string",
    "source": "string",
    "tcpOptions": {
      "destinationPortRange": {
        "max": 0,
        "min": 0
      },
      "sourcePortRange": {
        "max": 0,
        "min": 0
      }
    }
  }
]`
Response from the Command

{
  "assignPublicIp": true,
  "availabilityDomain": "string",
  "compartmentId": "string",
  "displayName": "string",
  "extendedMetadata": {
    "string1": {
      "string1": "string",
      "string2": "string"
    },
    "string2": {
      "string1": "string",
      "string2": "string"
    }
  },
  "hostnameLabel": "string",
  "imageId": "string",
  "metadata": {
    "string1": {
      "string1": "string",
      "string2": "string"
    },
    "string2": {
      "string1": "string",
      "string2": "string"
    }
  }
}
Use a JSON File as Input for a Security List Option

1. To generate the JSON for the `security-list-ids` option, run the following command.

   ```shell
   oci network subnet create --generate-param-json-input security-list-ids
   ```

2. Create a file and add the following content, which was returned in step 1. This content doesn't have to be escaped or on a single line, it just has to contain valid JSON.

   ```json
   ["string", "string"]
   ```

3. Edit the file and replace the "string" values with values, as shown in the following example.

   ```json
   [
   "ocid1.securitylist.oc1.phx.aaaaaaaaw7c62ybv4676muq5tdrwup3v2maiquhbkbb4sf75tjc5dm64y",
   "ocid1.securitylist.oc1.phx.aaaaaaaa7snx4jh5drwo2h33rwcdeqev6elir555hnrhij2yfnfedsfons5rct
   
   ```

4. Save the file as "security-list.json".

5. To create the subnet using "security-list.json" as input, run the following command.

   ```shell
   oci network subnet create --vcn-id ocid1.vcn.oc1.phx.aaaaaaaa6wmuahgxejkvy7ukyroqdrwlrumt16vyisxxavagiqw2eeet2sa
   --compartment-id ocid1.compartment.oc1..aaaaaaaal3gzijdliedxxhgl2rgndrwyg935n5zxi126astpgeyq7jnhwa
   --availability-domain "EMIr:PHX-AD-1" --display-name TESTSUB --dns-label "testinstances" --cidr-block "10.0.0.0/16" --security-list-ids file://security-list.json
   ```

### Use File Input for an Entire Command

This end-to-end example shows how to generate the JSON to create a virtual cloud network (VCN). The JSON is saved in a file, edited, and then used as command line input.

Use a JSON File as Input to Create a VCN

1. To generate the JSON needed to create a VCN, run the following command.

   ```shell
   oci network vcn create --generate-full-command-json-input
   ```

2. Create a file and add the following content, which was returned in step 1. This content doesn't have to be escaped or on a single line, it just has to contain valid JSON.

   ```json
   {
   "cidrBlock": "string",
   "compartmentId": "string",
   "displayName": "string",
   "dnsLabel": "string"
   }
   ```

### Use File Input for an Entire Command

This end-to-end example shows how to generate the JSON to create a virtual cloud network (VCN). The JSON is saved in a file, edited, and then used as command line input.

Use a JSON File as Input to Create a VCN

1. To generate the JSON needed to create a VCN, run the following command.

   ```shell
   oci network vcn create --generate-full-command-json-input
   ```

2. Create a file and add the following content, which was returned in step 1. This content doesn't have to be escaped or on a single line, it just has to contain valid JSON.

   ```json
   {
   "cidrBlock": "string",
   "compartmentId": "string",
   "displayName": "string",
   "dnsLabel": "string"
   }
   ```
3. Edit the file and replace the "string" values with values, as shown in the following example.

```json
{
   "cidrBlock": "10.0.0.0/16",
   "compartmentId": "ocid1.compartment.oc1..aaaaaaaal3gzijdliedxxhjqol2rggnrdwyyg35nz5zxil26astpgeyq7jnhw",
   "displayName": "TestVCN",
   "dnsLabel": "testdns"
}
```

4. Save the file and name it "create-vcn.json"

5. To create the VCN using "create-vcn.json" as input, run the following command.

```
oci network vcn create --from-json file://create-vcn.json
```

**Advanced Examples**

The following examples show how you can use the CLI to complete complex tasks in Oracle Cloud Infrastructure.

**Working with Object Storage**

You can use the CLI for several object operations with the Object Storage service.

**Uploading and Downloading Files**

Objects can be uploaded from a file or from the command line (STDIN), and can be downloaded to a file or to the command line (STDOUT).

Upload an object:

```
oci os object put -ns mynamespace -bn mybucket --name myfile.txt --file /Users/me/myfile.txt --metadata '{"key1":"value1","key2":"value2"}"
```

Upload object contents from the command line (STDIN):

```
oci os object put -ns mynamespace -bn mybucket --name myfile.txt --file <---'object content'
```

Download an object:

```
oci os object get -ns mynamespace -bn mybucket --name myfile.txt --file /Users/me/myfile.txt
```

Print object contents to the command line (STDOUT):

```
oci os object get -ns mynamespace -bn mybucket --name myfile.txt --file -
```

**Bulk Operations in Object Storage**

The CLI supports the following bulk operations in Object Storage:

- Uploading files in a directory and all its subdirectories to a bucket

```
# Upload all the files in a directory.
oci os object bulk-upload -ns mynamespace -bn mybucket --src-dir path/to/upload/directory
```
• Downloading all objects, or all the objects that match a specified prefix, in a bucket

```bash
# Download all the objects.
oci os object bulk-download -ns mynamespace -bn mybucket --download-dir path/to/download/directory

# Download all the objects that match the specified prefix.
oci os object bulk-download -ns mynamespace -bn mybucket --download-dir path/to/download/directory --prefix myprefix
```

• Deleting all objects, or all the objects that match a specified prefix, in a bucket

```bash
# Delete all the objects.
oci os object bulk-delete -ns mynamespace -bn mybucket

# Delete objects that match the specified prefix.
oci os object bulk-delete -ns mynamespace -bn mybucket --prefix myprefix
```

Bulk operations support several options that let you:

• Overwrite or skip files/objects using `--overwrite` or `--no-overwrite`. (**Note:** If you pass neither of these options you are prompted for confirmation every time there is something to overwrite.)

• Limit delete, upload, or download operations using `--prefix` and/or `--delimiter`

• Preview a bulk deletion with `--dry-run`

To get more information about the commands for bulk operations, run the following help commands:

```bash
# bulk-upload
oci os object bulk-upload -h

# bulk-download
oci os object bulk-download -h

# bulk-delete
oci os object bulk-delete -h
```

**Multipart Operations in Object Storage**

Multipart operations for Object Storage include object uploads and downloads.

**Multipart Uploads**

Large files can be uploaded to Object Storage in multiple parts to speed up the upload. By default, files larger than 128 MiB are uploaded using multipart operations. You can override this default by using the `--no-multipart` option.

You can configure the following options for the `oci os object put` command:

• `--no-multipart` overrides an automatic multipart upload if the object is larger than 128 MiB. The object is uploaded as a single part, regardless of size.

• `--part-size` in MiB, to use in a multipart operation. The default part size is 128 MiB and a part size that you specify must be greater than 10 MiB. If the object is larger than the `--part-size`, it is uploaded in multiple parts.

• `--parallel-upload-count`, to specify the number of parallel operations to perform. You can use this value to balance resources and upload times. A higher value may improve times but consume more system resources and network bandwidth. The default value is 10.

The `--resume-put` command allows you to resume a large file upload in cases where the upload was interrupted.
Multipart Uploads from STDIN

Objects uploaded from STDIN are uploaded in multiple parts. If the object content is smaller than 10 MiB, the upload is only 1 part, and the MultipartUpload API is used for the upload. Specifying --no-multipart when uploading from STDIN will result in an error.

The following example shows the command for a multipart upload if the object is larger than 200 MiB.

```bash
oci os object put -ns my-namespace -bn my-bucket --file path/to/large/file --part-size 200
```

For more information about multipart uploads, see Using Multipart Uploads on page 3477.

Multipart Downloads

Large files can be downloaded from Object Storage in multiple parts to speed up the download.

You can configure the following options for the `oci os object get` command:

- `--multipart-download-threshold` lets you specify the size, in MiB at which an object should be downloaded in multiple parts. This size must be at least 128 MiB.
- `--part-size`, in MiB, to use for a download part. This gives you the flexibility to use more (smaller size) or fewer (larger size) parts as appropriate for your requirements. For example, compute power and network bandwidth. The default minimum part size is 120 MiB.
- `--parallel-download-count` lets you specify how many parts are downloaded at the same time. A higher value may improve times but consume more system resources and network bandwidth. The default value is 10.

The following example shows the command to download any object with a size greater than 500 MiB. The object is downloaded in 128 MiB parts.

```bash
oci os object get -ns my-namespace -bn my-bucket --name my-large-object --multipart-download-threshold 500 --part-size 128
```

Upgrading the CLI

If you installed the CLI manually, use one of the following commands to upgrade the CLI.

- To upgrade a standard installation, run the following command.
  ```bash
  pip install oci-cli --upgrade
  ```
- To upgrade a standard virtualenv installation, run the following command.
  ```bash
  cli-testing/bin/pip install oci-cli --upgrade
  ```

If you installed the CLI using the install script, use the following process to upgrade the CLI:

- Run the install script and specify the same install directory.
- When prompted, reply Y to remove the existing directory.

Upgrading the CLI on Mac OS X with Homebrew

Homebrew offers a convenient way to manage your CLI install on Mac OS.

To upgrade your CLI install using Homebrew:

```bash
brew update && brew upgrade oci-cli
```
Uninstalling the CLI

For Manual Installations
If you manually installed the CLI using pip, run the following command:

```
pip uninstall oci-cli
```

If you manually installed the CLI in a virtual environment, run the following command:

```
<path/to/virtualenv>/bin/pip uninstall oci-cli
```

For Script Installations
If you used the install script and the default installation location, you should delete the following directories.

On Windows:

- %USERPROFILE%/lib/oracle-cli
- %USERPROFILE%/bin/oci
- %USERPROFILE%/bin/oci-cli-scripts

On Mac:

- $HOME/lib/oracle-cli
- $HOME/bin/oci
- $HOME/bin/oci-cli-scripts

If you used the install script, but installed to a custom location, you should delete the directories at that location.

Uninstalling Python

The script also installs Python as a dependency if it was not already installed. In Windows 10, you can uninstall Python in Control Panel or at the command line.

Using Control Panel

To uninstall Python in Control Panel, select Programs and Features. Right-click Python and select Uninstall. For more information, see Repair or remove programs in Windows 10.

Using the Command Line

To uninstall Python at the command line, run the following command:

```
msiexec /x python<version>.msi
```

If you do not have the MSI file, you can also use the package or product code. For more information, see Using the Windows Installer.

Uninstalling the CLI on Mac OS X with Homebrew

To unsinstall the CLI from Mac OS X using Homebrew:

```
brew uninstall oci-cli
```

Troubleshooting the CLI

This topic describes how to resolve issues that you might encounter when installing Python or the CLI, or when using the CLI.
Service Errors

Any operation resulting in a service error causes an error of type "ServiceError" to be returned by the CLI. For information about common service errors that Oracle Cloud Infrastructure returns, see API Errors.

Oracle Linux Permissions Issues

On Oracle Linux 7.3, if you encounter permission issues when running pip install, you might need to use sudo.

oci Command Not Found

If the oci command isn't found, this can be caused by one of the following reasons:

• pip installed the package to a different virtual environment than your active one.
• You switched to a different active virtual environment after you installed the CLI.

To determine where the CLI is installed, run the which pip and which oci commands.

Wheel File Won't Install

If the wheel file won't install, verify that pip is up to date. To update pip, run the pip install -U pip command. Try to install the wheel again.

Windows Issues

If the oci command isn't found, make sure that the oci.exe location is in your path (for example, the Scripts directory in your Python installation).

Contact Information

If you want to contribute ideas, report a bug, get notified about updates, have questions, or want to give feedback, use one of the following links.

Contributions

Got a fix for a bug, or a new feature you'd like to contribute? The CLI is open source and accepting pull requests on GitHub.

Notifications

To be notified when a new version of the CLI is released, subscribe to the Atom feed.

Questions or Feedback

Ways to get in touch:

• GitHub: To file bugs and feature requests only.
• Stack Overflow: Use the oracle-cloud-infrastructure and oci-cli tags in your post.
• Developer Tools section of the Oracle Cloud forums
• My Oracle Support

CLI Environment Variables

The Oracle Cloud Infrastructure CLI supports the use of environment variables to specify default values for some options.

Environment Variables

The following table lists the available environment variables and their corresponding CLI options or ~/.oci/config entries.
<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>CLI option</th>
<th>OCI config entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCI_CLI_PROFILE</td>
<td>--profile</td>
<td>Specified by [DEFAULT]</td>
<td>The profile in the OCI config file to load. This profile will also be used to locate any default parameter values which have been specified in the OCI CLI-specific configuration file.</td>
</tr>
<tr>
<td>OCI_CLI_USER</td>
<td>n/a</td>
<td>user</td>
<td>The OCID of the user calling the API. To get the value, see Required Keys and OCIDs on page 4179. Example: ocid1.user.oc1..&lt;unique_ID&gt;</td>
</tr>
<tr>
<td>OCI_CLI_REGION</td>
<td>--region</td>
<td>region</td>
<td>An Oracle Cloud Infrastructure region. See Regions and Availability Domains on page 180. Example: us-ashburn-1</td>
</tr>
<tr>
<td>OCI_CLI_FINGERPRINT</td>
<td>n/a</td>
<td>fingerprint</td>
<td>The fingerprint for the public key that was added to this user. To get the value, see Required Keys and OCIDs on page 4179. Example: 20:3b:97:13:55:1c:5b:0d:d3:37:d8:50:4e:c5:3a:34</td>
</tr>
<tr>
<td>OCI_CLI_KEY_FILE</td>
<td>n/a</td>
<td>key_file</td>
<td>The full path and filename of the private key. Important: The key pair must be in PEM format. For instructions on generating a key pair in PEM format, see Required Keys and OCIDs on page 4179. If you encrypted the key with a passphrase, you must also include the pass_phrase entry in the config file. Example: ~/.oci/oci_api_key.pem</td>
</tr>
<tr>
<td>Environment Variable</td>
<td>CLI option</td>
<td>OCI config entry</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OCI_CLI_TENANCY</td>
<td>n/a</td>
<td>tenancy</td>
<td>The OCID of your tenancy. To get the value, see Required Keys and OCIDs on page 4179. Example: ocid1.tenancy.oc1..&lt;unique_ID&gt;</td>
</tr>
<tr>
<td>OCI_CLI_ENDPOINT</td>
<td>--endpoint</td>
<td>n/a</td>
<td>The value to use as the service endpoint, including any required API version path. Example: <a href="https://iaas.us-phoenix-1.oracle.com/20160918">https://iaas.us-phoenix-1.oracle.com/20160918</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> The <strong>--region</strong> parameter is the recommended way of targeting different regions. This value can also be set in the OCI CLI-specific configuration file. See Configuring the CLI on page 4202 for more information.</td>
</tr>
<tr>
<td>OCI_CLI_CONFIG_FILE</td>
<td>--config-file</td>
<td>n/a</td>
<td>The path to the OCI config file.</td>
</tr>
<tr>
<td>OCI_CLI_RC_FILE</td>
<td>--cli-rc-file</td>
<td>n/a</td>
<td>The path to the OCI CLI-specific configuration file, containing parameter default values and other configuration information such as command aliases and predefined queries. See Configuring the CLI on page 4202 for more information.</td>
</tr>
<tr>
<td>OCI_CLI_CERT_BUNDLE</td>
<td>--cert-bundle</td>
<td>n/a</td>
<td>The full path to a CA certificate bundle to be used for SSL verification.</td>
</tr>
</tbody>
</table>
Software Development Kits and Command Line Interface

Oracle Cloud Infrastructure provides a number of Software Development Kits (SDKs) and a Command Line Interface (CLI) to facilitate development of custom solutions.

- Software Development Kits (SDKs) Build and deploy apps that integrate with Oracle Cloud Infrastructure services. Each SDK provides the tools you need to develop an app, including code samples and documentation to create, test, and troubleshoot. In addition, if you want to contribute to the development of the SDKs, they are all open source and available on GitHub.
  - SDK for Java
  - SDK for Python
  - SDK for TypeScript and JavaScript
  - SDK for .NET
  - SDK for Go
  - SDK for Ruby
- Command Line Interface (CLI) on page 4192 The CLI provides the same core capabilities as the Oracle Cloud Infrastructure Console and provides additional commands that can extend the Console's functionality. The CLI is convenient for developers or anyone who prefers the command line to a GUI.
- PL/SQL SDK The Oracle Cloud Infrastructure SDK for PL/SQL enables you to write code to manage Oracle Cloud Infrastructure resources. The latest version of the PL/SQL SDK is pre-installed by Oracle for all Autonomous Databases using shared Exadata infrastructure.

SDK for Java

The Oracle Cloud Infrastructure SDK for Java enables you to write code to manage Oracle Cloud Infrastructure resources.

This SDK and sample is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

Download: GitHub or Maven.
Tip:

The SDK for Java is pre-configured with your credentials and ready to use immediately from within Cloud Shell. For more information on using the SDK for Java from within Cloud Shell, see SDK for Java Cloud Shell Quick Start on page 4187.

Requirements

To use the SDK for Java, you must have the following:

- An Oracle Cloud Infrastructure account.
- A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users on page 57. For a list of typical policies you may want to use, see Common Policies on page 2142.
- A key pair used for signing API requests, with the public key uploaded to Oracle. Only the user calling the API should be in possession of the private key. For more information, see Configuring the SDK on page 4228.
- Java 8
- A TTL value of 60. For more information, see Configuring the SDK on page 4228.

Services Supported

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Cloud Guard
- Compute Instance Agent (Oracle Cloud Agent)
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Data Catalog
- Data Flow
- Data Integration
- Data Science
- Data Safe
- Data Transfer
- Database
- Database Management
- Digital Assistant
- DNS
- Email Delivery
- Events
- File Storage
- Functions
- Golden Gate
- Health Checks
Developer Tools

- IAM
- Integration
- Key Management (for the Vault service)
- Limits
- Load Balancing
- Logging
- Logging Analytics
- Logging Search
- Logging Ingestion
- Management Agent Cloud
- Management Dashboard
- Marketplace
- Monitoring
- MySQL Database
- NoSQL Database Cloud
- Notifications
- Object Storage
- OCI Registry
- Operations Insights
- Optimizer
- Organizations
- OS Management
- Quotas
- Resource Manager
- Roving Edge Infrastructure
- Search
- Secret Management (for the Vault service)
- Service Connector Hub
- Streaming
- Support Management
- Usage
- VMWare Solution
- Web Application Acceleration and Security
- Work Requests (Compute, Database)

Contact Us

Contributions
Got a fix for a bug or a new feature you’d like to contribute? The SDK is open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the SDK for Java is released, subscribe to the Atom feed.

Questions or Feedback
- GitHub Issues: To file bugs and feature requests only
- Stack Overflow: Please use the oracle-cloud-infrastructure and oci-java-sdk tags in your post
- Developer Tools section of the Oracle Cloud forums
- My Oracle Support
**Getting Started**

This topic describes how to install and configure the Oracle Cloud Infrastructure SDK for Java.

**Tip:**

The SDK for Java is pre-configured with your credentials and ready to use immediately from within Cloud Shell. For more information on using the SDK for Java from within Cloud Shell, see **SDK for Java Cloud Shell Quick Start** on page 4187.

Installing with Resource Manager

You can use Resource Manager to install the Oracle Cloud Development Kit on a Compute instance in your compartment. The Oracle Cloud Development Kit includes the SDK for Java, along with other Oracle development tools.

Downloading the SDK from GitHub

You can download the SDK for Java as a zip archive from GitHub. It contains the SDK, all of its dependencies, documentation, and examples. For best compatibility and to avoid issues, use the version of the dependencies included in the archive. Some notable issues are:

- Bouncy Castle: The SDK bundles 1.60 (included in this distribution). If you need FIPS compliance, see **Using BC-FIPS Instead of Bouncy Castle** on page 4232.
- Jersey Core and Client: The SDK bundles 2.24.1, which is required to support large object uploads to Object Storage. Older versions will not support uploads greater than ~2.1 GB.
- Jax-RS API: The SDK bundles 2.0.1 of the spec. Older versions will cause issues.

**Note:**

The SDK for Java is bundled with Jersey (included in this distribution), but you can also use your own JAX-RS implementation. For details, see **Using Your Own JAX-RS Implementation** on page 4233.

Downloading the SDK from Maven or JCenter

Maven Central and JCenter.

Installing with yum

If you're using Oracle Linux 7, you can use yum to install the OCI SDK for Java:

```
sudo yum-config-manager --enable ol7_developer
dsudo yum install java-oci-sdk.x86_64
```

The OCI jar file will be located in: `/usr/lib64/java-oci-sdk/lib/oci-java-sdk-full-<version>.jar`, and third-party libraries will be in `/usr/lib64/java-oci-sdk/third-party/lib`.

You can add the following entries to your classpath:

```
/usr/lib64/java-oci-sdk/lib/oci-java-sdk-full-<version>.jar:
/usr/lib64/java-oci-sdk/third-party/lib/*
```

For example:

```
javac -cp "/usr/lib64/java-oci-sdk/third-party/lib/*:/usr/lib64/java-oci-sdk/lib/oci-java-sdk-full-1.8.2.jar" MyFile.java
```

Configuring the SDK

The SDK services need two types of configuration: credentials and client-side HTTP settings.
**Configuring Credentials**

First, you need to set up your credentials and config file. For instructions, see SDK and CLI Configuration File on page 4184.

Next you need to set up the client to use the credentials. The credentials are abstracted through an AuthenticationDetailsProvider interface. Clients can implement this however you choose. We have included a simple POJO/builder class to help with this task (SimpleAuthenticationDetailsProvider).

- You can load a config with or without a profile:

```java
ConfigFile config = ConfigFileReader.parse("~/.oci/config");
ConfigFile configWithProfile = ConfigFileReader.parse("~/.oci/config", "DEFAULT");
```

- The private key supplier can be created with the file path directly, or using the config file:

```java
Supplier<InputStream> privateKeySupplier = new SimplePrivateKeySupplier("~/oci/oci_api_key.pem");
Supplier<InputStream> privateKeySupplierFromConfigEntry = new SimplePrivateKeySupplier(config.get("key_file"));
```

- To create an auth provider using the builder:

```java
AuthenticationDetailsProvider provider = SimpleAuthenticationDetailsProvider.builder()
    .tenantId("myTenantId")
    .userId("myUserId")
    .fingerprint("myFingerprint")
    .privateKeySupplier(privateKeySupplier)
    .build();
```

- To create an auth provider using the builder with a config file:

```java
AuthenticationDetailsProvider provider = SimpleAuthenticationDetailsProvider.builder()
    .tenantId(config.get("tenancy"))
    .userId(config.get("user"))
    .fingerprint(config.get("fingerprint"))
    .privateKeySupplier(privateKeySupplier)
    .build();
```

- Finally, if you use standard config file keys and the standard config file location, you can simplify this further by using ConfigFileAuthenticationDetailsProvider:

```java
AuthenticationDetailsProvider provider = new ConfigFileAuthenticationDetailsProvider("ADMIN_USER");
```

**Configuring Client-side Options**

Create a client-side configuration through the ClientConfiguration class. If you do not provide your own configuration, the SDK for Java uses a default configuration. To provide your own configuration, use the following:

```java
ClientConfiguration clientConfig = ClientConfiguration.builder()
    .connectionTimeoutMillis(3000)
    .readTimeoutMillis(60000)
    .build();
```

After you have both a credential configuration and the optional client configuration, you can start creating service instances.
Developer Tools

Configuring Custom Options

In the config file, you can insert custom key-value pairs that you define, and then reference them as necessary. For example, you could specify a frequently used compartment ID in the config file like so (highlighted in red italics):

```
[DEFAULT]
user=ocid1.user.oc1..aaaaaaat5nvwcna5j6aqzjcmdy5egbb6gt2jvpkanhtgdagf5w3rynjq
key_file=/usr/local/oci_api_key.pem
tenancy=ocid1.tenancy.oc1..aaaaaaaba3pv6kcr4jqae5f15p2bcmdyt2j6rx32uzr4h25vqstifsfsdsq

custom_compartment_id=ocid1.compartment.oc1..aaaaaaayzfqeibduyox6iib3olcmdar3ugly4fmame
```

Then you can retrieve the value like so:

```java
ConfigFile config = ConfigFileReader.parse("~/.oci/config");
String compartmentId = config.get("custom_compartment_id");
```

Using the SDK for Java

To use the Oracle Cloud Infrastructure SDK for Java in your project, import the `oci-java-sdk-bom`, followed by your project dependencies. For example:

```xml
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>com.oracle.oci.sdk</groupId>
      <artifactId>oci-java-sdk-bom</artifactId>
      <!-- replace the version below with your required version -->
      <version>1.5.2</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
  </dependencies>
</dependencyManagement>

<dependencies>
  <dependency>
    <groupId>com.oracle.oci.sdk</groupId>
    <artifactId>oci-java-sdk-audit</artifactId>
  </dependency>
  <dependency>
    <groupId>com.oracle.oci.sdk</groupId>
    <artifactId>oci-java-sdk-core</artifactId>
  </dependency>
  <dependency>
    <groupId>com.oracle.oci.sdk</groupId>
    <artifactId>oci-java-sdk-database</artifactId>
  </dependency>
  <!-- more dependencies if needed -->
</dependencies>
```

Configuration

This topic provides details on compatibility, advanced configurations, and add-ons for the Oracle Cloud Infrastructure SDK for Java.

Security Manager Permissions
If your application needs to run inside the Java Security Manager, you must grant additional permissions by updating a policy file, or by specifying an additional or a different policy file at runtime.

The SDK requires the following permissions:

- **Required by Jersey:**

  ```java
  permission java.lang.RuntimePermission "getClassLoader;"
  permission java.lang.reflect.ReflectPermission "suppressAccessChecks;"
  permission java.lang.RuntimePermission "accessDeclaredMembers;"
  permission java.util.PropertyPermission "+", "read,write;"
  permission java.lang.RuntimePermission "setFactory;"
  ```

- **Required by the SDK to overwrite reserved headers:**

  ```java
  permission java.util.PropertyPermission "sun.net.http.allowRestrictedHeaders", "write;"
  ```

- **Required by the SDK to open socket connections:**

  ```java
  permission java.net.SocketPermission "+", "connect;"
  ```

To include another policy file, in addition to Java Runtime Environment's default policy file, launch the Java Virtual Machine with:

```bash
java -Djava.security.manager -Djava.security.policy=</path/to/other_policy>
```

To replace the default policy file, launch the Java Virtual Machine with:

```bash
java -Djava.security.manager -Djava.security.policy==</path/to/other_policy>
```

**Note:**

Use a single equals sign (=) when supplying an additional policy file. Use a double equals sign (==) only if you wish to replace the default policy file.

### Java Virtual Machine TTL for DNS Name Lookups

The Java Virtual Machine (JVM) caches DNS responses from lookups for a set amount of time, called *time-to-live* (TTL). This ensures faster response time in code that requires frequent name resolution.

The JVM uses the `networkaddress.cache.ttl` property to specify the caching policy for DNS name lookups. The value is an integer that represents the number of seconds to cache the successful lookup. The default value for many JVMs, `-1`, indicates that the lookup should be cached forever.

Because resources in Oracle Cloud Infrastructure use DNS names that can change, we recommend that you change the TTL value to 60 seconds. This ensures that the new IP address for the resource is returned on next DNS query. You can change this value globally or specifically for your application:

- **To set TTL globally for all applications using the JVM,** add the following in the `$JAVA_HOME/jre/lib/security/java.security` file:

  ```java
  networkaddress.cache.ttl=60
  ```

- **To set TTL only for your application,** set the following in your application's initialization code:

  ```java
  java.security.Security.setProperty("networkaddress.cache.ttl", "60");
  ```

### Apache Connector Add-On

The `oci-java-sdk-addons-apache` is an optional add-on to the SDK for Java that allows for configuring a client connection pool and an HTTP proxy. The add-on leverages the Jersey `ApacheConnectorProvider`
instead of the SDK’s default `HttpUrlConnectorProvider` when making service calls. The add-on can be found in the `bmc-addons` directory of the SDK.

For details on installation and configuration, see the [Readme](#) for the add-on.

**Using BC-FIPS Instead of Bouncy Castle**

If you need FIPS compliance, you must download and use a FIPS-certified version. The SDK supports `bc-fips 1.0.2` and `bcpkix-fips 1.0.3`. You can download them at: [https://www.bouncycastle.org/fips-java/](https://www.bouncycastle.org/fips-java/)

For help installing and configuring Bouncy Castle FIPS, see "BC FIPS Documentation" in the [User Guides](#) and [Security Policy](#) of the Bouncy Castle Documentation.

**Self-Managed Dependencies**

If you are managing dependencies yourself:

1. Remove the non-FIPS Bouncy Castle jar files from the class path:
   
   a. `bcprov-jdk15on-1.60.jar`
   
   b. `bcpkix-jdk15on-1.60.jar`

2. Add the FIPS Bouncy Castle jar files to the class path instead:

   a. `bc-fips-1.0.2.jar`
   
   b. `bcpkix-fips-1.0.3.jar`

**Maven-Managed Dependencies**

If you are using Maven to manage your dependencies:

1. Add the correct versions of `bc-fips` and `bcpkix-fips` to your dependencies:

   ```xml
   <dependencies>
   . . .
   <dependency>
     <groupId>bc-fips</groupId>
     <artifactId>bc-fips</artifactId>
     <version>1.0.2</version>
   </dependency>
   <dependency>
     <groupId>bcpkix-fips</groupId>
     <artifactId>bcpkix-fips</artifactId>
     <version>1.0.3</version>
   </dependency>
   . . .
   </dependencies>
   ```

2. Since you are depending on an `oci-java-sdk*` package, you need to remove the non-FIPS Bouncy Castle dependencies:

   ```xml
   <dependencies>
   . . .
   <dependency>
     <groupId>com.oracle.oci.sdk</groupId>
     <artifactId>oci-java-sdk-common</artifactId>
     <version> . . .</version>
   </dependency>
   <exclusions>
     <exclusion>
       <groupId>org.bouncycastle</groupId>
       <artifactId>bcprov-jdk15on</artifactId>
     </exclusion>
     <exclusion>
       <groupId>org.bouncycastle</groupId>
       <artifactId>bcpkix-jdk15on</artifactId>
     </exclusion>
   </exclusions>
   </dependencies>
   ```
Using Your Own JAX-RS Implementation

The SDK for Java is bundled with Jersey, but you can also use your own JAX-RS implementation.

RESTEasy Client Configurator Add-On

The `oci-java-sdk-addons-resteasy-client-configurator` is provided to demonstrate how to configure an alternate JAX-RS implementation. The add-on can be found in the `bmc-addons` directory of the SDK.

For details on installation and configuration, see the Readme for the add-on.

For code samples that demonstrate how to configure the client, see:

- ResteasyClientExample.java
- ResteasyClientWithObjectStorageExample.java
- InstancePrincipalsAuthenticationDetailsProviderWithResteasyClientExample.java

Using SLF4J for Logging

Logging in the SDK is done through SLF4J. SLF4J is a logging abstraction that allows the use of a user-supplied logging library (e.g., log4j). For more information, see the SLF4J manual.

The following is an example that enables basic logging to standard out. More advanced logging options can be configured by using the log4j binding.

1. Download the SLF4J Simple binding jar: SLF4J Simple Binding
2. Add the jar to your classpath (e.g., add it to the `/third-party/lib` directory of the SDK download)
3. Add the following VM arg to enable debug level logging (by default, info level is used):
   ```
   -Dorg.slf4j.simpleLogger.defaultLogLevel=debug
   ```

Concepts

This topic explains some of the key concepts for using the Oracle Cloud Infrastructure SDK for Java.

Synchronous Calls

To make synchronous calls, create an instance of the synchronous client. The general pattern for synchronous clients is that for a service named Example, there will be an interface named ExampleService, and the synchronous client implementation will be called ExampleServiceClient. Here's an example of creating an Object Storage client:

```java
AuthenticationDetailsProvider provider = ...;
ObjectStorage clientWithDefaultClientConfig = new
    ObjectStorageClient(provider);
clientWithDefaultClientConfig.setRegion(Region.US_ASHBURN_1);

ClientConfiguration clientConfig = ...;
ObjectStorage clientWithExplicitClientConfig = new
    ObjectStorageClient(provider, clientConfig);
clientWithExplicitClientConfig.setRegion(Region.US_ASHBURN_1);
```

Synchronous calls will block until the response is available. All SDK APIs return a response object (regardless of whether or not the API sends any content back). The response object typically contains at least a request ID that you can use when contacting Oracle support for help on a particular request.

```java
ObjectStorage client = ...;
GetBucketResponse response = client.getBucket(
    GetBucketRequest.builder().namespaceName("myNamespace").bucketName("myBucket").build());
String requestId = response.getOpcRequestId();
Bucket bucket = response.getBucket();
```
Asynchronous Calls

To make asynchronous calls, create an instance of the asynchronous client. The general pattern for asynchronous clients is that for a service named Example, there will be an interface named ExampleServiceAsync, and the asynchronous client implementation will be called ExampleServiceAsyncClient. Here's an example of creating an Object Storage client:

```java
AuthenticationDetailsProvider provider = ...;
ObjectStorageAsync clientWithDefaultClientConfig = new
    ObjectStorageAsyncClient(provider);
clientWithDefaultClientConfig.setRegion(Region.US_ASHBURN_1);

ClientConfiguration clientConfig = ...;
ObjectStorageAsync clientWithExplicitClientConfig = new
    ObjectStorageAsyncClient(provider, clientConfig);
clientWithExplicitClientConfig.setRegion(Region.US_ASHBURN_1);
```

Asynchronous calls return immediately. You need to provide an AsyncHandler that will be invoked after the call completes either successfully or unsuccessfully:

```java
ObjectStorageAsync client = ...;
AsyncHandler<GetBucketRequest, GetBucketResponse> handler = new
    AsyncHandler<GetBucketRequest, GetBucketResponse>() {
        @Override
        public void onSuccess(GetBucketRequest request, GetBucketResponse response) {
            String requestId = response.getOpcRequestId();
            Bucket bucket = response.getBucket();
            System.out.println(requestId);
            System.out.println(bucket.getName());
        }
        
        @Override
        public void onError(GetBucketRequest request, Throwable error) { error.printStackTrace(); }
    };

Future<GetBucketResponse> future = client.getBucket(
    GetBucketRequest.builder().namespaceName("myNamespace").bucketName("myBucket").build(),
    handler);
```

Polling with Waiters

The SDK offers waiters that allow your code to wait until a specific resource reaches a desired state. A waiter can be invoked in both a blocking or a non-blocking (with asynchronous callback) manner, and will wait until either the desired state is reached or a timeout is exceeded. Waiters abstract the polling logic you would otherwise have to write into an easy-to-use single method call.

Waiters are obtained through the service client (client.getWaiters()). Both a `Get<Resource>Request` and the desired lifecycle state are passed in to the `waiters.for<Resource>` method. For example:

```java
public static Instance waitForInstanceProvisioningToComplete( ComputeClient computeClient, String instanceId) throws Exception {
    ComputeWaiters waiters = computeClient.getWaiters();
    GetInstanceResponse response = waiters.forInstance(}
GetInstanceRequest.builder().instanceId(instanceId).build(),
  Instance.LifecycleState.Running)
  .execute();
  return response.getInstance();
}

Each `waiters.for<Resource>` method has two versions:

- One version uses the default polling values. For example:

  ```java
  waiters.forInstance(GetInstanceRequest, LifecycleState)
  ```

- The other version gives you full control over how long to wait and how much time between polling attempts. For example:

  ```java
  waiters.forInstance(GetInstanceRequest, LifecycleState,
  TerminationStrategy, DelayStrategy)
  ```

Threading Model

A client becomes thread-safe when it is initialized. After setting its endpoint, you can safely use a client in multiple threads and concurrently call methods on it.

You can reuse a client on multiple requests, both across concurrent threads or within a single thread. Unless the environment's resources are constrained, you should only close the client immediately before it goes out of scope.

Note:

This guarantee applies only to the default JAX-RS implementation, Jersey. When using an alternate implementation, you must manage thread safety yourself. For more information, see Configuring the SDK on page 4228

Uploading Large Objects

The Object Storage service supports multipart uploads to make large object uploads easier by splitting the large object into parts. The SDK for Java supports raw multipart upload operations for advanced use cases, as well as a higher level upload class that uses the multipart upload APIs. Managing Multipart Uploads provides links to the APIs used for multipart upload operations. Higher level multipart uploads are implemented using the `UploadManager`, which will: split a large object into parts for you, upload the parts in parallel, and then recombine and commit the parts as a single object in storage.

The `UploadObject` example shows how to use the `UploadManager` to automatically split an object into parts for upload to simplify interaction with the Object Storage service.

Raw Requests

Raw requests are useful, and in some cases necessary. Typical use cases are: when using your own HTTP client, making a OCI-authenticated request to an alternate endpoint, and making a request to a OCI API that is not currently supported in the SDK. The SDK for Java exposes the `DefaultRequestSigner` class that you can use to create a `RequestSigner` instance for non-standard requests.

The Raw Request example on GitHub shows how to:

- create an authentication provider and request signer
- integrate with an HTTP client (Jersey in this example) to authenticate requests

Setting the Endpoints

Service endpoints can be set in three ways.

- Call `setEndpoint()` on the service instance. This lets you specify a full host name (for example, https://www.example.com).
• Call `setRegion()` on the service instance. This selects the appropriate host name for the service for the given region. However, if the service is not supported in the region you set, the SDK for Java returns an error.
• Pass the region in the configuration file. For more information, see [SDK and CLI Configuration File](#) on page 4184.

Note that a service instance cannot be used to communicate with different regions. If you need to make requests to different regions, create multiple service instances.

**Forward Compatibility and enums**

If you have conditional logic based on an enum, be sure that your code handles the `UnknownEnumValue` case to ensure forward compatibility. Some response fields are of type enum, but in the future, individual services may return values not covered by existing enums for that field. To address this possibility, every response field of type enum has an additional value named `UnknownEnumValue`. If a service returns a value that is not recognized by your version of the SDK, then the response field will be set to this value.

**New Region Support**

If you are using a version of the SDK released prior to the announcement of a new region, you can use a workaround to reach it.

A region is a localized geographic area. For more information on regions and how to identify them, see [Regions and Availability Domains](#) on page 180.

A realm is a set of regions that share entities. You can identify your realm by looking at the domain name at the end of the network address. For example, the realm for `xyz.abc.123.oraclecloud.com` is `oraclecloud.com`.

You must first call `Region.register` to register the new region, and then you can set the region by either using the configuration file or by calling the `setRegion` method.

```
Note:

Once a region is registered, the federation endpoint is no longer required while using instance principals. For an example, see [https://github.com/oracle/oci-java-sdk/blob/master/bmc-examples/src/main/java/NewRegionAndRealmSupportWithoutSDKUpdate.java](https://github.com/oracle/oci-java-sdk/blob/master/bmc-examples/src/main/java/NewRegionAndRealmSupportWithoutSDKUpdate.java).
```

**oraclecloud.com Realm**

For regions in the `oraclecloud.com` realm, you can pass new region names just as you would pass ones that are already defined in the `Region` enum for your SDK version.

```
Note:

For the following code samples, be sure to supply the appropriate endpoints for your region.
```

If you are using version 1.2.34 or later of the SDK for Java, you can pass the new region name as a string using one of the following methods:

• To set the region on a previously created client:

```
client.setRegion("ca-toronto-1");
```

• To set a region when building a new client:

```
Identity identityClient = IdentityClient.builder().
.region("ca-toronto-1")
 .build(provider);
```

• You can also pass the region in the configuration file. For more information, see [SDK and CLI Configuration File](#) on page 4184.
Other Realms

For regions in realms other than oraclecloud.com, you can use the following workarounds to reach new regions with earlier versions of the SDK.

To specify the endpoint:

```java
AuthenticationDetailsProvider provider =
    new ConfigFileAuthenticationDetailsProvider(configurationFilePath, profile);

IdentityClient client = IdentityClient.builder()
    .endpoint("https://identity.ca-toronto-1.oraclecloud.com")
    .build(provider);
```

If you are authenticating via instance principals, you can set the endpoint and federationEndpoint via the following process:

```java
InstancePrincipalsAuthenticationDetailsProvider provider =
    InstancePrincipalsAuthenticationDetailsProvider.builder()
    .federationEndpoint("https://auth.ca-toronto-1.oraclecloud.com/v1/x509")
    .build();

IdentityClient identityClient = IdentityClient.builder()
    .endpoint("https://identity.ca-toronto-1.oraclecloud.com")
    .build(provider);
```

Paginated Responses

Some APIs return paginated result sets, so you must check for additional items and if necessary, fetch the next page. You can do so manually or you can use an iterator.

Manually Fetching Pages

The Response objects contain a method to fetch the next page token. If the token is null, there are no more items. If it is not null, you can make an additional request, by setting the token on the Request object, to get the next page of responses.

**Note:**

Some APIs may return a token even if there are no additional results. Be sure to also check whether any items were returned and stop if there are none.

This example shows how to handle page tokens returned by the Object Storage API:

```java
ObjectStorage client = ...;

ListBucketsRequest.Builder builder =
    ListBucketsRequest.builder().namespaceName(namespace);
String nextPageToken = null;
while (nextPageToken != null) {
    builder.page(nextPageToken);
    ListBucketsResponse listResponse = client.listBuckets(builder.build());
    List<Bucket> buckets = listResponse.getItems();
    // handle buckets
    nextPageToken = listResponse.getOpcNextPage();
} while (nextPageToken != null);
```
Using an Iterator

Instead of manually working with page tokens, you can use an iterator. Each service client exposes a `getPaginators()` method that returns a `Paginator` object. This object contains methods to return objects of type `Iterable`. We support two approaches to using `Iterable`:

- **Response Iterator**: You can iterate over the `Response` objects that are returned by the list operation. These are referred to as `ResponseIterators`, and their methods are suffixed with "ResponseIterator," for example, `listUsersResponseIterator`.

  ```java
  Iterable<ListUsersResponse> responseIterator =
      identityClient.getPaginators().listUsersResponseIterator(request);
  for (ListUsersResponse response : responseIterator) {
      for (User user : response.getItems()) {
          System.out.println(user);
      }
  }
  ```

- **Record Iterator**: You can iterate over the resources/records that are listed. These are referred to as `RecordIterator`, and their methods are suffixed with "RecordIterator," for example, `listUsersRecordIterator`.

  ```java
  Iterable<User> recordIterator =
      identityClient.getPaginators().listUsersRecordIterator(request);
  for (User user : recordIterator) {
      System.out.println(user);
  }
  ```

Client-Side Encryption

Client Side Encryption allows you to encrypt data on the client side before storing it locally or using it with other Oracle Cloud Infrastructure services.

To use client-side encryption, you must create a master encryption key (MEK) using the Key Management Service. This can be done using the `CreateKey` or `ImportKey` operations.

The MEK is used to generate a Data Encryption Key (DEK) to encrypt each payload. A encrypted copy of this DEK (encrypted under the MEK) and other pieces of metadata are included in the encrypted payload returned by the SDKs so that they can be used for decryption.

Java Prerequisites

The unlimited policy files for earlier releases are required only for JDK 8, 7, and 6 updates earlier than 8u161, 7u171, and 6u16. For those versions and later the policy files are included but not enabled by default.

Current versions of the JDK do not require these policy files. They are provided here for use with older versions of the JDK. JDK 9 and later ship with the unlimited policy files and use them by default.

Examples

The following code example shows how to encrypt a string:

```java
// String encryption example
final byte[] plainText = "Hello World".getBytes();
String masterKeyId = "OCID....";
Map<String, String> context = Collections.singletonMap("Example", "value");
OciCrypto ociCrypto = new OciCrypto();
KmsMasterKey kmsMasterKey = new KmsMasterKey(authenticationProvider,
    Region.US_ASHBURN_1.getRegionId(), vaultId, masterKeyId);
KmsMasterKeyProvider kmsMasterKeyProvider = new
    KmsMasterKeyProvider(kmsMasterKey);
```
// Encrypt the data and embed the master key ID in the header
final OciCryptoResult encryptResult =
    ociCrypto.encryptData(kmsMasterKeyProvider, plainText, context);
final byte[] cipherText = encryptResult.getResult();

// Decrypt the data
final OciCryptoResult decryptResult =
    ociCrypto.decryptData(kmsMasterKeyProvider, cipherText);

The following example shows how to encrypt a file stream:

// Create Encryption file stream
FileInputStream in = new FileInputStream(srcFile);
OciCrypto ociCrypto = new OciCrypto();
KmsMasterKey kmsMasterKey = new KmsMasterKey(authenticationProvider,
    Region.US_ASHBURN_1.getRegionId(), vaultId, masterKeyId);
KmsMasterKeyProvider kmsMasterKeyProvider = new
    KmsMasterKeyProvider(kmsMasterKey);
OciCryptoInputStream encryptingStream =
    ociCrypto.createEncryptingStream(kmsMasterKeyProvider, in);

// Write the encrypted data to file
FileOutputStream out = new FileOutputStream(srcFile + "_.encrypted");
IOUtils.copy(encryptingStream, out);
encryptingStream.close();
out.close();

// For decryption, no need to pass key info
KmsMasterKeyProvider kmsMasterKeyProvider = new
    KmsMasterKeyProvider(authenticationProvider);
// Create the Decryption file stream.
in = new FileInputStream(srcFile + "_.encrypted");
OciCryptoInputStream decryptingStream =
    ociCrypto.createDecryptingStream(kmsMasterKeyProvider, in);

// Return the plaintext data
out = new FileOutputStream(srcFile + "_.decrypted");
IOUtils.copy(decryptingStream, out);
decryptingStream.close();
out.close();

Exception Handling

When handling an exception, you can get more information about the HTTP request that caused it, such as
the status code or timeout. You can also get the request ID when handling a BmcException by using the
getOpcRequestId method.

This example shows a try-catch block that handles a BmcException and prints the request ID.

ObjectStorage client = ...;
try {
    GetBucketResponse response = client.getBucket(
        GetBucketRequest.builder().namespaceName("myNamespace").bucketName("myBucket").build());
    String requestId = response.getOpcRequestId();
    System.out.println(requestId);
} catch (BmcException e) {
    String requestId = e.getOpcRequestId();
    System.out.println(requestId);
    e.printStackTrace();
}
Exceptions in the SDK for Java are runtime exceptions (unchecked), so they do not show up in method signatures. All APIs can throw a BmcException.

**Examples**

**GitHub**

Examples of SDK usage can be found on GitHub, including:

- Example: Synchronous Object Storage
- Example: Asynchronous Object Storage
- Example: Create an instance
- Example: Get an instance's public IP address

The examples are also in the downloadable .zip file for the SDK. Examples for older versions of the SDK are in the downloadable .zip for the specific version, available on GitHub.

If you'd like to see another example not already covered, file a GitHub issue.

**SDK Reference**

In addition to the examples found on GitHub, the SDK for Java API reference contains code examples that you can copy and modify to run in your own environment.

**Running Examples**

1. Download the SDK to a directory named oci. See GitHub for the download.
2. Unzip the SDK into the oci directory. For example: tar -xf oci-java-sdk-dist.zip
3. Create your configuration file in your home directory (~/.oci/config). See Configuring the SDK on page 4228.
4. Use javac to compile one of the previous example classes from the examples directory, ex:

   ```bash
   javac -cp lib/oci-java-sdk-full-<version>.jar:third-party/lib/* examples/ObjectStorageSyncExample.java
   ```

5. You should now have a class file in the examples directory. Run the example:

   ```bash
   java -cp examples:lib/oci-java-sdk-full-<version>.jar:third-party/lib/* ObjectStorageSyncExample
   ```

**Third-Party Dependencies and Shading**

The SDK requires a number of third-party dependencies, which are available in the third-party/lib directory. To use the SDK library lib/oci-java-sdk-full-<version>.jar, all of the third-party dependencies in third-party/lib have to be on the class path.

The SDK also includes a second version of the SDK library, shaded/lib/oci-java-sdk-full-shaded-<version>.jar, which contains most of the third-party dependencies already. Only a few more third-party libraries in shaded/third-party/lib have to be on the class path when you use this version of the SDK library.

These two versions of the SDK library are functionally the same, however the second version, shaded/lib/oci-java-sdk-full-shaded-<version>.jar can simplify dealing with different versions of third-party dependencies. This is because all the dependencies that are included in shaded/lib/oci-java-sdk-full-shaded-<version>.jar were shaded, which means they will not interfere with other versions of themselves you may want to include along with this SDK.

To use the shaded version of the SDK, replace the `javac` commands in steps 4 and 5 with the following:

- **Step 4:**

  ```
  ```

- **Step 5:**

  ```
  ```

**Troubleshooting**

This section contains troubleshooting information for the Oracle Cloud Infrastructure SDK for Java.

ObjectStorage client does not close connections when client is closed.

Too many file descriptors are opened up, and it takes too long to close existing ones. An exception may look like this:

```
Caused by: java.io.FileNotFoundException: classes/caspertest.pem (Too many open files)
  at java.io.FileInputStream.open0(Native Method)
  at java.io.FileInputStream.open(FileInputStream.java:195)
  at java.io.FileInputStream.<init>(FileInputStream.java:138)
```

Use one of the following workarounds to fix this issue.

- Make this call before creating a client:
  ```
  System.setProperty("http.keepAlive", "false");
  ```
- Use this command line argument when running Java:
  ```
  -Dhttp.keepAlive=false
  ```

Serialization errors when making requests or handling responses

An `UnrecognizedPropertyException` error when handling a response indicates that the version of the Jackson library does not support a feature that was injected at runtime from another dependency in your application's class path. This happens even if the `FAIL_ON_UNKNOWN_PROPERTIES` deserialization property is set to `false` for the configured `ObjectMapper`.

**Solution:**

Determine which version of Jackson libraries are referenced in your application’s class path and, if necessary, upgrade to version 2.9.5. For a complete list of Jackson libraries that the SDK for Java depends on, please refer to the `pom.xml` file that is hosted on GitHub.

An alternative solution is to use the shaded version of the SDK for Java jar file, which includes a bundled version of the Jackson libraries.

Encryption key size errors

By default, the SDK for Java can only handle keys of 128 bit or lower key length. Users get "Invalid Key Exception" and "Illegal key size" errors when they use longer keys, such as AES256.

Use one of the following workarounds to fix this issue.

- Use a 128 bit key, such as AES128.
- Install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction from the following location: [http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html](http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html)
Troubleshooting Service Errors

Any operation resulting in a service error will cause an exception of type com.oracle.bmc.model.BmcException to be thrown by the SDK. For information about common service errors returned by OCI, see API Errors.

SDK for Python

The Oracle Cloud Infrastructure SDK for Python enables you to write code to manage Oracle Cloud Infrastructure resources.

This SDK and sample is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

Download: The SDK for Python is available on GitHub or the Python Package Index (PyPi).

Documentation: Available on docs.cloud.oracle.com and readthedocs.io.

Tip: The SDK for Python is pre-configured with your credentials and ready to use immediately from within Cloud Shell. For more information on using the SDK for Python from within Cloud Shell, see SDK for Python Cloud Shell Quick Start on page 4187.

Services Supported

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Compute Instance Agent (Oracle Cloud Agent)
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Cloud Guard
- Data Catalog
- Data Flow
- Data Integration
- Data Safe
- Data Science
- Data Transfer
- Database
- Database Management
- Digital Assistant
- DNS
- Email Delivery
- Events
- File Storage
- Functions
- Golden Gate
- Health Checks
Installing with Resource Manager

You can use Resource Manager to install the Oracle Cloud Development Kit on a Compute instance in your compartment. The Oracle Cloud Development Kit includes the SDK for Python, along with other Oracle development tools.

Installing with yum

If you're using Oracle Linux 7, you can use yum to install the OCI SDK for Python.

The following example shows how to use yum to install the OCI SDK for Python 3.6:

```bash
sudo yum install python36-oci-sdk.x86_64
```

This example shows how to use yum to install the OCI SDK for Python 2.7:

```bash
sudo yum install python oci-sdk.x86_64
```
Client-Side Encryption

Client Side Encryption allows you to encrypt data on the client side before storing it locally or using it with other Oracle Cloud Infrastructure services.

To use client-side encryption, you must create a master encryption key (MEK) using the Key Management Service. This can be done using the CreateKey or ImportKey operations.

The MEK is used to generate a Data Encryption Key (DEK) to encrypt each payload. A encrypted copy of this DEK (encrypted under the MEK) and other pieces of metadata are included in the encrypted payload returned by the SDKs so that they can be used for decryption.

Examples

The following code example shows how to encrypt a string:

```
import oci

# user supplied vars
vault_id = TEST_VAULT_OCID
master_key_id = TEST_MASTER_KEY_ID
data_to_encrypt_bytes = b"This is a secret message"

crypto_result = crypto.encrypt(kms_master_key_provider, data_to_encrypt_bytes)
ciphertext = crypto_result.get_data()
print("ciphertext: {}".format(ciphertext))

# decrypt string example
crypto_result = crypto.decrypt(ciphertext, kms_master_key_provider)
print("unencrypted text: {}".format(crypto_result.get_data()))
```

The following example shows how to encrypt a file stream:

```
import oci
import shutil

# user supplied vars
vault_id = TEST_VAULT_OCID
master_key_id = TEST_MASTER_KEY_ID
file_to_encrypt = "/file/to/encrypt/message.txt"
output_encrypted_file = "/tmp/message.txt.encrypted"
output_decrypted_file = "/tmp/message.txt.decrypted"

# setup OCI KMS keys
config = oci.config.from_file()
kms_master_key = oci.encryption.KMSMasterKey(
    config=config, master_key_id=master_key_id, vault_id=vault_id
)
kms_master_key_provider = oci.encryption.KMSMasterKeyProvider(
    config=config,
    kms_master_keys=[kms_master_key]
)

crypto_result = crypto.encrypt(kms_master_key_provider, file_to_encrypt)
ciphertext = crypto_result.get_data()
print("ciphertext: {}".format(ciphertext))

# decrypt string example
crypto_result = crypto.decrypt(ciphertext, kms_master_key_provider)
print("unencrypted text: {}".format(crypto_result.get_data()))
```
```python
config=config,
kms_master_keys=[kms_master_key]
)

# encrypt stream example
with open(output_encrypted_file, 'wb') as output_stream,
open(file_to_encrypt, 'rb') as stream_to_encrypt:
    with crypto.create_encryption_stream(
        kms_master_key_provider,
        stream_to_encrypt
    ) as encryption_stream:
        shutil.copyfileobj(encryption_stream, output_stream)

# decrypt stream example
with open(output_decrypted_file, 'wb') as output_stream,
open(output_encrypted_file, 'rb') as stream_to_decrypt:
    with crypto.create_decryption_stream(
        stream_to_decrypt,
        kms_master_key_provider
    ) as decryption_stream:
        shutil.copyfileobj(decryption_stream, output_stream)
```

**Contact Us**

**Contributions**

Got a fix for a bug or a new feature you’d like to contribute? The SDK is open source and accepting pull requests on GitHub.

**Notifications**

To be notified when a new version of the SDK for Python is released, subscribe to the Atom feed.

**Questions or Feedback**

- **GitHub Issues**: To file bugs and feature requests only
- **Stack Overflow**: Please use the oracle-cloud-infrastructure and oci-python-sdk tags in your post
- **Developer Tools section** of the Oracle Cloud forums
- **My Oracle Support**

**SDK for TypeScript and JavaScript**

The Oracle Cloud Infrastructure SDK for TypeScript and JavaScript enables you to write code to manage Oracle Cloud Infrastructure resources.

This SDK and sample is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

**Download**: GitHub or NPM.

**Requirements**

To use the SDK for TypeScript and JavaScript, you must have the following:

- An Oracle Cloud Infrastructure account.
- A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users on page 57. For a list of typical policies you may want to use, see Common Policies on page 2142.
- A key pair used for signing API requests, with the public key uploaded to Oracle. Only the user calling the API should be in possession of the private key. For more information, see Getting Started on page 4247.
Services Supported

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Compute Instance Agent (Oracle Cloud Agent)
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Cloud Guard
- Data Catalog
- Data Flow
- Data Integration
- Data Safe
- Data Science
- Data Transfer
- Database
- Database Management
- Digital Assistant
- DNS
- Email Delivery
- Events
- File Storage
- Functions
- Golden Gate
- Health Checks
- IAM
- Integration
- Key Management (for the Vault service)
- Limits
- Load Balancing
- Logging
- Logging Analytics
- Logging Search
- Logging Ingestion
- Management Agent Cloud
- Management Dashboard
- Marketplace
- Monitoring
- MySQL Database
- NoSQL Database Cloud
- Notifications
- Object Storage
- OCI Registry
• Operations Insights
• Optimizer
• Organizations
• OS Management
• Quotas
• Resource Manager
• Roving Edge Infrastructure
• Search
• Secret Management (for the Vault)
• Service Connector Hub
• Streaming
• Support Management
• Usage
• VMWare Solution
• Web Application Acceleration and Security
• Work Requests (Compute, Database)

**Versions Supported**

The SDK for TypeScript and JavaScript currently supports NodeJS version 10.15.3 and TypeScript version 4.1.3.

**NodeJS & Browser Support**

The SDK for TypeScript and JavaScript currently supports NodeJS but does not have browser support.

**Contact Us**

**Contributions**

Got a fix for a bug or a new feature you’d like to contribute? The SDK is open source and accepting pull requests on GitHub.

**Notifications**

To be notified when a new version of the SDK for TypeScript and JavaScript is released, subscribe to the Atom feed.

**Questions or Feedback**

- GitHub Issues: To file bugs and feature requests only
- Stack Overflow: Please use the oracle-cloud-infrastructure and oci-typescript-sdk tags in your post
- Developer Tools section of the Oracle Cloud forums
- My Oracle Support

**Getting Started**

This topic describes how to install and configure the SDK for TypeScript and JavaScript.

To use the Oracle Cloud Infrastructure SDK for TypeScript and JavaScript in your project, import any service from `./oci-typescript-sdk/index.ts`. For example:

```typescript
// Container Engine
export import containerengine = require("oci-containerengine");

// Core
export import core = require("oci-core");

// Database
```
export import database = require("oci-database");

Downloading the SDK from GitHub

You can download the SDK for TypeScript and JavaScript as a zip archive from GitHub. It contains the SDK, all of its dependencies, documentation, and examples.

Installing with yum

If you're using Oracle Linux 7, you can use yum to install the OCI SDK for TypeScript and JavaScript:

```
sudo yum install oracle-nodejs-release-el7
sudo yum install --enablerepo=ol7_developer_nodejs10 --enablerepo=ol7_developer oci-typescript-sdk
```

The oci-typescript-sdk yum package will only work for Node version 10.X.X. The oci-sdk package will be installed into the global node_modules folder. To use the oci-sdk package in a project, link the oci-sdk global package to your local project.

For example:

```
# Assuming you are in your project's top level directory
npm link oci-sdk
# You should now see oci-sdk package in your local project's node_modules folder
```

Because the oci-sdk package is globally installed, you must update the import statements for oci-sdk's sub-packages when running the oci-typescript-sdk examples on GitHub.

For example:

```
import * as identity from "oci-identity"; // Change needed
import * as oci from "oci-sdk"; // No change needed

import * as identity from "oci-sdk/node_modules/oci-identity"; // Changed
import * as oci from "oci-sdk"; // No change
```

Using the SDK for TypeScript and JavaScript with NPM

NPM.

Configuring the SDK

The SDK services need two types of configuration: credentials and client-side HTTP settings.

**Configuring Credentials**

First, you need to set up your credentials and config file. For instructions, see SDK and CLI Configuration File on page 4184.

The default configuration location is "~/.oci/config" and "DEFAULT" profile is used. You can use ConfigFileAuthenticationDetailsProvider with or without specifying the configuration location and profile name:

```
// TypeScript
import common = require("oci-common");
// Using default configuration
const provider: common.ConfigFileAuthenticationDetailsProvider = new
common.ConfigFileAuthenticationDetailsProvider();
// Using personal configuration
const configurationFilePath = "~/your_config_location";
const configProfile = "your_profile_name";
const provider: common.ConfigFileAuthenticationDetailsProvider = new
common.ConfigFileAuthenticationDetailsProvider(
```
const common = require("oci-common");
// Using default configurations
const provider = new common.ConfigFileAuthenticationDetailsProvider();
// Using personal configuration
const configurationFilePath = "/your_config_location";
const configProfile = "your_profile_name";
const provider = new common.ConfigFileAuthenticationDetailsProvider(
    configurationFilePath,
    configProfile
);

Configuring Custom Options

In the configuration file, you can insert custom key-value pairs that you define, and then reference them as necessary. For example, you could specify a frequently used compartment ID in the config file:

```
[DEFAULT]
user=ocid1.user.oc1..<your_unique_id>
fingerprint=<your_fingerprint>
key_file=~/.oci/oci_api_key.pem
tenancy=ocid1.tenancy.oc1..<your_unique_id>
customCompartmentId=ocid1.compartment.oc1..<your_unique_id>
```

Then you can retrieve the value:

```
// TypeScript
import common = require("oci-common");
const configurationFilePath = "/your_config_location";
const configProfile = "your_profile_name";
const config = common.ConfigFileReader.parseDefault(configurationFilePath);
const profile =
    config.accumulator.configurationsByProfile.get(configProfile);
customCompartmentId = profile.get("customCompartmentId") || "";

// JavaScript
import common = require("oci-common");
const configurationFilePath = "/your_config_location";
const configProfile = "your_profile_name";
const config = common.ConfigFileReader.parseDefault(configurationFilePath);
const profile =
    config.accumulator.configurationsByProfile.get(configProfile);
customCompartmentId = profile.get("customCompartmentId") || "";
```

Concepts

This topic explains some of the key concepts for using the SDK for TypeScript and JavaScript.

Raw Requests

Raw requests are useful, and in some cases necessary. Typical use cases are: when using your own HTTP client, making a OCI-authenticated request to an alternate endpoint, and making a request to a OCI API that is not currently supported in the SDK. The SDK for TypeScript and JavaScript exposes the DefaultRequestSigner class that you can use to create an instance and call signHttpRequest.
The Raw Request example on GitHub shows how to create an instance of DefaultRequestSigner and call signHttpRequest.

Retries

You can configure the SDK for TypeScript and JavaScript to retry SDK operations that fail. The SDK allows you to specify the strategy to use for how retries are handled, including the number of times to retry, the condition under which the SDK should retry an operation, and when to stop retrying an operation. You can set these parameters at the client level and at the individual request level.

Delay Strategy

The delayStrategy parameter determines how long to wait between each retry call. There are two options for this parameter:

- **FixedTimeDelayStrategy (seconds)** - Each retry is delayed by a specified number of seconds.
- **ExponentialBackoffStrategy (seconds)** - The delay time for subsequent retry calls increases by an exponential factor of 2 until it reaches the defined maximum delay (in seconds), with a base value of one second.

The default delay strategy is set to ExponentialBackoffDelayStrategy with 30 seconds of delay.

Retry Condition

The retryCondition defines a function with an error argument that returns a boolean indicating whether to retry or not. The operation will be retried if this function returns true.

**Note:**

Retries are not supported for requests that have binary or stream bodies. This includes UploadManager operations. Requests with binary or stream bodies will not be retried.

Termination Strategy

The terminationStrategy parameter defines when to terminate the retry attempts. This parameter supports the following options:

- **MaxTimeTerminationStrategy (seconds)** - Defines total duration in seconds for which the retry attempts.
- **MaxAttemptsTerminationStrategy (attempts)** - Defines the total number of retry attempts.

Retry Examples

**TypeScript**

This example sets the retry configuration at the client level:

```javascript
identityClient.clientConfiguration = {
   retryConfiguration : {
      delayStrategy : new common.FixedTimeDelayStrategy(5),
      terminationStrategy : new common.MaxTimeTerminationStrategy(30),
      retryCondition : (error) => { return error.statusCode >= 500; }
   }
}
```

This example sets the retry configuration at the request level:

```javascript
const request: identity.requests.ListAvailabilityDomainsRequest = {
   compartmentId: tenancyId,
   retryConfiguration : {
      terminationStrategy : new common.MaxAttemptsTerminationStrategy(6),
   }
};
```
JavaScript

This example sets the retry configuration at the client level:

```javascript
identityClient.clientConfiguration = {
  retryConfiguration : {
    delayStrategy : new common.FixedTimeDelayStrategy(5),
    terminationStrategy : new common.MaxTimeTerminationStrategy(30),
    retryCondition : (error) => { return error.statusCode >= 500; }
  }
}
```

This example sets the retry configuration at the request level:

```javascript
const request = {
  compartmentId: tenancyId,
  retryConfiguration : {
    terminationStrategy : new 
    common.MaxAttemptsTerminationStrategy(6),
  }
};
```

Setting Endpoints

Service endpoints can be set in three ways:

- Set `.endpoint = '<YOUR_ENDPOINT>'` on the service instance. This lets you specify a full host name (for example, https://www.example.com).
- Set `.region = '<YOUR_REGION_ID>'` on the service instance. This selects the appropriate host name for the service for the given region. However, if the service is not supported in the region you set, the SDK for TypeScript and JavaScript returns an error. You can refer to the list of regionIds in: ./oci-typescript-sdk/common/lib/region.ts
- Pass the region in the configuration file. For more information, see SDK and CLI Configuration File.

Note that a service instance cannot be used to communicate with different regions. If you need to make requests to different regions, create multiple service instances.

New Region Support

If you are using a version of the SDK released prior to the announcement of a new region, you can use a workaround to reach it.

A region is a localized geographic area. For more information on regions and how to identify them, see Regions and Availability Domains.

A realm is a set of regions that share entities. You can identify your realm by looking at the domain name at the end of the network address. For example, the realm for xyz.abc.123.oraclecloud.com is oraclecloud.com.

You must first call Region.register to register the new region, and then you can set the region by either using the configuration file or by set .region = <Your_new_registered_region>.

oraclecloud.com Realm

For regions in the oraclecloud.com realm, you can pass new region names just as you would pass ones that are already defined in the Region enum for your SDK version.

To set the region:

```javascript
identityClient = await new 
identity.IdentityClient({ authenticationDetailsProvider: provider });
identityClient.region = 'us-phoenix-1'
```

Other Realms
For regions in realms other than oraclecloud.com, you can use the following workarounds to reach new regions with earlier versions of the SDK.

To set the endpoint:

```javascript
// Instantiate an identity client
identityClient = await new
    identity.IdentityClient({ authenticationDetailsProvider: provider });
identityClient.endpoint = 'https://<your_endpoint>.com'
```

### Paginated Responses

Sometimes it is better to lazy load a result. In order to retrieve more data from lazy load, you have to continue to make calls to the list operation, passing in the value of the most recent response’s next token. The pagination module allows you:

- Eagerly load all possible results from a list call
- Lazily load results

For an example on how to use these functions, please check [GitHub](https://github.com).

### Exception Handling

When handling an exception, you can get more information about the HTTP request that caused it, such as the status code or timeout. You can also get the request ID when handling an exception by looking at the opcRequestId property of the error object.

```javascript
try {
    const response = await identityClient.listAllUsersResponses(listUserReq);
} catch (err) {
    console.log('requestId: ', err.opcRequestId);
}
```

### Logging

The SDK for Typescript and JavaScript enables you to integrate your own logger. Logging in the SDK is done through the Logger interface. This interface is a logging abstraction that allows the use of a user-supplied logging library, such as log4js, bunyan, or winston.

For more information, see the [logging example on GitHub](https://github.com).

To enable logging:

```typescript
// TypeScript
// Download the logger that you want to use with the SDK (like bunyan)
import { LOG } from "oci-sdk";
var bunyan = require("bunyan");

// Set the logger here
var bunLog = bunyan.createLogger({ name: "LoggingExample", level: "debug" });
LOG.logger = bunLog;
```

```javascript
// Javascript
import { LOG } from "oci-sdk";
var bunyan = require("bunyan");

// Set the logger here.
var bunLog = bunyan.createLogger({ name: "LoggingExample", level: "debug" });
LOG.logger = bunLog;
```

**Examples**

[GitHub](https://github.com)
Examples of SDK usage can be found on GitHub, including:

- Example: Create an instance
- Example: Invoke Oracle Function
- Example: Move Compartment

The examples are also in the downloadable .zip file for the SDK. Examples for older versions of the SDK are in the downloadable .zip for the specific version, available on GitHub.

If you’d like to see another example not already covered, file a GitHub issue.

**SDK Reference**

In addition to the examples found on GitHub, the SDK for TypeScript and JavaScript API reference contains code examples that you can copy and modify to run in your own environment.

**Running Examples**

**Note:**
If you're using Windows, you'll need to install Git Bash for Windows before running the following commands.

1. git clone the SDK for TypeScript and JavaScript

   ```
git clone https://github.com/oracle/oci-typescript-sdk.git
   ```

2. Change to the directory where you installed the oci-typescript-sdk repository.

3. Run npm install

4. Run npm run build

5. If you do not have typescript globally installed, run:

   ```
   npm install -g typescript@4.1.3.
   ```

**Note:**
We've tested and support TypeScript version 4.1.3 with the OCI SDK for TypeScript and JavaScript. We cannot guarantee full support for other versions of TypeScript.

6. You can optionally install ts-node globally to make it easier to run examples:

   ```
   npm install -g ts-node
   ```

7. Create your configuration file in your home directory. See SDK and CLI Configuration File on page 4184 for more information.

8. Change directory into the TypeScript example folder to run TypeScript examples. For example:

   ```
   cd ./oci-typescript-sdk/examples/typescript/
   ```

9. Run any of the examples.

   For example, if you're running ts-node:

   ```
   ts-node "./identity.ts"
   ```

   If you're not running ts-node:

   ```
   tsc ./identity.ts
   node ./identity.js
   ```
10. Some examples are available in JavaScript. They are located in the `oci-typescript-sdk/examples/javascript` folder. To run the JavaScript equivalent of the above example:

```
node "./identity.js"
```

**SDK for .NET**

The Oracle Cloud Infrastructure SDK for .NET enables you to write code to manage Oracle Cloud Infrastructure resources.

This SDK is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

**Download:** [GitHub](#) or [Nuget](#).

**Requirements**

To use the SDK for .NET, you must have the following:

- An Oracle Cloud Infrastructure account.
- A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see [Adding Users](page 57). For a list of typical policies you may want to use, see [Common Policies](page 2142).
- A key pair used for signing API requests, with the public key uploaded to Oracle. Only the user calling the API should be in possession of the private key. For more information, see [SDK and CLI Configuration File](page 4184).
- [.NET Standard version 2.0 or higher](#)

**Services Supported**

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Compute Instance Agent (Oracle Cloud Agent)
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Cloud Guard
- Data Catalog
- Data Flow
- Data Integration
- Data Safe
- Data Science
- Data Transfer
- Database
- Database Management
- Digital Assistant
- DNS
- Email Delivery
Contact Us

Contributions
Got a fix for a bug or a new feature you'd like to contribute? The SDK is open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the SDK for .NET is released, subscribe to the Atom feed.

Questions or Feedback
- GitHub Issues: To file bugs and feature requests only
- Stack Overflow: Please use the oracle-cloud-infrastructure and oci-dotnet-sdk tags in your post
- The Developer Tools section of the Oracle Cloud forums
• My Oracle Support

Getting Started

This topic describes how to install and configure the SDK for .NET.

To use a specific Oracle Cloud Infrastructure service in your project, you can use the dotnet add package command from the root directory of your project workspace that contains the project file. The syntax for the add package command is:

```
dotnet add package <PACKAGE_ID> -v <DESIRED_VERSION>
```

If you do not specify a version number, the `add package` command will install the latest version.

This example installs the latest version of the Core Service package:

```
dotnet add package OCI.DotNetSDK.Core
```

This example installs version 1.0.0 of the Identity Service package:

```
dotnet add package OCI.DotNetSDK.Identity -v 1.0.0
```

**Note:**

To avoid dependency conflicts, you should use the same versions of all OCI .NET SDK Nuget packages within an application.

Downloading the SDK from GitHub

You can download the SDK for .NET as a zip archive from GitHub. It contains the SDK, all of its dependencies, documentation, and examples.

Installing the SDK with Yum

If you're using Oracle Linux 7, you can use yum to install the OCI SDK for .NET.

1. To install the OCI SDK for .NET using yum:

   ```
   sudo yum-config-manager --enable ol7_developer
   sudo yum install oci-dotnet-sdk
   ```

   The OCI Dotnet SDK service packages and its dependencies are located in `/usr/lib/dotnet/NuPkgs/`.

2. So the dotnet CLI can find the installed packages, you must do one of the following:

   a. Create a file named `nuget.config` in the root of your .NET application project and add the following content:

   ```xml
   <?xml version="1.0" encoding="utf-8"?>
   <configuration>
     <packageSources>
       <clear />
       <add key="local" value="/usr/lib/dotnet/NuPkgs" />
     </packageSources>
   </configuration>
   ```

   ...or...

   b. Use the `--source` option with the dotnet CLI commands, passing in the directory `/usr/lib/dotnet/NuPkgs/`. For example:

   ```
   dotnet build --source /usr/lib/dotnet/NuPkgs/
dotnet restore --source /usr/lib/dotnet/NuPkgs/
   ```
Developer Tools

3. To get information about the installed package, run the following command:

```bash
rpm -qi oci-dotnet-sdk
```

4. Add the OCI Service packages to your project using the dotnet command line:

```bash
dotnet add package OCI.DotNetSDK.Common
dotnet add package OCI.DotNetSDK.Audit --version 4.3.0
```

5. You can now import namespaces into your project. For example:

```csharp
using Oci.AuditService;
using Oci.AuditService.Models;
using Oci.Common;
using Oci.Common.Auth;
```

Using the SDK for .NET with Nuget

**Nuget.**

Configuring the SDK

The SDK services need two types of configuration: credentials and client-side HTTP settings.

**Configuring Credentials**

First, you need to set up your credentials and config file. For instructions, see [SDK and CLI Configuration File](#) on page 4184.

Next, you need to set up the client to use the credentials. The credentials are abstracted through an `IAuthenticationDetailsProvider` interface that the client needs to implement.

These examples show implementations of `ConfigFileAuthenticationDetailsProvider` and `SimpleAuthenticationDetailsProvider`.

**Using a Standard Configuration**

If you use standard config file keys and the standard config file location, you can use `ConfigFileAuthenticationDetailsProvider`:

```csharp
using Oci.Common.Auth;

// uses DEFAULT profile in default file location: i.e ~/.oci/config
var provider = new ConfigFileAuthenticationDetailsProvider("DEFAULT");
```

**Using a Custom Configuration**

If you are using custom key names in the config file, you can use `SimpleAuthenticationDetailsProvider`.

To load a config with or without a profile:

```csharp
using Oci.Common;

var config = ConfigFileReader.Parse(ConfigFileReader.DEFAULT_FILE_PATH);
```
var configWithProfile = ConfigFileReader.Parse(ConfigFileReader.DEFAULT_FILE_PATH, "DEFAULT");

Next, create an Auth provider using SimpleAuthenticationDetailsProvider:

using Oci.Common;
using Oci.Common.Auth;

var config = ConfigFileReader.Parse(ConfigFileReader.DEFAULT_FILE_PATH);

// The private key supplier can be created with the file path, or using the config file
var provider = new SimpleAuthenticationDetailsProvider {
    TenantId = config.GetValue("tenancy"),
    UserId = config.GetValue("user"),
    Fingerprint = config.GetValue("fingerprint"),
    Region = Region.FromRegionId(config.GetValue("region")),
    PrivateKeySupplier = new FilePrivateKeySupplier(config.GetValue("key_file"),
        config.GetValue("pass_phrase"))
};

Configuring Client-Side Options

Create a client-side configuration through the ClientConfiguration class. If you do not provide your own configuration, the SDK for .NET uses a default configuration.

The following example shows how to provide your own configuration:

var clientConfiguration = new ClientConfiguration {
    ClientUserAgent = "DotNet-SDK-Example",
    RetryConfiguration = new RetryConfiguration {
        MaxAttempts = 5,
        // retries the request if the response status code is in the range [400-499] or [500-599]
        RetryableStatusCodeFamilies = new List<int> { 4, 5 }
    }
};

Configuring Custom Options

In the configuration file, you can insert custom key-value pairs that you define, and then reference them as necessary. For example, you could specify a frequently used compartment ID in the config file:

[DEFAULT]
user=ocid1.user.oc1..<your_unique_id>
fingerprint=<your_fingerprint>
key_file=~/.oci/oci_api_key.pem
tenancy=ocid1.tenancy.oc1..<your_unique_id>
customCompartmentId=ocid1.compartment.oc1..<your_unique_id>

Then you can retrieve the value:

using Oci.Common;
var config = ConfigFileReader.parse(ConfigFileReader.DEFAULT_FILE_PATH);
String compartmentId = config.GetValue("customCompartmentId");
Enabling Logging

The OCI SDK for .NET uses the NLog package for logging. NLog is automatically installed with the .NET SDK, so no additional installation is required.

To enable logging in your project:

1. Add an NLog.config file at the project's root directory. You can find an example NLog.config file here
2. Add an ItemGroup section in the project file. For example:

```xml
<ItemGroup>
  <Content Include="PATH TO NLog.config File" />
  <CopyToOutputDirectory>PreserveNewest</CopyToOutputDirectory>
</Content>
```

3. To log from an application, create a Logger and use the Info() method. For example:

```csharp
var logger = NLog.LogManager.GetCurrentClassLogger();
logger.Info("Hello World");
```

**Note:**

Only SDK logging will be captured if you don’t create a logger from an application.

Concepts

This topic explains some of the key concepts for using the Oracle Cloud Infrastructure SDK for .NET.

Raw Requests

Raw requests can be useful, and in some cases necessary. Typical use cases include using your own HTTP client, making a OCI-authenticated request to an alternate endpoint, or making a request to a OCI API that is not currently supported in the SDK. The SDK for .NET exposes the OciHttpClientHandler class that you can use to create a client handler which signs the request.

This raw request example on GitHub shows how to use the OciHttpClientHandler.

Setting the Endpoints

Service endpoints can be set in several ways:

- Call `SetEndpoint(<YOUR_ENDPOINT>)` on the service client instance. This lets you specify a full host name (for example, https://www.example.com).
- Call `SetRegion(<YOUR_REGION_ID>)` on the service client instance. This selects the appropriate host name for the service for the given region. However, if the service is not supported in the region you set, the SDK for .NET returns an error.
- Call `SetRegion(<Region>)` on the service client instance. For example, `SetRegion(Region.US_PHOENIX_1)`.
- Pass the region in the configuration file. For more information, see SDK and CLI Configuration File on page 4184.

An example on setting endpoint can be found on GitHub.

Note that a service client instance cannot be used to communicate with different regions. If you need to make requests to different regions, create multiple service client instances.

New Region Support

If you are using a version of the SDK released prior to the announcement of a new region, you can use a workaround to reach it.

A region is a localized geographic area. For more information on regions and how to identify them, see Regions and Availability Domains on page 180.
A realm is a set of regions that share entities. You can identify your realm by looking at the domain name at the end of the network address. For example, the realm for `xyz.abc.123.oraclecloud.com` is `oraclecloud.com`.

You must first call `Region.Register()` to register the new region, and then you can set the region by either using the configuration file or by calling the `SetRegion` method.

An example on adding a new region can be found on GitHub.

**oraclecloud.com Realm**

For regions in the oraclecloud.com realm, you can pass new region names just as you would pass ones that are already defined in the `Region` enum for your SDK version.

To set the region:

```csharp
using Oci.IdentityService;
var identityClient = new IdentityClient(<IAuthenticationDetailsProvider>);
identityClient.SetRegion("US_NEWYORK_1");
```

**Other Realms**

For regions in realms other than oraclecloud.com, you can use the following workarounds to reach new regions with earlier versions of the SDK.

To set the region:

```csharp
using Oci.IdentityService;
var identityClient = new IdentityClient(<IAuthenticationDetailsProvider>);
identityClient.SetEndpoint("https://<your_endpoint>.com");
```

**Uploading Large Objects**

The Object Storage service supports multipart uploads to make large object uploads easier by splitting the large object into parts. The SDK for .NET supports raw multipart upload operations for advanced use cases, as well as a higher level upload class that uses the multipart upload APIs. Managing Multipart Uploads provides links to the APIs used for multipart upload operations. Higher level multipart uploads are implemented using the `UploadManager`, which will: split a large object into parts for you, upload the parts in parallel, and then recombine and commit the parts as a single object in storage.

The `UploadObject` example shows how to use the `UploadManager` to automatically split an object into parts for upload to simplify interaction with the Object Storage service.

**Paginated Responses**

For large result sets, most OCI calls supported paginated responses. Paginated responses require you to make multiple calls to the list operation, passing in the value of the most recent response's next token. The pagination module allows you to:

- Load all possible results from a list call in one call
- Lazily load results using token-based paginated responses

For an example on how to use these functions, please see GitHub.

**Polling with Waiters**

The SDK offers *waiters* that allow your code to wait until a specific resource reaches a desired state. A waiter can be invoked in both a blocking or a non-blocking (with asynchronous callback) manner, and will wait until either the desired state is reached or a timeout is exceeded. Waiters abstract the polling logic you would otherwise have to write into an easy-to-use single method call.
Waiters are obtained through the service client (client.Waiters). Both a Get<Resource>Request and the desired lifecycle state are passed in to the Waiters.For<Resource> method.

For example:

```csharp
using Oci.CoreService;

public static Instance WaitForInstanceProvisioningToComplete(ComputeClient computeClient, String instanceId)
{
    GetInstanceRequest getInstanceRequest = new GetInstanceRequest
    { InstanceId = instanceId
    );
    GetInstanceResponse getInstanceResponse =
    computeClient.Waiters.ForInstance(getInstanceRequest,
    Instance.LifecycleStateEnum.Running).Execute();
    return getInstanceResponse.Instance;
}
```

Each `waiters.for<Resource>` method has two versions:

One version uses the default polling values. For example:

```csharp
Waiters.ForInstance(getInstanceRequest, Instance.LifecycleStateEnum.Running)
```

The other version gives you full control over how long to wait and how much time between polling attempts. For example:

```csharp
using Oci.Common.Waiters;
WaiterConfiguration waiterConfiguration = new WaiterConfiguration
{
    MaxAttempts = 5,
    GetNextDelayInSeconds = DelayStrategy.GetExponentialDelayInSeconds
};
Waiters.ForInstance(getInstanceRequest, waiterConfiguration,
Instance.LifecycleStateEnum.Running)
```

Some API requests return work request identifiers to track the progress of the request. Waiters can be used to wait until the work request has reached the desired state.

For example:

```csharp
using Oci.Common.Waiters;
using Oci.ContainerengineService;
using Oci.ContainerengineService.Responses;
using Oci.ContainerengineService.Requests;
CreateClusterResponse clusterResponse = await
    containerEngineClient.CreateCluster(createClusterRequest);
GetWorkRequestResponse workRequestResponse =
    WaitForWorkRequestFinished(containerEngineClient, workRequestId);
private static GetWorkRequestResponse
    WaitForWorkRequestFinished(ContainerEngineClient containerEngineClient,
    string workRequestId)
{
    var waiterConfiguration = new WaiterConfiguration
    {
        MaxAttempts = 5,
        GetNextDelayInSeconds = DelayStrategy.GetExponentialDelayInSeconds
    };
    GetWorkRequestRequest getWorkRequestRequest = new GetWorkRequestRequest
    {
```
Developer Tools

WorkRequestId = workRequestId
};
return
containerEngineClient.Waiters.ForWorkRequest(getWorkRequestRequest,
waiterConfiguration, WorkRequestStatus.Succeeded).Execute();
}
Further examples on waiters can be found on Github.
Exception Handling
When handling an exception, you can get more information about the HTTP request that caused it, such as the status
code or service code. You can also get the request ID when handling an exception by looking at the opcRequestId
property of the error object.
For example:

try {
var response = await identityClient.ListAllUsersResponses(listUserReq);
} catch (OciException e) {
logger.Info($"requestId: {e.OpcRequestId}");
logger.Info($"StatusCode: {e.StatusCode}");
logger.Info($"ServiceCode: {e.ServiceCode}");
}
Authenticating with Instance Principals
Instance principals is an IAM service feature that enables instances to be authorized actors (or principals) that
can perform actions on service resources. Each compute instance has its own identity, and it authenticates using
the certificates that are added to it. These certificates are automatically created, assigned to instances and rotated,
preventing the need for you to distribute credentials to your hosts and rotate them.
Note:
For more information on instance principals, see Calling Services from an
Instance on page 2410.
While using the .NET SDK on an OCI Instance, you can use
InstancePrincipalsAuthenticationDetailsProvider class as shown in the following example. You
will not need to provide your authentication details when you use this class.
using Oci.Common.Auth;
using Oci.IdentityService;
// Creates an Instance Principal provider that holds authentication details
of the OCI Instance
var instanceProvider = new
InstancePrincipalsAuthenticationDetailsProvider();
// Create a client for the service to enable using its APIs
var client = new IdentityClient(instanceProvider);
A full working example of using instance principals with the OCI .NET SDK can be found on GitHub.
Examples
GitHub
Examples of SDK usage can be found on GitHub, including:
•
•
•

Example: Create an instance
Example: Invoke Oracle Function
Example: Move Compartment

Oracle Cloud Infrastructure User Guide

4262


The examples are also in the downloadable .zip file for the SDK. Examples for older versions of the SDK are in the downloadable .zip for the specific version, available on GitHub.

If you'd like to see another example not already covered, file a GitHub issue.

**SDK Reference**

In addition to the examples found on GitHub, the SDK for .NET API reference contains code examples that you can copy and modify to run in your own environment.

**Running Examples**

1. Use git to clone the OCI SDK for .NET repository:
   
   ```
   git clone https://github.com/oracle/oci-dotnet-sdk.git
   ```

2. Create a configuration file in your home directory (`~/.oci/config`). See SDK and CLI Configuration File on page 4184 for more information.

3. Change directory into the .NET Examples folder. For example:
   
   ```
   cd ./oci-dotnet-sdk/Examples/
   ```

4. All of the examples require the environment variable `OCI_COMPARTMENT_ID` populated with the tenant ID or compartment ID.

5. From the command line, run `dotnet run`. The Audit example runs by default.

6. To run any other example, make sure it has a `Main()` function.

**SDK for Go**

The Oracle Cloud Infrastructure SDK for Go enables you to write code to manage Oracle Cloud Infrastructure resources.

This SDK and sample is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

**Download:** Download the SDK from GitHub.

**Documentation:** The reference documentation is available from Oracle here and at godoc.org.

---

**Tip:**

The SDK for Go is pre-configured with your credentials and ready to use immediately from within Cloud Shell. For more information on using the SDK for Go from within Cloud Shell, see SDK for Go Cloud Shell Quick Start on page 4189.

**Services Supported**

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Compute Instance Agent (Oracle Cloud Agent)
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Cloud Guard
- Data Catalog
- Data Flow
• Data Integration
• Data Safe
• Data Science
• Data Transfer
• Database
• Database Management
• Digital Assistant
• DNS
• Email Delivery
• Events
• File Storage
• Functions
• Golden Gate
• Health Checks
• IAM
• Integration Cloud
• Key Management (for the Vault service)
• Limits
• Load Balancing
• Logging
• Logging Analytics
• Logging Search
• Logging Ingestion
• Management Agent Cloud
• Management Dashboard
• Marketplace
• Monitoring
• MySQL Database
• NoSQL Database Cloud
• Notifications
• Object Storage
• OCI Registry
• Operations Insights
• Optimizer
• Organizations
• OS Management
• Quotas
• Resource Manager
• Roving Edge Infrastructure
• Search
• Secret Management (for the Vault service)
• Service Connector Hub
• Streaming
• Support Management
• Usage
• VMWare Solution
• Web Application Acceleration and Security
• Work Requests (Compute, Database)
Installing with Resource Manager

You can use Resource Manager to install the Oracle Cloud Development Kit on a Compute instance in your compartment. The Oracle Cloud Development Kit includes the SDK for Go, along with other Oracle development tools.

Installing with yum

If you're using Oracle Linux 7, you can use yum to install the OCI SDK for Go:

```
sudo yum-config-manager --enable ol7_developer
sudo yum install go-oci-sdk.x86_64
```

The OCI Go SDK requires at least Golang version 1.13. To install a recent version of Golang:

```
sudo yum install -y oracle-golang-release-el7.x86_64
sudo yum install golang
```

Contact Us

Contributions

Got a fix for a bug or a new feature you'd like to contribute? The SDK is open source and accepting pull requests on GitHub.

Notifications

To be notified when a new version of the SDK for Go is released, subscribe to the Atom feed.

Questions or Feedback

- GitHub Issues: To file bugs and feature requests only
- Stack Overflow: Please use the oracle-cloud-infrastrucure and oci-go-sdk tags in your post
- Developer Tools section of the Oracle Cloud forums
- My Oracle Support

SDK for Ruby

The Oracle Cloud Infrastructure SDK for Ruby enables you to write code to manage Oracle Cloud Infrastructure resources.

Note:

This project is no longer being actively developed by Oracle. We will continue to address security vulnerabilities for the foreseeable future, and will respond to questions on github, but have no plans to introduce any new functionality, and may not be able to address any non-security related issues. We encourage developers to migrate to other OCI SDKs, and developers may fork the project and enhance it as they desire.

This SDK and sample are dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

Download: The SDK for Ruby is available on GitHub or RubyGems.

Documentation: SDK for Ruby documentation.

Installing with yum

If you're using Oracle Linux 7, you can use yum to install the OCI SDK for Ruby.

The following example shows how to use yum to install the OCI SDK for Ruby 2.6:

```
sudo yum-config-manager --enable ol7_developer
```
sudo yum install -y oci-ruby-sdk
source /opt/rh/rh-ruby26/enable
export GEM_PATH="/usr/share/gems:`gem env gempath`"

**Services Supported**

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Cloud Guard
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Data Catalog
- Data Flow
- Data Integration
- Data Safe
- Data Science
- Data Transfer
- Database
- Digital Assistant
- DNS
- Email Delivery
- Events
- File Storage
- Functions
- Health Checks
- IAM
- Integration
- Key Management (for the Vault service)
- Limits
- Logging
- Logging Analytics
- Logging Search
- Logging Ingestion
- Load Balancing
- Management Agent Cloud
- Management Dashboard
- Marketplace
- Monitoring
- MySQL Database
- NoSQL Database Cloud
- Notifications
- Object Storage
- OS Management
• Quotas
• Resource Manager
• Roving Edge Infrastructure
• Search
• Secret Management (for the Vault service)
• Service Connector Hub
• Streaming
• Support Management
• Usage
• VMWare Solution
• Web Application Acceleration and Security
• Work Requests (Compute, Database)

Contact Us

Contributions
Got a fix for a bug or a new feature you'd like to contribute? The SDK is open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the SDK for Ruby is released, subscribe to the Atom feed.

Questions or Feedback
• GitHub Issues: To file bugs and feature requests only
• Stack Overflow: Please use the oracle-cloud-infrastructure and oci-ruby-sdk tags in your post
• Developer Tools section of the Oracle Cloud forums
• My Oracle Support

PL/SQL SDK
The Oracle Cloud Infrastructure SDK for PL/SQL enables you to write PL/SQL code to manage Oracle Cloud Infrastructure resources.

The latest version of the SDK is pre-installed by Oracle for all Autonomous Databases using shared Exadata infrastructure.

Requirements
To use the PL/SQL SDK, you must have the following:
• An Oracle Cloud Infrastructure account.
• A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users on page 57. For a list of typical policies you may want to use, see Common Policies on page 2142.
• A key pair used for signing API requests, with the public key uploaded to Oracle. Only the user calling the API should be in possession of the private key.

Services Supported
• Analytics Cloud
• Announcements
• API Gateway
• Application Migration
• Audit
• Autoscaling (Compute)
Examples

This section contains examples of how to use the PL/SQL SDK.

Working with Object Storage Buckets
The following example shows examples of how to use the PL/SQL SDK to create and delete buckets using the OCI Object Storage service:

```
-- ###################################################################
-- ## Create bucket ##
-- ###################################################################
set serveroutput on
declare
  response_body  dbms_cloud_oci_obs_object_storage_bucket_t;
  response       dbms_cloud_oci_obs_object_storage_create_bucket_response_t;
  bucket_details dbms_cloud_oci_obs_object_storage_create_bucket_details_t;
  json_obj       json_object_t;
  l_keys         json_key_list;
begin
  bucket_details :=
    dbms_cloud_oci_obs_object_storage_create_bucket_details_t();
  bucket_details.name := 'bucketname';
  bucket_details.compartment_id := 'compartment_OCID';
  response := dbms_cloud_oci_obs_object_storage.create_bucket(
    namespace_name => 'namespace-string',
    opc_client_request_id => 'random-request-id',
    create_bucket_details => bucket_details,
    credential_name => 'OCI_KEY_CRED',
    region => 'region-identifier');
  response_body := response.response_body;
  -- Response Headers
  dbms_output.put_line('Headers: ' || CHR(10) || '------------');
  json_obj := response.headers;
  l_keys := json_obj.get_keys;
  for i IN 1..l_keys.count loop
    dbms_output.put_line(l_keys(i)||':'||
      json_obj.get(l_keys(i)).to_string);
  end loop;
  -- Response status code
  dbms_output.put_line('Status Code: ' || CHR(10) || '------------' ||
    CHR(10) || response.status_code);
  dbms_output.put_line(CHR(10));
  -- Response body
  dbms_output.put_line(response_body.namespace);
  dbms_output.put_line(response_body.name);
  dbms_output.put_line(response_body.compartment_id);
  dbms_output.put_line(response_body.metadata.to_string());
  dbms_output.put_line(response_body.created_by);
  dbms_output.put_line(response_body.time_created);
  dbms_output.put_line(response_body.approximate_count);
  dbms_output.put_line(response_body.approximate_size);
  dbms_output.put_line(response_body.etag);
  dbms_output.put_line(response_body.public_access_type);
  dbms_output.put_line(response_body.storage_tier);
  dbms_output.put_line(response_body.freeform_tags.to_string());
  dbms_output.put_line(response_body.defined_tags.to_string());
  dbms_output.put_line(response_body.kms_key_id);
  dbms_output.put_line(response_body.object_lifecycle_policy_etag);
  dbms_output.put_line(response_body.id);
end;
/```
set serveroutput on
declare
response       dbms_cloud_oci_obs_object_storage_delete_bucket_response_t;
json_obj       json_object_t;
l_keys         json_key_list;
begin

response := dbms_cloud_oci_obs_object_storage.delete_bucket(
    namespace_name => 'namespace-string',
    bucket_name => 'bucketname',
    credential_name => 'OCI_KEY_CRED',
    region => 'region-identifier');

-- Response Headers
dbms_output.put_line('Headers: ' || CHR(10) ||'------------');
json_obj := response.headers;
l_keys := json_obj.get_keys;
for i IN 1..l_keys.count loop
    dbms_output.put_line(l_keys(i)||':'||
        json_obj.get(l_keys(i)).to_string);
end loop;

-- Response status code
dbms_output.put_line('Status Code: ' || CHR(10) || '------------' ||
    CHR(10) || response.status_code);
dbms_output.put_line(CHR(10));
end;
/

Working with Object Storage Objects

The following example shows how to use the PL/SQL SDK to store and retrieve objects using the OCI Object Storage service:

declare
my_blob_data   blob;
response       dbms_cloud_oci_obs_object_storage_put_object_response_t;
json_obj       json_object_t;
l_keys         json_key_list;
begin

/* Some processing producing BLOB data and populating my_blob_data */
response := dbms_cloud_oci_obs_object_storage.put_object(
    namespace_name => 'namespace-string',
    bucket_name => 'bucketname',
    object_name => 'objectname',
    put_object_body => my_blob_data,
    credential_name => 'OCI_KEY_CRED',
    region => 'region-identifier');

-- Response Headers
dbms_output.put_line('Headers: ' || CHR(10) ||'------------');
json_obj := response.headers;
l_keys := json_obj.get_keys;
for i IN 1..l_keys.count loop
    dbms_output.put_line(l_keys(i)||':'||
        json_obj.get(l_keys(i)).to_string);
end loop;
-- Response status code
dbms_output.put_line('Status Code: ' || CHR(10) || '------------' ||
CHR(10) || response.status_code);
dbms_output.put_line(CHR(10));
end;
/

-- #################################
-- ## Get Object      ##
-- #################################
declare
    response       dbms_cloud_oci_obs_object_storage_get_object_response_t;
    response_body  blob;
    json_obj       json_object_t;
    l_keys         json_key_list;
begin
    response := dbms_cloud_oci_obs_object_storage.get_object(
        namespace_name => 'namespace-string',
        bucket_name => 'bucketname',
        object_name => 'objectname',
        credential_name => 'OCI_KEY_CRED',
        region => 'region-identifier');
    response_body := response.response_body;
    -- Response Headers
    dbms_output.put_line('Headers: ' || CHR(10) || '------------');
    json_obj := response.headers;
    l_keys := json_obj.get_keys;
    for i IN 1..l_keys.count loop
        dbms_output.put_line(l_keys(i)||':'||
        json_obj.get(l_keys(i)).to_string);
    end loop;
    -- Response status code
    dbms_output.put_line('Status Code: ' || CHR(10) || '------------' ||
    CHR(10) || response.status_code);
    dbms_output.put_line(CHR(10));
    -- Response body
    dbms_output.put_line('Contents: ' ||
    UTL_RAW.cast_to_varchar2(response_body));
end;
/

Listing Compartments

The following example shows how to list compartments using the PL/SQL SDK:

-- #################################
-- ## ListCompartments  ##
-- #################################
set serveroutput on
declare
    response_body  dbms_cloud_oci_id_identity_compartment_tbl;
    response       dbms_cloud_oci_id_identity_list_compartments_response_t;

```sql
json_obj       json_object_t;
l_keys         json_key_list;
begin
  response := dbms_cloud oci id identity . list compartments(
      compartment_id  => 'compartment OCID',
      limit           => 2,
      credential_name => 'OCI KEY CRED',
      region          => 'region identifier');

  response_body := response . response_body;

  -- Response Headers
  dbms_output . put_line ('Headers: ' || CHR(10) || '----------');
  json_obj := response . headers;
  l_keys := json_obj . get_keys;
  for i IN 1..l_keys . count loop
    dbms_output . put_line (l_keys (i) || ':' ||
                           json_obj . get (l_keys (i)) . to_string);
  end loop;

  -- Response status code
  dbms_output . put_line ('Status Code: ' || CHR(10) || '----------' ||
                           CHR(10) || response . status_code);
  dbms_output . put_line (CHR(10));
  for i in 1 .. response_body . count loop
    dbms_output . put_line (response_body (i) . id);
    dbms_output . put_line (response_body (i) . compartment_id);
    dbms_output . put_line (response_body (i) . name);
    dbms_output . put_line (response_body (i) . description);
    dbms_output . put_line (response_body (i) . time_created);
    dbms_output . put_line (response_body (i) . lifecycle_state);
    dbms_output . put_line (response_body (i) . inactive_status);
    dbms_output . put_line (response_body (i) . is_accessible);
    dbms_output . put_line (response_body (i) . freeform_tags . to_string());
    dbms_output . put_line (response_body (i) . defined_tags . to_string());
  end loop;
end;
/
```

### Working With Streams

The following example shows how to create and delete stream pools using the PL/SQL SDK:

```sql
-- #################################
-- ## Create stream pool ##
-- #################################
set serveroutput on
declare
  response_body       dbms_cloud oci st stream admin stream pool_t;
  response
    dbms_cloud oci st stream admin create stream pool response_t;
  stream_pool_details
    dbms_cloud oci st stream admin create stream pool details_t;
  json_obj            json_object_t;
  l_keys              json_key_list;
begin
  stream_pool_details :=
    dbms_cloud oci st stream admin create stream pool details_t();
  stream_pool_details . name := 'streampoolname';
```
stream_pool_details.compartment_id := 'compartment_OCID';

response := dbms_cloud_oci_st_stream_admin.create_stream_pool(
    create_stream_pool_details => stream_pool_details,
    opc_request_id => 'random-request-id',
    credential_name => 'OCI_KEY_CRED',
    region => 'region-identifier');
response_body := response.response_body;

-- Response Headers
dbms_output.put_line('Headers: ' || CHR(10) ||'------------');
json_obj := response.headers;
l_keys := json_obj.get_keys;
for i IN 1..l_keys.count loop
    dbms_output.put_line(l_keys(i)||':'||
        json_obj.get(l_keys(i)).to_string);
end loop;

-- Response status code
dbms_output.put_line('Status Code: ' || CHR(10) || '------------' ||
   CHR(10) || response.status_code);

-- Response body
dbms_output.put_line('id: ' || response_body.id);
dbms_output.put_line('name: ' || response_body.name);
dbms_output.put_line('compartment_id: ' || response_body.compartment_id);
dbms_output.put_line('lifecycle_state: ' || response_body.lifecycle_state);
for i in 1 .. response_body.private_endpoint_settings.nsg_ids.count loop
    dbms_output.put_line(response_body.private_endpoint_settings.nsg_ids(i));
end loop;
/

-- # Delete stream pool #
set serveroutput on
declare
    response dbms_cloud_oci_st_stream_admin_delete_stream_pool_response_t;
    json_obj json_object_t;
    l_keys json_key_list;
begin
    response := dbms_cloud_oci_st_stream_admin.delete_stream_pool(
        stream_pool_id => 'stream-pool-ocid',
        credential_name => 'OCI_KEY_CRED',
        region => 'region-identifier');

    -- Response Headers
    dbms_output.put_line('Headers: ' || CHR(10) ||'------------');
    json_obj := response.headers;
    l_keys := json_obj.get_keys;
    for i IN 1..l_keys.count loop
        dbms_output.put_line(l_keys(i)||':'||
            json_obj.get(l_keys(i)).to_string);
    end loop;
end;
DevOps Tools and Plug-ins

Oracle Cloud Infrastructure provides a number of DevOps tools and plug-ins for working with Oracle Cloud Infrastructure services. These can simplify provisioning and managing infrastructure or enable automated testing and continuous delivery.

**Terraform Provider** - Manage "infrastructure as code" with this component that connects Terraform to a given Oracle Cloud Infrastructure service.

- **Documentation**: Terraform Provider on page 4275
- **Download**: GitHub

**OCI Modules for PowerShell** - A set of cmdlet modules that can be used with PowerShell Core to manage Oracle Cloud Infrastructure resources, such as Compute, Load Balancing, and Database services.

- **Documentation**: OCI Modules for PowerShell on page 4314
- **Download**: GitHub or PowerShell Gallery

**Ansible Collection** - Automate provisioning and configuring of Oracle Cloud Infrastructure resources, such as Compute, Load Balancing, and Database services.

- **Documentation**: Ansible Collection on page 4330
- **Download**: GitHub

**Compute Jenkins Plug-in** - Bring up and down services or nodes as required to serve Jenkins Build Jobs and dynamically allocate Oracle Cloud Infrastructure resources for continuous integration tasks.

- **Documentation**: Compute Jenkins Plug-in on page 4344
- **Download**: GitHub

**Chef Knife Plug-in** - Manage Oracle Cloud Infrastructure resources with Chef Knife, a command line tool that provides an interface between a local chef-repo and the Chef server.

- **Documentation**: Chef Knife Plug-in on page 4344
- **Download**: GitHub

**Grafana Plug-in** - Visualize metrics from the Monitoring service in your Grafana instance.

- **Documentation**: Grafana Plug-in on page 4345
- **Download**: GitHub

**Terraform Kubernetes Installer** - Provision and configure the resources needed to run a highly available and configurable Kubernetes cluster.

- **Download**: GitHub

**Kubernetes Volume Provisioner** - Enable dynamic provisioning of storage resources when running Kubernetes on Oracle Cloud Infrastructure.

- **Download**: GitHub

DevOps Integrations

- **Jenkins X Integration**: Create a new Kubernetes cluster on Oracle Cloud Infrastructure Container Engine for Kubernetes.
- **Packer Integration**: Create reusable custom images.

Other Services and Features for DevOps

Oracle Cloud Infrastructure provides other services and features relevant to DevOps professionals.

- **Container Engine for Kubernetes (OKE)** Reliably build, deploy, and manage cloud-native containerized applications. You specify the compute resources that your applications require, and Container Engine for Kubernetes provisions them on Oracle Cloud Infrastructure in an existing tenancy.
• **Oracle Cloud Infrastructure Registry** Store, share, and manage development artifacts like Docker images. As Oracle Cloud Infrastructure Registry is managed by Oracle, your applications are deployed reliably and you don’t have to deal with operational issues.

**Terraform Provider**

Terraform is an open source tool that allows you to programmatically manage, version, and persist infrastructure through the "infrastructure-as-code" model. Terraform configurations codify your infrastructure in declarative files that contain the steps required to provision your infrastructure and maintain its state. You can share these files among team members, treat them as code, edit, review, and version them.

Terraform uses providers to interface between the Terraform engine and the supported cloud platform. The Oracle Cloud Infrastructure (OCI) Terraform provider is a component that connects Terraform to the OCI services that you want to manage.

You can use the OCI Terraform provider to manage OCI resources wherever you use a Terraform distribution, including Terraform Cloud and the OCI Resource Manager. Oracle Public Cloud has its own Terraform provider.

Resource Manager is an Oracle Cloud Infrastructure service that uses Terraform to automate the process of provisioning your Oracle Cloud Infrastructure.

**Tip:**

You can migrate existing Terraform state files to Resource Manager using an Import State job.

See Getting Started on page 102 to begin using the Terraform provider to manage your OCI resources.

**Licensing:** This provider and samples are licensed under the Mozilla Public License 2.0; third-party content is separately licensed as described in the code.

**Availability**

The Oracle Cloud Infrastructure Terraform provider is region agnostic. You can use the Terraform provider to work with supported services in all Oracle Cloud Infrastructure regions in which they are available. Government Cloud customers should use the FIPS-compatible OCI Terraform provider.

See Regions and Availability Domains on page 180 for the list of available regions, along with associated locations, region identifiers, region keys, and availability domains.

**Contributions**

Got a fix for a bug, or a new feature you’d like to contribute? The Terraform provider is open source and accepting pull requests on GitHub.

**Notifications**

To be notified when a new version of the OCI Terraform provider is released, subscribe to the Atom feed.

**Questions or Feedback**

Refer to Troubleshooting Basics and a list of common issues to see if your question has an answer.

You can also use GitHub to file bugs and submit feature requests.

**What’s New**

Terraform, the Oracle Cloud Infrastructure (OCI) Terraform provider, and Terraform modules all have the ability to introduce changes or add new functionality.

**Terraform Updates**

Major Terraform releases might include changes in behavior you should consider when upgrading.

**Terraform v0.14**

The Oracle Cloud Infrastructure (OCI) Terraform provider now supports Terraform v0.14.

Terraform v0.14 changes the output of the `terraform plan` command and introduces a dependency lock file you can use to track the version of the (OCI) Terraform provider used to interact with your OCI resources.

Refer to the official Terraform v0.14 upgrade guide for more information.
Concise Terraform plan output

To reduce the verbosity of `terraform plan` output, Terraform output now omits any attribute that has not changed, except for some attributes whose values often contain human-recognizable identifying information.

You can temporarily re-enable verbose output by setting the environment variable `TF_X_CONCISE_DIFF=0` when you run Terraform.

Sensitive values in Terraform plan output

Because Terraform v0.14 tracks expressions whose result is derived from a sensitive input variable or sensitive output value, you might find that more values are obscured in the `terraform plan` output than would have been in earlier versions.

If a different module uses a value in its output that was derived from a sensitive variable or value, you must set `sensitive = true` in the output of the second module.

Provider dependency lock file

In Terraform v0.13 and earlier, the `terraform init` command would always install the newest version of any provider in the configuration that would meet the configured version constraints. To keep the behavior of an already tested configuration as stable as possible unless intentionally changed by the user, Terraform v0.14 introduces a new dependency lock file.

Terraform generates this file automatically after running `terraform init` in the same directory as the configuration's root module. The dependency lock file includes the specific version numbers selected for each provider, including the OCI Terraform provider. After running `terraform init` for the first time after upgrading to Terraform v0.14, you will find a new file `.terraform.lock.hcl` in your root module directory. Future initializations of Terraform automatically read and respect the entries in that file.

Because of this new feature, manually placing extra plugins into the local cache directory `.terraform/plugins` is no longer effective.

Terraform v0.12

If upgrading to Terraform v0.12, the Oracle Cloud Infrastructure (OCI) Terraform provider and some existing configurations might need to be updated as well.

See Upgrading Configurations to Terraform v0.12 on page 4294 for detailed information.

Tutorials

For step-by-step instructions and examples of using Terraform and Oracle Cloud Infrastructure, see the following tutorials:

• Set Up the OCI Terraform Provider
• Create a Compartment
• Create a Compute Instance
• Create a Virtual Cloud Network
• Set Up a Simple Infrastructure
• Create a Kubernetes Cluster
• Set up Resource Discovery
• Create Scripts and State Files with Resource Discovery

For More Information

For more information, see the following resources:

• Blog: Getting Started Using Terraform with OCI

Examples and Solutions

The Oracle Cloud Infrastructure (OCI) Terraform provider uses Terraform configuration files to manage your OCI infrastructure.

Referring to existing example configurations and sample solutions can help you understand HashiCorp Configuration Language format (HCL) and see how it is used to define OCI resources.
You can also modify examples or entire solution sets to meet your needs.

Example Configurations

We provide many example Terraform configuration files that show you how to create specific OCI resources. These examples are intended to be as simple as possible. In most cases, they contain only the specific resource and any dependencies required for it to run.

Examples are are grouped by service, including Compute, Database, Networking, Load Balancing, and several others. These do not represent production configurations or real world scenarios, but they can serve as a starting point and be modified and combined as necessary.

Sample Solutions

Oracle also provides sample solutions for Resource Manager. Resource Manager uses Terraform to automate deployment and operations for OCI resources.

Solutions can help those new to infrastructure-as-code and those who are updating production configurations. Use solutions to try out Resource Manager and inspect the underlying oracle-terraform-modules to familiarize yourself with Terraform configuration files.

Architecture Center

The Oracle Architecture Center contains reference architectures, solution playbooks, and best practices. You can filter the content to see Terraform-specific information that you can use with the OCI Terraform provider or Resource Manager.

Guides

This section describes how to configure the Oracle Cloud Infrastructure (OCI) Terraform provider for specific use cases and write Terraform configuration files that manage specific OCI resources.

See the following topics for additional information:

- Authoring Configurations on page 4277
- Specifying Versions on page 4283
- Enabling FIPS Compatibility on page 4284
- Managing Boot Volumes on page 4289
- Migrating an Exadata DB System to the New Resource Model on page 4291
- Targeting Multiple Regions on page 4293
- Upgrading Configurations to Terraform v0.12 on page 4294
- Using Object Storage for State Files on page 4297

Authoring Configurations

Overview

Using Terraform, you can describe your Oracle Cloud Infrastructure using the HashiCorp Configuration Language format (HCL) in Terraform configuration files (see Configuration Syntax). Terraform configuration files can use either of two formats: Terraform domain-specific language (HashiCorp Configuration Language format [HCL]), which is the recommended approach, or JSON format if the files need to be machine-readable. Configuration files that use the HCL format end with the .tf file extension; those using JSON format end with the .tf.json file extension. The Terraform format is human-readable, while the JSON format is machine readable.

Use Terraform configurations to define your Oracle Cloud Infrastructure (OCI) resources, variable definitions, data sources, and a great deal more. Terraform, then, converts your OCI configurations into a set of API calls against OCI API endpoints. The key to writing Terraform configuration is understanding how to abstract the desired infrastructure conceptually into Terraform configuration syntax.

Important:

While the Oracle Cloud Infrastructure API uses camelCase extensively, Terraform does not support camelCase in configuration files. For this reason,
Configuration File Requirements

Terraform configuration (.tf) files have specific requirements, depending on the components that are defined in the file. For example, you might have your Terraform provider defined in one file (provider.tf), your variables defined in another (variables.tf), your data sources defined in yet another.

Note:
For example configuration files, see Terraform Provider Examples on the Oracle Cloud Infrastructure GitHub.

Provider Definitions

The following example using Terraform syntax illustrates the requirements for an OCI Terraform provider definition, and also shows associated variable definitions. The provider definition relies on variables so that the configuration file itself does not contain sensitive data. Including sensitive data creates a security risk when exchanging or sharing configuration files.

```terraform
variable "tenancy_ocid" {}
variable "user_ocid" {}
variable "fingerprint" {}
variable "private_key_path" {}
variable "region" {}

provider "oci" {
  tenancy_ocid = "${var.tenancy_ocid}"
  user_ocid = "${var.user_ocid}"
  fingerprint = "${var.fingerprint}"
  private_key_path = "${var.private_key_path}"
  region = "${var.region}"
}
```

The `region` attribute specifies the geographical region in which your provider resources are created. To target multiple regions in a single configuration, you simply create a provider definition for each region and then differentiate by using a provider alias, as shown in the following example. Notice that only one provider, named "oci" is defined, and yet the oci provider definition is entered twice, once for the us-phoenix-1 region (with the alias "phx"), and once for the region us-ashburn-1 (with the alias "iad").

```terraform
variable "tenancy_ocid" {}
variable "user_ocid" {}
variable "fingerprint" {}
variable "private_key_path" {}
variable "compartment_ocid" {}

provider "oci" {
  region = "us-phoenix-1"
  alias = "phx"
  tenancy_ocid = "${var.tenancy_ocid}"
  user_ocid = "${var.user_ocid}"
  fingerprint = "${var.fingerprint}"
  private_key_path = "${var.private_key_path}"
}

provider "oci" {
  region = "us-ashburn-1"
  alias = "iad"
  tenancy_ocid = "${var.tenancy_ocid}"
  user_ocid = "${var.user_ocid}"
}
```
```java
fingerprint = "${var.fingerprint}"
private_key_path = "${var.private_key_path}"
}
```

For more information, see Provider Configuration.

**Variable Definitions**

Variables in Terraform represent parameters for Terraform modules. In variable definitions, each block configures a single input variable, and each definition can take any or all of three optional arguments:

- **type** (optional): Defines the variable type as one of three allowed values: string, list, and map. If this argument is not used, the variable type is inferred based on default. If no default is provided, the type is assumed to be string.
- **default** (optional): Sets the default value for the variable. If no default value is provided, the caller must provide a value or Terraform throws an error.
- **description** (optional): A human-readable description of the variable.

Following are examples of several variable definitions. Some definitions include optional parameters.

```java
variable "tenancy_ocid" {}
variable "user_ocid" {}
variable "fingerprint" {}
variable "private_key_path" {}
variable "region" {}

variable "AD" {
    default = "1"
    description = "Availability Domain"
}

variable "CPUCoreCount" {
    default = "2"
    type = "string"
}
```

For more information, see Input Variable Configuration. See also Input Variables.

**Output Configuration**

Output variables provide a means to support Terraform end-user queries. This allows users to extract meaningful data from among the potentially massive amount of data associated with a complex infrastructure. For example, you might be interested only in a handful of key values at any given time and defining output variables allows you to extract exactly the information that you need.

Following is a simple example in which only a few output variables (instance IP addresses and boot volume IDs) are defined:

```java
# Output the private and public IPs of the instance
output "InstancePrivateIPs" {
    value = ["${oci_core_instance.TFInstance.*.private_ip}"]
}

output "InstancePublicIPs" {
    value = ["${oci_core_instance.TFInstance.*.public_ip}"]
}

# Output the boot volume IDs of the instance
output "BootVolumeIDs" {
    value = ["${oci_core_instance.TFInstance.*.boot_volume_id}"]
}
```
For more information, see Output Variables. See also Output Configuration.

Resources

Resources are components of your Oracle Cloud Infrastructure. These resources include everything from low-level components such as physical and virtual servers, to higher-level components such as email and database providers, your DNS record.

Refer to the full reference of the OCI Terraform provider’s supported resources and data sources for usage, argument, and attribute details. The resources are grouped by service.

Declaring Resources

Following is a simple example of a resource definition that illustrates their basic structure.

```tenseindentresource "oci_core_virtual_network" "vcn1" {  
cidr_block = "10.0.0.0/16"  
dns_label = "vcn1"  
compartment_id = "$(var.compartment_ocid)"  
display_name = "vcn1" 
}
```

The resource declaration on the first line of the example uses the keyword "resource" and takes two parameters, resource type and resource name ("oci_core_virtual_network" and "vcn1" in the example). Inside the code block, then, is the resource configuration.

For more information, see Resource Configuration.

Referencing Resources in Another Stack

You can reference resources that exist in other stacks. The Terraform remote_state data source allows you to read output variables from state files.

For example, when writing a Terraform configuration for a new web application, you can make the web application use the subnet previously created from your network stack, as long as the required subnet values were output in the network stack state file. In the Terraform configuration for your new web application, do the following:

- Pull the state file of the existing network stack into the context of your current Terraform configuration.
- Load the pulled state file to a data source for remote state files.
- Populate the subnet data source in your current configuration with values from the relevant output variables of the referenced state file.
- Optionally print the identifying information for the populated data source to confirm expected values.

**Note:**

In addition to permissions required for Resource Manager operations, you'll need appropriate permissions for resource types you're referencing, in the compartment that you're referencing them. In this example, you need read permissions for network resources in the compartment where they're located.

The following Terraform configuration excerpt references a subnet in another stack.

```tenseindent# The following example assumes that the source stack (defined by `stack_id`) has output a value named `subnet_id`    # Terraform v0.12 is assumed
variable "stack_id" {} 

# Pull the state file of the existing Resource Manager stack (the network stack) into this context
data "oci_resourcemanager_stack_tf_state" "stack1_tf_state" {  
    stack_id   = "${var.stack_id}" 
} 
```

Oracle Cloud Infrastructure User Guide
local_path = "stack1.tfstate"
}

# Load the pulled state file into a remote state data source
data "terraform_remote_state" "external_stack_remote_state" {
    backend = "local"
    config = {
        path = "${data.oci_resourcemanager_stack_tf_state.stack1_tf_state.local_path}"
    }
}

# Populate a data source in this configuration using a value from the remote state data source
data "oci_core_subnet" "subnet1" {
    subnet_id = "${data.terraform_remote_state.external_stack_remote_state.outputs.subnet_id}"  
}

# Print the values of the populated data source
output "print-subnet1" {
    value = "${data.oci_core_subnet.subnet1}"  
}

Data Sources

Data sources represent read-only views of existing infrastructure intended for semantic use in Terraform configurations. Following is a simple example of a data source configuration to illustrate its basic structure:

# Gets a list of Availability Domains
data "oci_identity_availability_domains" "ADs" {
    compartment_id = "${var.tenancy_ocid}"
}

# Get DB node list
data "oci_database_db_nodes" "DBNodeList" {
    compartment_id = "${var.compartment_ocid}"
    db_system_id = "${oci_database_db_system.TFDBNode.id}"  
}

# Get DB node details
data "oci_database_db_node" "DBNodeDetails" {
    db_node_id = "${lookup(data.oci_database_db_nodes.DBNodeList.db_nodes[0], "id")}"  
}

# Gets the OCID of the first (default) vNIC
data "oci_core_vnic" "DBNodeVnic" {
    vnic_id = "${data.oci_database_db_node.DBNodeDetails.vnic_id}"  
}

For more information, see Data Source Configuration.

Filtering Data Sources

Data sources that return lists of resources support filtering semantics. To use a filter, include this block in your data source definition:

filter {
    name = ""
    values = ["""]
}
The name value corresponds to the qualified property name to filter with and the values lists can contain one or more values filter with.

Nested properties and map elements can be addressed by qualifying the property name with parent property name. Example r1 will give all the instances which have source_type image. Example r2 will give all the instances which contain a defined tag with value "42" for key CostCenter in the namespace Operations.

```hcl
data "oci_core_instances" "r1" {
  ...
  filter {
    name = "source_details.source_type"
    values = ["image"]
  }
}
data "oci_core_instances" "r2" {
  ...
  filter {
    name = "defined_tags.Operations.CostCenter"
    values = ["42"]
  }
}
```

Multiple values work as an OR type filter. In the shape example below, the resulting data source would contain both VM shapes Standard 1.1 and Standard 1.2:

```hcl
data "oci_core_shape" "t" {
  ...
  filter {
    name = "name"
    values = ["VM.Standard1.1", "VM.Standard1.2"]
  }
}
```

Multiple filters blocks can be composed to form AND type comparisons. The example below will return a data source containing running instances in the first AD of a region:

```hcl
data "oci_core_instances" "s" {
  ...
  filter {
    name = "availability_domain"
    values = ["\w*-AD-1"]
    regex = true
  }
  filter {
    name = "state"
    values = ["RUNNING"]
  }
}
```

As shown above, filters can also employ regular expressions. By setting regex = true, each item in the values list will be treated as a regular expression. Backslashes in strings for regular expression special characters need to be escaped with another slash, shown above as the first \ before \w in "\w*-AD-1".

**Note:**

Drilling into lists of structured objects is not currently supported. If these properties are targeted no results will be returned from the datasource.
Terraform offers a number of built-in functions that you can use in your configuration files. These functions allow you to modify strings, perform calculations against numeric values, manage collections, and much more.

For more information, see Functions.

For More Information

- Creating Terraform Modules
- Terraform Configurations
- Terraform Configuration Syntax

Specifying Versions

Terraform, the Oracle Cloud Infrastructure (OCI) Terraform provider, and Terraform modules you call in your configuration files all introduce changes or add new functionality from time to time. As these changes are made, new versions are released.

In order to ensure that your configurations are applied consistently to OCI resources, you can explicitly set the version of these components in Terraform configuration files.

Terraform CLI Version

If your Terraform configuration requires that you use a particular version of the Terraform CLI, you can specify that within the `terraform` block using the `required_version` setting. For example:

```terraform
terraform {
  required_version = ">= 0.12.16"
}
```

For more information, see Specifying a Required Terraform Version.

**Note:**

Resource Manager manages the Terraform version based on the stack version. Do not set a specific CLI version if you use Resource Manager.

Provider Version

You can control the version of the OCI Terraform provider that Terraform uses when interacting with OCI resources. This ability is especially helpful when your configuration relies on features introduced with a particular version of the provider or it has only been tested with a particular version of the provider.

You can use the `>=` or `=` operators to specify the version, depending on your use case.

For more information, see Specifying Provider Requirements.

Using Terraform v0.12 or earlier

Terraform v0.12 or earlier allowed you to specify `version` within the `provider` block. For example:

```terraform
provider "oci" {
  version          = ">= 3.27.0"
  region           = "${var.region}"
  ...
}
```

Using Terraform v0.13

Terraform v0.13 deprecated `version` within `provider` blocks. Instead, versions should be specified within a `required_providers` block. For example:

```terraform
terraform {
  required_providers {
    oci = {
```
Module Version

In addition to specifying the version of the Terraform CLI and the OCI Terraform provider, you can also specify the version of Terraform modules.

If a module has been upgraded to use a newer version of Terraform core, but you still use an earlier version of Terraform, you can specify a compatible version of the module. If your configurations have only been tested with a specific version of the module, you can specify that version to ensure compatibility.

Modules accept the version argument. For example:

```terraform
module "oke" {
  source  = "oracle-terraform-modules/oke/oci"
  version = "1.0.0"
  # insert required variables here
}
```

For more information, see Module Blocks.

Enabling FIPS Compatibility

You can use Terraform and a special FIPS compatible version of the Oracle Cloud Infrastructure (OCI) Terraform provider, as long as a few specific requirements and best practices are employed. This topic provides guidance on these requirements and practices.

**FIPS encryption**

To ensure the highest security standards, traffic from Terraform to OCI endpoints should transit over a TLS connection established with an HTTP client using FIPS certified encryption.

The standard OCI Terraform provider is implemented in Go. Go’s native cryptography implementations, while fully capable of establishing secure TLS connections with OCI endpoints, have not been FIPS certified.

For Terraform traffic to transit to OCI endpoints over FIPS-compliant connections, you must use a special version of the Terraform provider that leverages FIPS certified cryptography. This version of the OCI Terraform provider uses the FIPS 140-2 certified Oracle Cloud Infrastructure Cryptographic Library for Kubernetes instead of Go’s native cryptography implementation.

Installing the FIPS Compliant Terraform Provider

The FIPS compliant OCI Terraform provider is only available for Oracle Linux. You can install the provider using yum.

**Tip:**

Before installing the OCI Terraform provider, download and install Terraform from HashiCorp, or install Terraform using yum.

If any existing OCI Terraform provider packages are already installed on the Oracle Linux machine, remove them first:

```bash
yum remove terraform-provider-oci
```
To install the FIPS compatible OCI Terraform provider, run the following yum command from an Oracle Linux machine:

```
yum install terraform-provider-oci-fips
```

Operating Terraform in a Single Region

To ensure that traffic between Terraform and OCI services does not transit over public internet infrastructure, we recommend that you run Terraform and the OCI Terraform provider from a Compute instance that is hosted in the same region as the resources they create and manage.

Creating a Compute Instance

After Terraform and the OCI Terraform provider are installed on an Oracle Linux machine, you can use Terraform and the following sample Terraform configuration file to:

- Create a designated Compute instance you can use to provision additional infrastructure within the same region.
- Install Terraform and the latest FIPS compliant OCI Terraform provider on the new instance.
- Restrict communication with the instance to OCI endpoints and HTTPS using a service gateway.
- Enable instance principal authentication.

See Authoring Configurations on page 4277 for more information.

To create the compute instance:

1. Copy the `main.tf` file to your Oracle Linux machine.
2. Gather the information required to populate the Terraform configuration file's variables.
3. Refer to Oracle-Provided Images on page 629 to locate the Oracle Linux image OCID value for your region.
   Modify the `oel-image` value in the Terraform configuration file.
4. Initialize Terraform in the directory that contains the Terraform configuration file:

   ```
terraform init
   ```

5. Apply the Terraform configuration:

   ```
terraform plan
   terraform apply
   ```

**Important:**

The `instance-ip` output variable provides the IP address you will need to use to sign in to the new Compute instance.

```
main.tf

variable "tenancy_ocid" {
}
variable "user_ocid" {
}
variable "fingerprint" {
}
variable "private_key_path" {
}
variable "region" {
}
variable "compartment_ocid" {
```
variable "ssh_public_key" {
}

variable "ssh_private_key" {
}

locals {
    prefix = "terraform"
    oel-image = "<Oracle_Linux_image_OCID>"
    vm-shape = "VM.Standard2.1"

    user-data = <<EOF
#!/bin/bash -x
    echo "export TF_VAR_auth='InstancePrincipal'" >> ~/.bash_profile
    echo "export TF_VAR_region='${var.region}'" >> ~/.bash_profile
    yum install -y terraform terraform-provider-oci-fips
EOF

provider "oci" {
    tenancy_ocid = var.tenancy_ocid
    user_ocid = var.user_ocid
    fingerprint = var.fingerprint
    private_key_path = var.private_key_path
    region = var.region
}

resource "oci_core_vcn" "vcn1" {
    compartment_id = var.compartment_ocid
    display_name = "${local.prefix}Vcn"
    cidr_block = "10.0.0.0/16"
}

resource "oci_core_subnet" "subnet1" {
    compartment_id = var.compartment_ocid
    vcn_id = oci_core_vcn.vcn1.id
    cidr_block = "10.0.0.0/24"
    display_name = "${local.prefix}Subnet"
    security_list_ids = [oci_core_vcn.vcn1.default_security_list_id]
    route_table_id = oci_core_vcn.vcn1.default_route_table_id
    dhcp_options_id = oci_core_vcn.vcn1.default_dhcp_options_id
}

resource "oci_core_internet_gateway" "internet-gateway1" {
    compartment_id = var.compartment_ocid
    vcn_id = oci_core_vcn.vcn1.id
    display_name = "${local.prefix}InternetGateway"
}

resource "oci_core_default_route_table" "route-table1" {
    manage_default_resource_id = oci_core_vcn.vcn1.default_route_table_id
    display_name = "${local.prefix}RouteTable"

    route_rules {
        destination = "0.0.0.0/0"
        destination_type = "CIDR_BLOCK"
        network_entity_id = oci_core_internet_gateway.internet-gateway1.id
    }
}

data "oci_core_services" "service-gateway-services" {
filter {
    name = "name"
    values = ["All.* Services In Oracle Services Network"]
    regex = true
}

resource "oci_core_service_gateway" "service-gateway1" {
    compartment_id = var.compartment_ocid
    vcn_id = oci_core_vcn.vcn1.id
    display_name = "${local.prefix}ServiceGateway"

    services {
        service_id = data.oci_core_services.service-gateway-services.services[0]["id"]
    }
}

resource "oci_core_default_security_list" "security-list1" {
    manage_default_resource_id = oci_core_vcn.vcn1.default_security_list_id
    display_name = "${local.prefix}SecurityList"

    // inbound ssh traffic
    ingress_security_rules {
        protocol = "6" // tcp
        source = "0.0.0.0/0"
        stateless = false

        tcp_options {
            min = 22
            max = 22
        }
    }

    // outbound traffic to OCI services
    egress_security_rules {
        destination = data.oci_core_services.service-gateway-services.services[0]["cidr_block"]
        destination_type = "SERVICE_CIDR_BLOCK"
        protocol = "6"

        tcp_options {
            max = "443"
            min = "443"
        }
    }

    // outbound tcp traffic on all ports
    egress_security_rules {
        destination = "0.0.0.0/0"
        protocol = "6"
    }
}

data "oci_identity_compartment" "compartment1" {
    id = var.compartment_ocid
}

resource "oci_identity_dynamic_group" "dynamic-group1" {
    compartment_id = var.tenancy_ocid
    name = "${local.prefix}DynamicGroup"
    description = "Dynamic Group for executing Terraform with Instance Principal authentication"
```hcl
matching_rule = "ANY {instance.compartment.id = '${var.compartment_ocid}')" }

resource "oci_identity_policy" "instance-principal-policy1" {
    compartment_id = var.compartment_ocid
    name           = "${local.prefix}Policy"
    description    = "Policy to allow Instance Principal Terraform execution"
    statements     = ["ALLOW dynamic-group
                      ${oci_identity_dynamic_group.dynamic-group1.name} to manage all-resources
                      IN compartment ${data.oci_identity_compartment.compartment1.name}"
    }

data "oci_identity_availability_domain" "ad" {
    compartment_id = var.tenancy_ocid
    ad_number      = 1
}

resource "oci_core_instance" "instance1" {
    availability_domain = data.oci_identity_availability_domain.ad.name
    compartment_id      = var.compartment_ocid
    display_name        = "${local.prefix}Instance"
    shape               = local.vm-shape

    source_details {
        source_type = "image"
        source_id   = local.oel-image
    }

    metadata = {
        ssh_authorized_keys = var.ssh_public_key
        user_data           = base64encode(local.user-data)
        tenancy_ocid        = var.tenancy_ocid
    }

    create_vnic_details {
        subnet_id        = oci_core_subnet.subnet1.id
        assign_public_ip = true
    }
}

output "instance-ip" {
    value = [oci_core_instance.instance1.public_ip]
}
```

**Signing in to the Instance**

Use the following SSH command to access the instance:

```bash
$ ssh -i <private_key_path> <username>@<instance_ip_address>
```

*<private_key_path>* is the full path and name of the file that contains the private key associated with the instance you want to access.

*<username>* is the default username for the instance. For Oracle Linux images, the default username is *opc*.

*<instance_ip_address>* is the instance IP address that was the output of the Terraform commands.

**Installing and Configuring Terraform on the Instance**

1. Use yum to install Terraform and the FIPS compatible OCI Terraform provider on the instance:

    ```bash
    yum install -y terraform terraform-provider-oci-fips
    ```
2. Add an environment variable to enable instance principal authentication to the bash profile:

```bash
echo "export TF_VAR_auth='InstancePrincipal'" >> ${HOME}/.bash_profile
```

3. Add an environment variable to set the target region for Terraform:

```bash
echo "export TF_VAR_region='<your_region>'" >> ${HOME}/.bash_profile
```

4. Add an environment variable to disable interprocess traffic encryption between Terraform and the OCI Terraform provider:

```bash
echo "export TF_DISABLE_PLUGIN_TLS=1" >> ${HOME}/.bash_profile
```

5. Add an environment variable to prevent Terraform from accessing the HashiCorp Checkpoint service:

```bash
echo "export CHECKPOINT_DISABLE=1" >> ${HOME}/.bash_profile
```

6. Exit the instance:

```bash
exit
```

### Implementing Security Rules

Before using the new instance to run Terraform, you should update the security rules to prevent egress traffic to any third-party endpoints other than OCI services. You can do this by removing the following egress rule from the Terraform configuration file's `security-list1` resource and running `terraform apply` from the Oracle Linux machine:

```terraform
// outbound tcp traffic on all ports
// remove this rule or comment it out to prevent egress traffic to third-party endpoints
#egress_security_rules {
#  destination = "0.0.0.0/0"
#  protocol    = "6"
#}
```

**Tip:**
You can also use the OCI Console to update your security rules on the new instance.

### Running Terraform from the Instance

After creating the instance, installing and configuring Terraform on the instance, and updating the security rules, you can use Terraform to provision additional OCI infrastructure within the same region. Copy any additional Terraform configuration files to your instance, sign in to the instance, and run your Terraform commands like any other Terraform provider:

```bash
ssh -i <private_key_path> opc@<instance_ip_address>
terraform init
terraform apply
```

### Managing Boot Volumes

This guide details the following scenarios:

1. Preserving boot volume when performing Compute instance scaling
2. Boot volume troubleshooting and repair

To read more about boot volumes, see Boot Volumes

Preserving Boot Volumes
You may want to change Compute instance shape while using the same boot volume. When you terminate your instance, you can keep the associated boot volume and use it to launch a new instance using a different instance type or shape. This approach is useful for scenarios where instance shape cannot be changed while resizing instances.

To achieve this, you need to detach the boot volume from the running instance. This can be performed by either terminating the instance while preserving the boot volume or by stopping the instance and detaching the boot volume.

All terraform resources of type `oci_core_instance` have the parameter `preserve_boot_volume` set as true by default. This parameter ensures that upon termination of the instance, the attached boot volume is not terminated.

```terraform
resource "oci_core_instance" "TFInstance" {
  ...  
  state = "STOPPED"                  // set this state to stop the instance
  preserve_boot_volume = true
}

output "bootVolumeFromInstance" {
  value = [oci_core_instance.TFInstance.boot_volume_id]
}
```

Once the boot volume is detached, the OCID of the boot volume can be referred as the source of the new instance, as illustrated below:

```terraform
resource "oci_core_instance" "TFScaleInstance" {
  ...  
  source_details {
    source_type = "bootVolume"
    source_id   = "ocid1.bootvolume.oc1.phx.exampleuniqueID"
  }
}
```

Detaching Boot Volumes for Troubleshooting and Repair

If you think a boot volume issue is causing a compute instance problem, you can stop the instance and detach the boot volume. Then you can attach it to another instance as a data volume to troubleshoot it. After resolving the issue, you can then reattach it to the original instance or use it to launch a new instance.

Once the boot volume has been detached, the OCID of the boot volume can be referred as the block volume parameter for another instance.

```terraform
resource "oci_core_volume_attachment" "TFBlockAttach" {
  ...  
  attachment_type = "iscsi"
  compartment_id  = "ocid1.compartment.oc1..exampleuniqueID"
  instance_id     = "ocid1.instance.oc1.phx.exampleuniqueID"
  volume_id       = "ocid1.bootvolume.oc1.phx.exampleuniqueID"
}
```

Once you have resolved the issue, detach this volume from the second instance and attach it as a boot volume to the original instance.

```terraform
resource "oci_core_instance" "TFScaleInstance" {
  ...  
  source_details {
```
Migrating an Exadata DB System to the New Resource Model

The X8M generation of Exadata hardware introduces a new resource model that replaces the Exadata DB system. The new resource model uses new APIs to provision and manage its resources. The existing DB system APIs for Exadata will be deprecated by Oracle Cloud Infrastructure for all users following written notification and a transition period allowing you to switch to the new API and Console interfaces.

If you have existing Exadata DB systems in Oracle Cloud Infrastructure, you can use Terraform to switch them to the new resource model and APIs.

**Caution:**

Switching an Exadata DB system to the new resource model and APIs cannot be reversed. If you have automation for your system that utilizes the DB system APIs, you may need to update your applications prior to switching.

Switching to the new resource model:

- Does not impact the DB system's existing Exadata databases or client connections
- Does not change the underlying hardware or shape family of your Exadata Cloud Service instance
- Will not affect bare metal and virtual DB systems

After converting your DB system, you will have two new resources in place of the DB system resource: a cloud Exadata infrastructure resource, and a cloud VM cluster resource.

What to expect after switching:

- Your new cloud Exadata infrastructure resource and cloud VM cluster are created in the same compartment as the DB system they replace
- Your new cloud Exadata infrastructure resource and cloud VM cluster use the same networking configuration as the DB system they replace
- After the switch, you cannot perform operations on the old Exadata DB system resource
- Switching is permanent, and the change cannot be undone
- X6, X7, X8 and Exadata base systems retain their fixed shapes after the switch, and cannot be expanded

See [Exadata Cloud Service](#) on page 1221 for more information.

To Migrate an Exadata DB System

These migration steps use the following example, which shows an existing Exadata Cloud Service instance using the old DB system resource model:

```
resource "oci_database_db_system" "test_db_system" {
  availability_domain = data.oci_identity_availability_domain.ad.name
  compartment_id      = var.compartment_ocid
  cpu_core_count      = var.cpu_core_count
  database_edition    = var.db_edition
  time_zone           = var.time_zone

  db_home {
    database {
      admin_password = var.db_admin_password
      db_name        = "TFdb1Exa"
      character_set  = var.character_set
      ncharacter_set = var.n_character_set
    }
  }
}
```
db_workload = var.db_workload
pdb_name = var.pdb_name

db_backup_config {
    auto_backup_enabled = false
}
}
db_version = var.db_version
display_name = "MyTFDBHome1Exa"

maintenance_window_details {
    preference = "CUSTOM_PREFERENCE"

days_of_week {
    name = "MONDAY"
}

hours_of_day       = ["4"]
lead_time_in_weeks = 2

months {
    name = "APRIL"
}

weeks_of_month = ["2"]
}
disk_redundancy = var.db_disk_redundancy
shape = var.db_system_shape
subnet_id = oci_core_subnet.subnet.id
backup_subnet_id = oci_core_subnet.subnet_backup.id
ssh_public_keys = [var.ssh_public_key]
display_name = var.db_system_display_name
sparse_diskgroup = var.sparse_diskgroup
hostname = var.hostname
data_storage_percentage = var.data_storage_percentage

#data_storage_size_in_gb = var.data_storage_size_in_gb
license_model = var.license_model
node_count = data.oci_database_db_system_shapes.test_db_system_shapes[0]["minimum_node_count"]
backup_network_nsg_ids = [oci_core_network_security_group.test_network_security_group.id]
nsg_ids = [oci_core_network_security_group.test_network_security_group_backup.id, oci_core_network_security_group.test_network_security_group.id]
}

To migrate the system to the new resource model, first create the oci_database_migration resource:

// This is 1 time action to migrate test_db_system into db ExaCS
// and the test_db_system will become 'Migrated'
resource "oci_database_migration" "test_migration" {
    #Required
db_system_id = "${oci_database_db_system.test_db_system.id}"
Provisioning the `oci_database_migration` resource creates two new resources: `oci_database_cloud_exadata_infrastructure` and `oci_database_cloud_vm_cluster`.

You can get OCIDs of these two resources from the `oci_database_migration` resource:

```hcl
output "cloud_exadata_infrastructure_id" {
  value =
  oci_database_migration.test_migration.cloud_exadata_infrastructure_id
}
output "cloud_vm_cluster_id" {
  value = oci_database_migration.test_migration.cloud_vm_cluster_id
}
```

Create a Terraform configuration for the two new resources:

```hcl
resource "oci_database_cloud_exadata_infrastructure" "test_cloud_exadata_infrastructure"{}
resource "oci_database_cloud_vm_cluster" "test_cloud_vm_cluster" {}
```

Then run the Terraform import command:

```bash
terraform import
oci_database_cloud_exadata_infrastructure.test_cloud_exadata_infrastructure <cloud_exadata_infrastructure_id>
terraform import
oci_database_cloud_vm_cluster.test_cloud_vm_cluster <cloud_vm_cluster_id>
```

Terraform now manages the two new resources. After switching to the new Exadata resource model, remove the old `oci_database_db_system` config.

**Tip:**

After the migration, you can use Resource Discovery on page 4304 to create a full configuration and state file for importing these two new resources.

**Targeting Multiple Regions**

You can use a single Terraform configuration to create Oracle Cloud Infrastructure (OCI) resources in multiple regions.

**Create a Provider for Each Region**

A Terraform configuration may have only a single OCI Terraform provider block, but to apply configurations to multiple regions, you need to create multiple provider blocks.

A typical OCI Terraform provider block might look like the following:

```hcl
provider "oci" {
  region = var.region
  tenancy_ocid = var.tenancy_ocid
  user_ocid = var.user_ocid
  fingerprint = var.fingerprint
  private_key_path = var.private_key_path
}
```

**Tip:**

All parameters should be set using variables.

If you want to use more than one region within a single Terraform config, multiple providers are required. Each provider must be given an alias. For example:

```hcl
provider "oci" {
```
When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region, which is your home region. The home region has special properties. For example, IAM resources can only be created in your home region. For that reason, you should designate that region with an appropriate alias, like `home`. Use simple aliases for other regions so that users can easily map configurations to the regions that they want (for example, `region2`).

Note:
Specific regions (us-phoenix-1, us-ashburn-1, and so on) are not hardcoded into either the `region` or `alias` fields.

Provision a Resource
To provision a resource in a region, specify the aliased provider name in the resource.

For example:

```terraform
resource "oci_core_instance" "test_instance" {
  provider = oci.home
  ...
}
```

Modules and Multiple Regions
Typically, a module should use only a single region. If more regions are needed, you should use separate modules.

If the config contains multiple providers, the module should specify the provider to use by using the following format:

```terraform
module "compartments" {
  source = "./compartments"
  providers = {
    oci = "oci.home"
  }
}
```

Upgrading Configurations to Terraform v0.12
With the release of Terraform v0.12, Oracle Cloud Infrastructure Terraform providers need to be upgraded and some existing configurations may need to be updated as well.

Upgrading the Terraform Provider
Oracle Cloud Infrastructure (OCI) Terraform provider versions 3.26.0 and below are not compatible with Terraform v0.12. OCI Terraform provider version 3.27.0 is the earliest version that supports Terraform v0.12.

Note:
All OCI Terraform provider versions remain compatible with Terraform v0.11 and v0.10.
The simplest way to begin using the latest v0.12-compatible provider from the HashiCorp provider registry is to place an explicit version requirement in your provider configuration block, as shown here:

```hcl
provider "oci" {
  version          = ">= 3.27.0"
  region           = "${var.region}"
  tenancy_ocid     = "${var.tenancy_ocid}"
  user_ocid        = "${var.user_ocid}"
  fingerprint      = "${var.fingerprint}"
  private_key_path = "${var.private_key_path}"
}
```

For guidance using additional version configuration options, see Provider Versions.

Upgrading Terraform Configurations

Some users may find that no changes are needed to run existing Terraform configurations with v0.12.

For configurations that do need to be upgraded, see Upgrading Terraform configuration.

**Upgrading configurations while preserving v0.11 compatibility**

As recommended in Upgrading Terraform configuration, the simplest way to upgrade your configurations is to use the `terraform 0.12upgrade` command. Using the `terraform 0.12upgrade` command to upgrade your configurations, however, renders them incompatible with Terraform v0.11 and earlier.

**Caution:**

Prior to making configuration changes, it is strongly recommended that configuration and state files are backed up using version control or another preferred mechanism.

It may be possible to manually upgrade configurations to work with v0.12 while preserving compatibility with v0.11. Not all possible configurations can be made compatible with both v0.11 and v0.12. This method should only be used as a best-effort to preserve compatibility with v0.11.

The following cases detail where it is possible to convert existing v0.11 usage to be compatible with both v0.11 and v0.12.

**Attributes vs. Blocks**

In v0.11, it was possible to treat attributes and nested blocks interchangeably. Note how the attribute `metadata` and the nested block `source_details` are both assigned using only braces.

```hcl
// v0.11 compatible representation
resource "oci_core_instance" "my_instance" {
  metadata {
    ssh_authorized_keys = "${var.ssh_public_key}"  
  }

  source_details {
    source_type = "image"
    source_id   = "${var.instance_image_ocid[var.region]}"
    kms_key_id  = "${oci_kms_key.test_key.id}"
  }
}
```

In v0.12, attributes need to be assigned using the = operator while blocks need to be assigned using only braces. Note how the attribute `metadata` is now assigned with =. This usage is still compatible with v0.11.

```hcl
// v0.12 and v0.11 compatible representation
resource "oci_core_instance" "my_instance" {

```
metadata = {
    ssh_authorized_keys = "${var.ssh_public_key}"
}

source_details {
    source_type = "image"
    source_id = "${var.instance_image_ocid[var.region]}"
    kms_key_id = "${oci_kms_key.test_key.id}"
}

### Nested blocks with multiple elements

In v0.11, it was possible to wrap lists of nested blocks inside `[]` like this example.

```hcl
// v0.11 compatible representation
resource "oci_core_virtual_circuit" "virtual_circuit_public" {
    public_prefixes = [
        {
            cidr_block = "${var.virtual_circuit_public_prefixes_cidr_block}" 
        },
        {
            cidr_block = "${var.virtual_circuit_public_prefixes_cidr_block2}" 
        },
        {
            cidr_block = "${var.virtual_circuit_public_prefixes_cidr_block3}" 
        },
    ]
}
```

In v0.12, it is required to specify each nested block individually without wrapping it in `[]`. This usage is still compatible with v0.11.

```hcl
// v0.11 compatible representation
resource "oci_core_virtual_circuit" "virtual_circuit_public" {
    public_prefixes {
        cidr_block = "${var.virtual_circuit_public_prefixes_cidr_block}" 
    }
    public_prefixes {
        cidr_block = "${var.virtual_circuit_public_prefixes_cidr_block2}" 
    }
    public_prefixes {
        cidr_block = "${var.virtual_circuit_public_prefixes_cidr_block3}" 
    }
}
```

### Quotes around attribute names

In v0.11, it was possible to put quotation marks " around attribute names. Note how the `min` and `max` attributes have quotation marks around them.

```hcl
// v0.11 compatible representation
resource "oci_core_security_list" "bastion" {
    egress_security_rules {
        destination = "${var.vcn_cidr}"
        protocol   = "${local.tcp_protocol}" 
        tcp_options {
```
In v0.12, quotation marks " around attribute names are no longer allowed.

```hcl
resource "oci_core_security_list" "bastion" {
  egress_security_rules {
    destination = "${var.vcn_cidr}"
    protocol    = "${local.tcp_protocol}"
    tcp_options {
      min = 22
      max = 22
    }
  }
  ...
}
```

**Variable names starting with non-alphabetical characters**

In v0.11, it was possible to specify variable names that begin with non-alphabetical characters.

```hcl
variable "2TB" {
  default = "2048"
}
```

In v0.12, variable names must begin with alphabetical characters.

```hcl
variable "Size2TB" {
  default = "2048"
}
```

**Computing list index values**

In v0.11, division operations often resulted in integer values that could be used as a valid index in a list.

```hcl
instance_id     = "${oci_core_instance.TFInstance.*.id[count.index / var.NumParavirtualizedVolumesPerInstance]}"
```

In v0.12, division operations can result in floating point values that may no longer be valid. To avoid this situation, use the `floor` interpolation to convert floating point values to an index.

```hcl
instance_id     = "${oci_core_instance.TFInstance.*.id[floor(count.index / var.NumParavirtualizedVolumesPerInstance)]}"
```

**Using Object Storage for State Files**

You can store Terraform state files in Oracle Cloud Infrastructure (OCI) Object Storage. Doing so requires that you configure a backend using one of the Terraform backend types.
Terraform supports various backend types to allow flexibility in how state files are loaded into Terraform. (For more information, see **Terraform Backend Types**.) For our purposes, we address two of these approaches:

- Using an HTTP remote state backend
- Using an S3-compatible remote state backend

**Using an HTTP Backend**

Using the **HTTP backend type** allows you to store state using a simple REST client. With the HTTP backend type, you can easily fetch, update, and purge state using the **HTTP GET**, **POST**, and **DELETE** methods.

To configure the HTTP backend to store your OCI Terraform state files, do the following:

**Create a Pre-Authenticated Request**

Creating a pre-authenticated request in Oracle Object Storage enables accessing a bucket or object in the OCI without needing to provide credentials. To do so, you must create a pre-authenticated request that has read/write permissions to the object store where you intend to save the Terraform state file. You can do so in any of three ways: by using the Console UI, by using the command line interface (CLI), or by using the REST APIs.

**Note:**

A state file must exist in the bucket before you create the pre-authenticated request. This file can be an existing state file, or an empty file for the initial state.

For guidance, see Using Pre-Authenticated Requests on page 3482.

**Upload Existing State**

If you have an existing state file, you can upload it using Curl to make an **HTTP PUT** request to the object store URL, as shown here:

```bash
curl -X PUT -H "Content-Type: text/plain" --data-binary "@path/to/local/tfstate" http://<prefix>/<my-access-uri>
```

**Configure HTTP as a Terraform Backend**

The **HTTP backend type** stores state using a simple REST client and allows you to easily fetch, update, and purge state using the **HTTP GET**, **POST**, and **DELETE** methods.

The access URI for addressing OCI Terraform configurations must be of the form: `https://objectstorage.us-phoenix-1.oraclecloud.com/my-access-uri` (where region and access URI are specific to you).

For more example configuration and state files that reference code, and a summary of configuration variables, see **Standard Backends: HTTP**.

Following is an example Terraform configuration. The region in the URL can be something other than the Phoenix region.

```terraform
terraform {
    backend "http" {
        address = "https://objectstorage.us-phoenix-1.oraclecloud.com/<my-access-uri>"
        update_method = "PUT"
    }
}
```
Reinitialize Terraform

Finally, you must reinitialize Terraform and then run the `apply` command:

```bash
terraform init
terraform apply
```

After completing these steps, you are able to use Oracle Cloud Infrastructure as the backend for storing Terraform state files.

Using an S3-Compatible Backend

Configuring the S3-compatible backend requires that the account be enabled with S3 authentication keys, which are set on a per-user basis.

1. In the Console, open the navigation menu, then, under Governance and Administration, navigate to Identity, then Users. Under User Details, click Customer Secret Key. For guidance, see Working with Customer Secret Keys on page 2457.
2. Set the location for the credentials file. The default location is `~/.aws/credentials`. You can set an alternate location by using the S3 backend `shared_credentials_file` option.

   **Caution:** Never set the `access_key` and the `secret_key` attributes in the same Terraform backend configuration, since this creates a security risk.

3. Configure the `[default]` entry in the credentials file with the appropriate object storage credentials. The file can contain any number of credential profiles. If you provide a different profile name, you must also update the backend `profile` option in your Terraform configuration file.

   Following is an example of Object Storage credentials:

   ```
   [default]
   aws_access_key_id=ocid1.credential.oc1..exampleuniqueID
   aws_secret_access_key=mSTdaWhlbWj3ty4JZXl1m0NUZV52x1ImWjayJLJ6OH9A=
   ```

   Where `aws_access_key_id` and `aws_secret_access_key` are user-specific values provided from the Console. The key values provided in the example are not valid and provided as examples only.

4. Set the object storage endpoint value in the following format:

   ```
   https://<namespace>.compat.objectstorage.<region>.oraclecloud.com
   ```

5. Reinitialize Terraform and then run the `apply` command:

   ```bash
   terraform init
   terraform apply
   ```

Following is a full example of an Object Storage backend configuration:

```bash
terraform {
  backend "s3" {
    bucket = "terraform-states"
    key = "networking/terraform.tfstate"
    region = "us-phoenix-1"
    endpoint = "https://acme.compat.objectstorage.us-phoenix-1.oraclecloud.com"
    shared_credentials_file = "../terraform-states_bucket_credentials"
    skip_region_validation = true
    skip_credentials_validation = true
    skip_metadata_api_check = true
    force_path_style = true
  }
}
```
Caution:

If the same bucket is used across multiple Terraform configurations, the key must be unique to avoid overwriting the state file. This example uses a single bucket (terraform-states) to store all Terraform state files, but uses a unique prefix for the object name based on the resource (networking).

Once you have configured the backend, you must run `terraform init` to finish the setup. If you already have an existing `terraform.tfstate` file, then Terraform prompts you to confirm that the current state file is the one to upload to the remote state.

Note:

The S3 backend configuration can also be used for the `terraform_remote_state` data source to enable sharing state across Terraform projects.

For More Information

- Using Pre-Authenticated Requests on page 3482
- State Files
- Terraform Backend Types

Best Practices

This section documents some best practices that you can apply when you use the Oracle Cloud Infrastructure (OCI) Terraform provider to manage OCI resources.

See the following topics for more information:

- Managing Default VCN Resources on page 4300
- Referencing Availability Domains on page 4301
- Referencing Images on page 4303
- Storing Sensitive Data on page 4303
- Tagging Resources on page 4303

Managing Default VCN Resources

When you create an `oci_core_vcn` resource, it will also create the following associated resources by default.

- `oci_core_security_list`
- `oci_core_dhcp_options`
- `oci_core_route_table`

These default resources will be implicitly created even if they are not specified in the Terraform configuration. Their OCIDs are returned by the following attributes under the `oci_core_vcn` resource:

- `default_security_list_id`
- `default_dhcp_options_id`
- `default_route_table_id`

Default resources must be configured in Terraform using a separate resource type. Here are the mappings between the resource and the new resource type to use for configuring default resources:

- `oci_core_security_list` => `oci_core_default_security_list`
- `oci_core_dhcp_options` => `oci_core_default_dhcp_options`
- `oci_core_route_table` => `oci_core_default_route_table`

Default resources types are configured in the same way as their non-default counterparts. The only difference is specifying the ID of the default resource using the `manage_default_resource_id` argument.

Consequently, the compartment_id and vcn_id are no longer necessary for default resources.
The following example modifies a VCN's default DHCP options:

```hcl
resource "oci_core_vcn" "vcn1" {
  cidr_block = "10.0.0.0/16"
  dns_label = "vcn1"
  compartment_id = var.compartment_ocid
  display_name = "vcn1"
}

resource "oci_core_default_dhcp_options" "default-dhcp-options" {
  manage_default_resource_id = oci_core_vcn.vcn1.default_dhcp_options_id

  // required
  options {
    type = "DomainNameServer"
    server_type = "VcnLocalPlusInternet"
  }

  // optional
  options {
    type = "SearchDomain"
    search_domain_names = [ "abc.com" ]
  }
}
```

Limitations

Default resources can only be removed when the associated `oci_core_vcn` resource is removed. When attempting a targeted removal of a default resource, the resource will be removed from the Terraform state file but the resource may still exist in OCI with empty settings.

Examples of targeted removal include:

- Removing a default resource from a Terraform configuration that was previously applied
- Running a `terraform destroy -target=<default resource>` command
- Changing the `manage_default_resource_id` for a default resource that was previously applied

Referencing Availability Domains

With respect to availability domains, we caution against a common pattern, as shown here:

```hcl```
```hcl
// Get all availability domains for the region
data "oci_identity_availability_domains" "ads" {
  compartment_id = "${var.tenancy_ocid}"
}

// Then either use it to get a single AD name based on the index:
resource "oci_core_instance" "nat" {
  availability_domain = "${lookup(data.oci_identity_availability_domains.ads.availability_domains["nat_instance_ad"], "name")}
  ...
}

// Or iterate through all the ADs:
resource "oci_core_subnet" "nat" {
  count = "${length(data.oci_identity_availability_domains.ads.availability_domains)}"
  availability_domain = "${lookup(data.oci_identity_availability_domains.ads.availability_domains[count.index], "name")}"" ..
    ohbflh rawsdf 1329
```
The recommendation, then, is to explicitly list the availability domain names for the regions in your configuration. To do so, use a variable that you have defined as follows:

```hcl
variable "ad_list" {
  type = "list"
}
```

You can then use the variable as shown here:

```hcl```
// Index:
resource "oci_core_instance" "nat" {
  availability_domain = "${var.ad_list[var.nat_instance_ad_index]}"
} ...

// Or iterate through all the ADs:
resource "oci_core_subnet" "nat" {
  count = "${length(var.ad_list)}"
  availability_domain = "${var.ad_list[count.index]}"
} ...
```

You can then set the `ad_list` variable directly by using the availability domain names for your tenant and region, as shown here:

```hcl```
variable "ad_list" {
  type = "list"
  default = ["kIdk:PHX-AD-1","kIdk:PHX-AD-2","kIdk:PHX-AD-3"]
}
```

The advantage of using this method is that it gives you control over your availability domain usage and prevents unexpected changes over time. However, this approach is problematic when configurations are shared between tenancies and regions, since availability domain names are tenancy- and region-specific.

A convenient alternative is to instead set the `ad_list` value by using the `oci_identity_availability_domains` data source. You should do this in the configuration, then pass them into the modules. This effectively centralizes the list of ADs, making it easy to switch to an explicit list later, should that become necessary: Note that the modules themselves should not use the `oci_identity_availability_domains` data source.

```hcl```
data "oci_identity_availability_domains" "ad" {
  compartment_id = "${var.tenancy_ocid}"
}
data "template_file" "ad_names" {
  count = "${length(data.oci_identity_availability_domains.ad.availability_domains)}"
  template = "${lookup(data.oci_identity_availability_domains.ad.availability_domains[count.index], "name")}"
}
module "ssm_network" {
  ad_list = "${data.template_file.ad_names.*.rendered}" ...
}
```

Regions with a Single Availability Domain

Some Oracle Cloud Infrastructure regions have a single availability domain. When writing configurations that use plural data sources, like `oci_identity_availability_domains`, ensure that you account for a single domain if required by your region.
The following example uses the `oci_identity_availability_domains` data source when listing fault domains in a single-availability domain region. The `availability_domains` index must be 0. Any other index value is invalid in this region:

```terraform
data "oci_identity_availability_domains" "AvailabilityDomains" {
  compartment_id = var.tenancy_ocid
}

data "oci_identity_fault_domains" "FaultDomains" {
  availability_domain = 
  data.oci_identity_availability_domains.AvailabilityDomains.availability_domains[0] {"name"}
  compartment_id = `${var.compartment_ocid}`
}
```

Referencing Images

When launching Compute instances, your Terraform configuration should use the same image every time you run a Terraform apply job.

To ensure this, specify the image OCID directly, rather than locating it using the `oci_core_image` data source. This is because the `oci_core_image` data source calls into the `ListImages` API, whose return values can change over time because over time images are added and older ones deleted. For a list of Oracle-provided images and their OCIDs, see Oracle-Provided Images on page 629. For more information, see Results of `oci_core_images` will change over time for Oracle-provided images.

We recommend the following pattern for specifying an image for a given region:

```terraform
variable "image_id" {
  type = "map"
  default = {
    // See https://docs.cloud.oracle.com/iaas/images/
    // Oracle-provided image "Oracle-Linux-7.4-2018.02.21-1"
    us-phoenix-1 = "ocid1.image.oc1.phx..<unique_ID>
    us-ashburn-1 = "ocid1.image.oc1.iad..<unique_ID>
    eu-frankfurt-1 = "ocid1.image.oc1.eu-frankfurt-1..<unique_ID>
    uk-london-1 = "ocid1.image.oc1.uk-london-1..<unique_ID>
  }
}
```

A Compute instance can use this in the following way:

```terraform
resource "oci_core_instance" "TFInstance" {
  image = `${var.image_id[var.region]}`
  ...
}
```

Storing Sensitive Data

**Caution:**

Terraform configuration files and state files may contain sensitive data.

When configuring your Oracle Cloud Infrastructure (OCI) Terraform provider, you should use variables to define your provider instead of including sensitive information within the file.

Terraform state files contain all resource attributes that are specified as part of configuration files. If you manage any sensitive data with Terraform, like database or user passwords or instance private keys, you should treat the state itself as sensitive data. Please refer to Sensitive Data in State for more details.

Tagging Resources

When you have many resources (for example, instances, VCNs, load balancers, and block volumes) across multiple compartments in your tenancy, it can become difficult to track resources used for specific purposes, or to aggregate...
them, report on them, or take bulk actions on them. Tagging allows you to define keys and values and associate them with resources. You can then use the tags to help you organize and list resources based on your business needs. See Tagging Overview to familiarize yourself with concept of tagging and features available.

Managing Tags and Tag Namespaces

- See tag_namespaces for guidance on managing lifecycle of tag namespaces.
- See tags for guidance on managing lifecycle of tags.

How To Manage Tags on OCI Resources

- **Freeform tags**: Freeform tags are simple key/value map.
- **Defined tags**: Defined tags provide a key/value map and are organized by combining the tag namespaces with tag keys using dot notation. For example, a tag namespace called HumanResources could have a key named CostCenter. You then associate the namespace and key HumanResource.CostCenter and then assign the desired tag, as shown in the following example.

Propagation of tagging on resources

If your Terraform configuration has a primary resource (e.g. compute instance) with a nested secondary resource (e.g. VNIC for the compute instance) where both these resources support freeform tags or defined tags, OCI Services will propagate all the primary resource's freeform tags and defined tags to secondary resource. This could cause a drift in the Terraform state resulting in a diff after apply. To avoid this, explicitly add all the primary resource's freeform tags and defined tags on the secondary resources as part of the configuration. The same behavior can be seen while using the Tag Default or Required Tags feature. This can also be avoided by applying the Tag Default or Required Tags on all resources (primary and secondary if any) in the tenancy where Tag Default or Required Tags exist.

Resource Discovery

You can use the Oracle Cloud Infrastructure (OCI) Terraform provider's resource discovery feature to search for deployed resources in your compartment and export them to Terraform configuration and state files.

Resource discovery simplifies the move from manually managed infrastructure to Terraform-managed infrastructure. With a single command, you can generate a file that captures your existing compartment's baseline configuration and state.

### Important:

Resource discovery is not a migration tool. When cloning or migrating resources, configurations generated by resource discovery are a starting point. They may require changes.

Common uses cases for your new Terraform configuration and state files include:

- Duplication or rebuild of your existing infrastructure architecture in a new tenancy or region.
- Detection of state drift. Run reports to see if the state of your Terraform-managed resources has changed and differs from your base configuration.

### Note:

Terraform resource discovery is available with OCI Terraform provider version 3.50 and above.

Supported Services

Refer to Supported Services on page 4309 for the list of services the OCI Terraform provider's resource discovery feature supports. You can also see the list of supported services by running this command:

```
terraform-provider-oci -command=list_export_services
```
Developer Tools

Note:
Terraform resource discovery may not be available for all services that the OCI Terraform provider supports.

Supported Resources
Each supported service has one or more discoverable resources. You can see the list of supported resources by running this command:

```
terraform-provider-oci -command=list_export_resources
```

Using Resource Discovery
The Oracle Cloud Infrastructure (OCI) Terraform provider's resource discovery feature uses HashiCorp's terraform-exec to import the discovered OCI resources into Terraform configuration and state files.

Prerequisites
Terraform-exec requires the Terraform CLI to be present on your system. See Download and Install Terraform on page 103 for installation details.

Note:
If you are using Terraform version v0.11, this tool cannot generate a state file. Only configurations are supported in v0.11. By default the configurations are generated in v0.12.

If you use v0.13.* of the Terraform CLI, make sure that the version is compatible with v0.12 syntax.

Additionally, you must have the OCI Terraform provider downloaded and installed. See Download and Install the Provider on page 103 for download instructions.

Adding the Tools to Your Path
To run the OCI Terraform provider as an executable and use resource discovery, you can:

- Add `terraform-provider-oci` to your system path.
- Run the provider from the directory where it is located.
- Specify the full path to the provider when you run resource discovery commands.

Because resource discovery commands use terraform-exec to call Terraform on your behalf, your system must specify the location of the Terraform CLI using either of the following methods:

- Provide the full path including name for the Terraform CLI using the `terraform_bin_path` environment variable. See Environment Variables for more information on setting variables.
- Add the Terraform CLI to your system path.

Authentication
To discover resources in your compartment, the OCI Terraform provider needs authentication information about the user, tenancy, and region with which to discover the resources. It is recommended that you specify a user that has access to inspect and read the resources to discover.

You can use API Key Authentication and Environment Variables or Instance Principal Authorization to provide the required information.

Exporting Resources
Once you have specified the location of the Terraform CLI and authentication settings, either of the following commands can be used to export a compartment’s resources:

- `terraform-provider-oci -command=export -compartment_name=<compartment_name> -output_path=<output_path>`
- `terraform-provider-oci -command=export -compartment_id=<compartment_OCID> -output_path=<output_path>`

These commands discover all supported resources within the compartment and generate Terraform configuration files in the given `output_path`. The generated `.tf` files contain the Terraform configuration with the resources that the command has discovered.

**Note:**
Export of compartment resources supports only the target compartment. Resources in child compartments are not discovered.

**Note:**
The `compartment_id` parameter is required if using Instance Principal Authorization.

### Parameters

You can use the following parameters to control the behavior of the resource discovery tool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
</table>
| `command`                | The command to run. Supported commands include:  
|                          | • `export` - discovers OCI resources within your compartment and generates Terraform configuration files for them  
|                          | • `list_export_resources` - lists the Terraform OCI resource types that are discovered by the export command  
|                          | • `list_export_services` - lists the allowed values for services arguments along with scope in JSON format  
| `compartment_id`         | The OCID of the compartment to export. If `compartment_id` or `compartment_name` is not specified, the root compartment is used.  
| `compartment_name`       | The name of a compartment to export. If `compartment_id` or `compartment_name` is not specified, the root compartment is used.  
| `generate_state`         | Provide this flag to import the discovered resources into a state file in addition to the Terraform configuration files.  
| `ids`                    | A comma-separated list of resource IDs to export. The ID could either be an OCID or a Terraform import ID. By default, all resources are exported.  
| `list_export_services_path` | The full path, including the filename, to use as the output for list of supported services, in JSON format. |
### Parameter Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>output_path</strong></td>
<td>The path to output the generated configurations and state files of the exported compartment.</td>
</tr>
<tr>
<td><strong>parallelism</strong></td>
<td>The number of threads that will be used to discover resources in parallel. The default value is 1.</td>
</tr>
<tr>
<td><strong>services</strong></td>
<td>A comma-separated list of service resources to export. If not specified, all resources within the given compartment (excluding IAM resources) are exported.</td>
</tr>
<tr>
<td><strong>tf_version</strong></td>
<td>The version of Terraform syntax to use when generating configuration files. The default is v0.12. The allowed values are:</td>
</tr>
<tr>
<td></td>
<td>• 0.11</td>
</tr>
<tr>
<td></td>
<td>• 0.12</td>
</tr>
<tr>
<td></td>
<td>If you specify 0.11 as the syntax version, you should use v0.11 of the Terraform CLI to discover resources.</td>
</tr>
<tr>
<td></td>
<td>If you use Terraform CLI v0.13 and above to discover resources, make sure the version is compatible with v0.12 syntax.</td>
</tr>
<tr>
<td></td>
<td>State files are generated in Terraform syntax matching the version of the Terraform CLI used to discover resources. The tf_version parameter does not apply to state files.</td>
</tr>
</tbody>
</table>

### Exit Status

If there is any error related to the OCI APIs or service unavailability while discovering resources, the tool moves on to find next resource. All of the errors encountered are displayed after the discovery is complete.

- **Exit code 0** - Success.
- **Exit code 1** - Failure due to errors such as incorrect environment variables, arguments or configuration.
- **Exit code 2** - Partial success. Resource discovery was not able to find all the resources because of service failures.

### Exporting Identity Resources

Some resources, such as identity resources, exist only at the tenancy level and cannot be discovered within a specific compartment. To discover such resources, use the following command, which omits any compartment parameter:

```
terraform-provider-oci -command=export -output_path=<output_path> -services=identity
```

**Note:**

When exporting identity resources, the **compartment_id** value, if provided, is ignored.

### Exporting Resources to Another Compartment

Once you have reviewed the generated Terraform configuration files and made any necessary changes, the configuration can be used with Terraform. One such use case is the re-deploying of those resources in a new compartment or tenancy, using Terraform.
To do so, specify the following environment variables:

```bash
export TF_VAR_tenancy_ocid=<target_tenancy OCID>
export TF_VAR_compartment_ocid=<target_compartment OCID>
```

Then run the following command:

```bash
terraform apply
```

Generating a Terraform State File

It is also possible to generate a Terraform state file to manage the discovered resources. To do so, run the following command, which includes the `-generate_state` flag:

```bash
terraform-provider-oci -command=export -compartment_id=<compartment OCID> -output_path=<output_path> -generate_state
```

The results of this command are both the `.tf` files representing the Terraform configuration and a `terraform.tfstate` file representing the state. See `State` for more information.

**Caution:**
The state file contains all resource attributes that are specified as part of configuration files. If you manage any sensitive data with Terraform, treat the state file itself as sensitive data. See `Storing Sensitive Data` on page 4303 for more information.

**Note:**
The Terraform state file generated by this command is only compatible with Terraform v0.12.4 and above.

Output File Contents

The Oracle Cloud Infrastructure (OCI) Terraform provider's resource discovery `export` command discovers resources that are in an active or usable state. Resources that have been terminated or otherwise made inactive are generally excluded from the generated configuration.

By default, the Terraform names of the discovered resources share the same name as the display name for that resource, if one exists.

The attributes of the resources are populated with the values that are returned by the OCI services.

In some cases, a required or optional attribute may not be discoverable from the OCI services and may be omitted from the generated Terraform configuration. This may be expected behavior from the service, which may prevent discovery of certain sensitive attributes or secrets. In such cases, a placeholder value will be set along with a comment like this:

```bash
admin_password = "" #Required attribute not found in discovery, placeholder value set to avoid plan failure
```

The missing required attributes are also added to lifecycle `ignore_changes`. This is done to avoid Terraform plan failure when moving manually-managed infrastructure to Terraform-managed infrastructure. Any changes made to such fields will not reflect in Terraform plan. If you want to update these fields, remove them from `ignore_changes`.

Resources that are dependent on availability domains will be generated under `availability_domain.tf` file. These include:

- `oci_core_boot_volume`
- `oci_file_storage_file_system`
- `oci_file_storage_mount_target`
This section provides additional information on how to use the Oracle Cloud Infrastructure (OCI) Terraform provider with the services it supports, including some best practices for those services.

Full Reference Documentation

The full reference of the OCI Terraform provider's supported resources and data sources contains usage, argument, and attribute details. The resources are grouped by service within the reference.

Supported Services

The following table lists the services supported by the OCI Terraform provider and the services supported by the resource discovery feature. This list also includes the values accepted by resource discovery's services parameter.

<table>
<thead>
<tr>
<th>Supported OCI service</th>
<th>Resource discovery support</th>
<th>Resource discovery services parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics Cloud</td>
<td>Yes</td>
<td>analytics</td>
</tr>
<tr>
<td>API Gateway</td>
<td>Yes</td>
<td>apigateway</td>
</tr>
<tr>
<td>Audit</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Autoscaling (Compute)</td>
<td>Yes</td>
<td>auto_scaling</td>
</tr>
<tr>
<td>Big Data</td>
<td>Yes</td>
<td>bds</td>
</tr>
<tr>
<td>Blockchain Platform</td>
<td>Yes</td>
<td>blockchain</td>
</tr>
<tr>
<td>Budgets</td>
<td>Yes</td>
<td>budget</td>
</tr>
<tr>
<td>Cloud Guard</td>
<td>Yes</td>
<td>cloud_guard</td>
</tr>
<tr>
<td>Container Engine for Kubernetes</td>
<td>Yes</td>
<td>containerengine</td>
</tr>
<tr>
<td>Content and Experience</td>
<td>Yes</td>
<td>oce</td>
</tr>
<tr>
<td>Core Services (Networking, Compute, Block Volume)</td>
<td>Yes</td>
<td>core</td>
</tr>
<tr>
<td>Cost Analysis (Usage API)</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>Yes</td>
<td>datacatalog</td>
</tr>
<tr>
<td>Data Flow</td>
<td>Yes</td>
<td>dataflow</td>
</tr>
<tr>
<td>Data Integration</td>
<td>Yes</td>
<td>dataintegration</td>
</tr>
<tr>
<td>Data Safe</td>
<td>Yes</td>
<td>data_safe</td>
</tr>
<tr>
<td>Data Science</td>
<td>Yes</td>
<td>datascience</td>
</tr>
<tr>
<td>Database</td>
<td>Yes</td>
<td>database</td>
</tr>
<tr>
<td>Database Management</td>
<td>Yes</td>
<td>database_management</td>
</tr>
<tr>
<td>Digital Assistant</td>
<td>Yes</td>
<td>oda</td>
</tr>
<tr>
<td>DNS Service</td>
<td>Yes</td>
<td>dns</td>
</tr>
<tr>
<td>Email Delivery</td>
<td>Yes</td>
<td>email, email_tenancy</td>
</tr>
<tr>
<td><strong>Supported OCI service</strong></td>
<td><strong>Resource discovery support</strong></td>
<td><strong>Resource discovery services parameter</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Events</td>
<td>Yes</td>
<td>events</td>
</tr>
<tr>
<td>FastConnect</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>File Storage</td>
<td>Yes</td>
<td>file_storage</td>
</tr>
<tr>
<td>Functions</td>
<td>Yes</td>
<td>functions</td>
</tr>
<tr>
<td>Health Checks</td>
<td>Yes</td>
<td>health_checks</td>
</tr>
<tr>
<td>IAM</td>
<td>Yes</td>
<td>identity, availability_domain</td>
</tr>
<tr>
<td>Integration Cloud</td>
<td>Yes</td>
<td>integration</td>
</tr>
<tr>
<td>Key Management (for the Vault service)</td>
<td>Yes</td>
<td>kms</td>
</tr>
<tr>
<td>Limits</td>
<td>Yes</td>
<td>limits</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>Yes</td>
<td>load_balancer</td>
</tr>
<tr>
<td>Logging</td>
<td>Yes</td>
<td>logging</td>
</tr>
<tr>
<td>Logging Analytics</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Management Agent</td>
<td>Yes</td>
<td>management_agent</td>
</tr>
<tr>
<td>Management Dashboard</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Marketplace</td>
<td>Yes</td>
<td>marketplace</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Yes</td>
<td>monitoring</td>
</tr>
<tr>
<td>MySQL Database</td>
<td>Yes</td>
<td>mysql</td>
</tr>
<tr>
<td>NoSQL Database Cloud</td>
<td>Yes</td>
<td>nosql</td>
</tr>
<tr>
<td>Notifications</td>
<td>Yes</td>
<td>ona</td>
</tr>
<tr>
<td>Object Storage</td>
<td>Yes</td>
<td>object_storage</td>
</tr>
<tr>
<td>Optimizer</td>
<td>Yes</td>
<td>optimizer</td>
</tr>
<tr>
<td>OS Management</td>
<td>Yes</td>
<td>osmanagement</td>
</tr>
<tr>
<td>Registry (Artifacts and Container Images API)</td>
<td>Yes</td>
<td>artifacts</td>
</tr>
<tr>
<td>Service Connector Hub</td>
<td>Yes</td>
<td>sch</td>
</tr>
<tr>
<td>Streaming</td>
<td>Yes</td>
<td>streaming</td>
</tr>
<tr>
<td>Tagging</td>
<td>Yes</td>
<td>tagging</td>
</tr>
<tr>
<td>Oracle Cloud VMware Solution</td>
<td>Yes</td>
<td>ocvp</td>
</tr>
<tr>
<td>Web Application Firewall (WAF)</td>
<td>Yes</td>
<td>waas</td>
</tr>
</tbody>
</table>

**Deprecated Resources**

This topic covers the list of resources and data sources that have been marked deprecated by the Oracle Cloud Infrastructure (OCI) Terraform provider and their respective suggested replacements, if any.
Resources and data sources marked for deprecation will trigger warnings during Terraform plan and apply operations. For example:

The 'oci_autonomous_data_warehouse' resource has been deprecated. Please use 'oci_autonomous_database' instead.

Resources on path to deprecation may stop working in future, use the respective guide, if available, on how to migrate using the new replacements.

**Deprecated Resources and Data Sources**

Resources that have a migration path have deprecation guides available on how to rename and migrate them to their new replacements.

Data sources do not have deprecation guide as you can directly replace them in their Terraform configuration and refresh the state.

<table>
<thead>
<tr>
<th>Caution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before executing any deprecation guide, ensure that you have backed up your Terraform state file to avoid any data loss.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provider Version</th>
<th>Type</th>
<th>Old Deprecated Resource Name</th>
<th>New Resource Name</th>
<th>Migration?</th>
<th>Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.97.0</td>
<td>Resource</td>
<td>oci_dns_records</td>
<td>oci_dns_rrsets</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.97.0</td>
<td>Resource</td>
<td>oci_dns_records</td>
<td>oci_dns_rrsets</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.18</td>
<td>Resource</td>
<td>oci_autonomous_data_warehouse</td>
<td>oci_autonomous_database</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.18</td>
<td>Data Source</td>
<td>oci_autonomous_data_warehouse</td>
<td>oci_autonomous_databases</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.18</td>
<td>Data Source</td>
<td>oci_autonomous_data_warehouse</td>
<td>oci_autonomous_databases</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.18</td>
<td>Resource</td>
<td>oci_autonomous_data_warehouse_backup</td>
<td>oci_autonomous_database_backup</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.18</td>
<td>Data Source</td>
<td>oci_autonomous_data_warehouse_backup</td>
<td>oci_autonomous_database_backups</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3.18</td>
<td>Data Source</td>
<td>oci_autonomous_data_warehouse_backup</td>
<td>oci_autonomous_database_backups</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2.1.12</td>
<td>Resource</td>
<td>oci_swift_password</td>
<td>oci_identity_auth_token</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2.1.12</td>
<td>Data Source</td>
<td>oci_swift_passwords</td>
<td>oci_identity_auth_tokens</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Version</td>
<td>Provider version in which said resource or data source was marked deprecated</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the deprecated resource or data source</td>
</tr>
<tr>
<td>Old Deprecated Resource Name</td>
<td>Deprecated resource or data source name</td>
</tr>
<tr>
<td>New Resource Name</td>
<td>New resource or data source name that will provide the same functionality</td>
</tr>
<tr>
<td>Migration?</td>
<td>If migration is possible to the new resource through Terraform state import</td>
</tr>
<tr>
<td>Guide</td>
<td>Link to deprecation guide on how to rename and migrate to new resource, if applicable</td>
</tr>
</tbody>
</table>
**Deprecation Notices**

Deprecation notices for fields can be found in any of the previously released CHANGELOG. Deprecation notices are also shown as deprecated during Terraform `plan` and `apply` operations. For example:

The `size_in_mbs` field has been deprecated. Please use `size_in_gbs` instead.

**Troubleshooting**

This topic describes how to troubleshoot common Oracle Cloud Infrastructure (OCI) Terraform provider issues. Refer to Troubleshooting Basics for first steps.

**Common Issues**

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>See Terraform state drift with tag defaults and tags for secondary resources for a known issue with tags related to Terraform.</td>
</tr>
</tbody>
</table>

**Automatic Retries**

While applying, refreshing, or destroying a plan, Terraform may encounter some intermittent OCI errors (such as 429 or 500 errors) that could succeed on retry. By default, the OCI Terraform provider automatically retries such operations for up to 10 minutes. The following fields can be specified in the provider block to further configure the retry behavior:

- `disable_auto_retries` - Disable automatic retries for retriable errors.
- `retry_duration_seconds` - The minimum duration (in seconds) to retry a resource operation in response to HTTP 429 and HTTP 500 errors. The actual retry duration may be slightly longer due to jittering of retry operations. This value is ignored if the `disable_auto_retries` field is set to true.

**Concurrency Control using Retry Backoff and Jitter**

To alleviate contention between parallel operations against OCI services; the OCI Terraform provider schedules retry attempts using quadratic backoff and full jitter. Quadratic backoff increases the maximum interval between subsequent retry attempts, while full jitter randomly selects a retry interval within the backoff range.

For example, the wait time between the first and second retry attempts is chosen randomly between 1 and 8 seconds. The wait time between the second and third retry attempts is chosen randomly between 1 and 18 seconds. Regardless of the number of retry attempts, the retry interval time is capped after the 12th attempt at 288 seconds.

Note that the `retry_duration_seconds` field only affects retry duration in response to HTTP 429 and 500 errors; as these errors are more likely to result in success after a long retry duration. Other HTTP errors (such as 400, 401, 403, 404, and 409) are unlikely to succeed on retry. The `retry_duration_seconds` field does not affect the retry behavior for such errors.

**Resources are destroyed when applying changes**

Existing OCI resources might be destroyed and re-created when Terraform configurations attempt to update a resource property that is not updatable. Terraform warns you when changes will destroy a resource. Always run `terraform plan` before applying changes to see what resources will be affected. See Destructive Changes for more information.

**"NotAuthenticated" error when using Terraform**

If the Terraform CLI returns an error message like the following:

```plaintext
* oci_core_vcn.resource1: Service error:NotAuthenticated. The required information to complete authentication was not provided or was incorrect.
  http status code: 401
```

- Verify you have properly set `user_ocid`, `tenancy_ocid`, `fingerprint` and `private_key_path`. 
• Verify your `private_key_path` is pointing to your private key and not the corresponding public key.
• Verify you have added the corresponding public key to the user account you have specified with `user_ocid`.
• Verify the public/private key pairs you are using are of the correct format. See Required Keys for details on the correct format and how to generate keys.
• Verify the user account is part of a group with the appropriate permissions to perform the actions in the plan you are executing.
• Verify your Tenancy has been subscribed to the Region you are targeting in your plan.

"TCP...i/o timeout" message when connecting via proxy

If the Terraform CLI returns an error message like the following:

* provider.oci: ... dial tcp 134.70.16.0:443: i/o timeout

Then you may not have properly configured your proxy settings. The OCI Terraform provider supports `http_proxy`, `https_proxy` and `no_proxy` variables where the inclusion or exclusion lists can be defined as follows:

```bash
export http_proxy=http://www.your-proxy.com:80/
export https_proxy=http://www.your-proxy.com:80/
export no_proxy=localhost,127.0.0.1
```

"Timeout while waiting for state" message

If the Terraform CLI returns an error message like the following:

* oci_database_backup.mydb: timeout while waiting for state to become 'ACTIVE' (last state: 'CREATING', timeout: 15m0s)

Then the OCI service is indicating that the resource has not yet reached the expected state after polling for some time.

You may need to increase the operation timeout for your resource to continue polling for longer. See Operation Timeouts for details on how to do this.

"Field cannot be set" error message

If the Terraform CLI returns an error message like the following:

* Error: "field_name": this field cannot be set

You are likely using an older version of the OCI Terraform provider and the field you are trying to set was released in a later version. Use the following command to check your Terraform provider version.

```bash
terraform -version
```

The OCI Terraform provider documentation reflects the latest version.

"No such file" error after upgrading the OCI Terraform provider

If the Terraform CLI returns an error message like the following:

Error asking for user input: 1 error(s) occurred:

* provider.oci: dial unix /var/folders/6r/8fk5dmbj4_z3s10mc_y_fhjw0000gn/T/plugin811254328|netrpc: connect: no such file or directory

You are likely using a version of the OCI Terraform provider that is not compatible with the Terraform binary you have installed. For OCI Provider versions v3.x.x and above, a minimum Terraform version of v.0.10.1 is required.
"x509: certificate signed by unknown authority" error message

If the Terraform CLI returns an error message like the following:

```
Error: Get https://iaas.<region>.oraclecloud.com/20160918/services: x509:
  certificate signed by unknown authority
  on ../modules/network/modules/main/main.tf line 3...
```

Ensure that Terraform is using trusted TLS certificates and the certificate chain is valid. See Terraform runs failing with "x509: certificate signed by unknown authority" error for more information. If using MacOS Catalina, refer to the MacOS section of the document for more specifics on resolving certificate issues.

"Could not get info about the first DbHome in the dbSystem" error message when importing db_home

If the oci_database_db_system being imported is missing a primary db_home, an empty placeholder for db_home is set in the Terraform state file. To keep configurations consistent with the imported state, add an empty placeholder for db_home to your configuration. For example:

```ruby
# Add this placeholder into your oci_database_db_system configuration to
# indicate that the primary db home is empty.
db_home {
  database {
    admin_password = ""
  }
}
```

Errors about service limits

While using Terraform, you may encounter errors indicating that you have reached or exceeded the service limits for a resource.

To understand more about your OCI service limits and how to request a limit increase, see Service Limits

OCI Modules for PowerShell

The Oracle Cloud Infrastructure Modules for PowerShell is a set of cmdlet modules that can be used with PowerShell Core to manage Oracle Cloud Infrastructure resources. You can invoke these cmdlets from the PowerShell command-line and with the associated PowerShell scripting language.

Requirements

To use the OCI Modules for PowerShell, you must have the following:

- An Oracle Cloud Infrastructure account.
- A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users. For a list of typical policies you may want to use, see Common Policies on page 2142.
- A configuration file and key pair used for signing API requests, with the public key uploaded to Oracle Cloud using Oracle Cloud Infrastructure Console. Only the user calling the API should possess the private key.
- A supported version of PowerShell installed on Windows, Linux, or macOS operating systems.

**Note:**
For installation instructions, see Installing PowerShell.

Supported PowerShell Versions

To use the OCI Modules for PowerShell, you must have the following:

- PowerShell Core version 6.0 or higher
Services Supported

- Analytics Cloud
- Announcements
- API Gateway
- Application Migration
- Application Performance Monitoring
- Audit
- Autoscaling (Compute)
- Big Data
- Blockchain Platform
- Budgets
- Compute Instance Agent (Oracle Cloud Agent)
- Container Engine for Kubernetes
- Content and Experience
- Core Services (Networking, Compute, Block Volume)
- Cloud Guard
- Data Catalog
- Data Flow
- Data Integration
- Data Safe
- Data Science
- Data Transfer
- Database
- Database Management
- Digital Assistant
- DNS
- Email Delivery
- Events
- File Storage
- Functions
- Golden Gate
- Health Checks
- IAM
- Integration
- Vault
- Limits
- Load Balancing
- Logging
- Logging Analytics
- Logging Search
- Logging Ingestion
- Management Agent Cloud
- Management Dashboard
- Marketplace
- Monitoring
- Object Storage
- OCI Registry
- Operations Insights
- Optimizer
- Organizations
• OS Management
• Quotas
• Resource Manager
• Roving Edge Infrastructure
• Search
• Secret Management (for the Vault)
• Service Connector Hub
• Streaming
• Support Management
• Usage
• VMWare Solution
• Web Application Acceleration and Security
• Work Requests (Compute, Database)

Contact Us

Contributions
Got a fix for a bug or a new feature you’d like to contribute? The OCI Modules for PowerShell are open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the OCI Modules for PowerShell is released, subscribe to the Atom feed.

Questions or Feedback
• GitHub Issues: To file bugs and feature requests only.
• Stack Overflow: Please use the oracle-cloud-infrastructure and oci-powershell-modules tags in your post.
• Developer Tools section of the Oracle Cloud forums.
• My Oracle Support

Getting Started
This topic describes how to install and configure the OCI Modules for PowerShell.

Prerequisites
Be sure to satisfy all the requirements listed here.

Installing Modules
1. Start a PowerShell session:
   a. On Windows, launch PowerShell from the Start Menu.
   b. On Linux or MacOS, run pwsh from a shell prompt:

   ```
   $ pwsh
   PowerShell 7.0.3
   Copyright (c) Microsoft Corporation. All rights reserved.
   https://aka.ms/powershell
   Type 'help' to get help.
   PS /Users/username>
   ```

   2. Cmdlets corresponding to each OCI service supported by OCI Modules for PowerShell are packaged into an individual PowerShell module named OCI.PSModules.<ServiceName>.

   3. Continue to either Installing from PowerShell Gallery or Installing from GitHub on page 4317.
Installing from PowerShell Gallery

1. By default, PowerShell Gallery ("PS Gallery") is configured as a PSRepository. This can be verified by running the `Get-PSRepository` command:

   ```
   PS /> Get-PSRepository
   Name                      InstallationPolicy   SourceLocation
   ----                      ------------------   --------------
   PSGallery                 Untrusted            https://www.powershellgallery.com/api/v2
   ```

2. You can set PS Gallery as a trusted repository to avoid prompts every time you attempt to install a module from PS Gallery:

   ```
   PS /> Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
   ```

3. PowerShell modules that correspond to a supported OCI service are called service modules. To install a service module run the `Install-Module` command. This example installs the service module for the OCI Identity service:

   ```
   PS /> Install-Module -Name OCI.PSModules.Identity
   ```

   **Note:**
   Each service module depends on the `OCI.PSModules.Common` (Common Module), which offers functionality common to all service modules. Installing a service module will also install the corresponding version of `OCI.PSModules.Common` for that service module.

4. Installed modules can be found in the path specified by the `$Env:PSModulePath` environment variable, or by running the `Get-Module` command with the `ListAvailable` parameter.

   ```
   PS /> Get-Module -ListAvailable
   ```

Installing from GitHub

To install the OCI PowerShell modules from GitHub:

1. Download the latest OCI Modules artifacts and extract them into a local directory.

   **Note:**
   Cmdlets corresponding to each OCI service supported by OCI Modules for PowerShell are packaged into an individual PowerShell module named `OCI.PSModules.<ServiceName>`.

2. Register the extracted directory as the local PowerShell repository:

   ```
   PS /> Register-PSRepository -Name "LocalRepo" -SourceLocation \<extractedlocation>
   ```

3. Find the modules available in the local repository:

   ```
   PS /> Find-Module -Repository "LocalRepo"
   ```
4. Install a specific module:

```
PS /> Install-Module -Name OCI.PSModes.Module.Objectstorage -Verbose -Repository LocalRepo
```

**Note:**
Each service module depends on the OCI.PSModes.Module.Common (Common Module), which offers functionalities common to all service modules. Installing a service module will also install the corresponding version of OCI.PSModes.Module.Common for that service module.

5. Installed modules can be found in the path specified by the $Env:PSModulePath environment variable, or by running the Get-Module command with the ListAvailable parameter.

```
PS /> Get-Module -ListAvailable
```

**Installing with Yum**

If you are using Oracle Linux version 7.x, the OCI PowerShell Modules packages can be installed with yum.

1. To install the OCI PowerShell modules using yum:

```
$sudo yum install oci-powershell-modules
```

2. Start a PowerShell Session and register the downloaded directory /usr/lib/dotnet/NuPkgs as a local PowerShell repository using the following command:

```
$pwsh
PS /> Register-PSRepository -Name "LocalRepo" -SourceLocation /usr/lib/dotnet/NuPkgs
```

3. Find the modules available in the local repository using the following command:

```
PS /> Find-Module -Repository "LocalRepo"
```

4. Install a specific module:

```
PS /> Install-Module -Name OCI.PSModes.Module.Objectstorage -Verbose -Repository LocalRepo
```

**Note:**
Each service module depends on the OCI.PSModes.Module.Common (Common Module), which offers functionalities common to all service modules. Installing a service module will also install the corresponding version of OCI.PSModes.Module.Common for that service module.

5. Installed modules can be found in the path specified by the $Env:PSModulePath environment variable, or by running the Get-Module command with the ListAvailable parameter.

```
PS /> Get-Module -ListAvailable
```

**Setup**

Follow these installation steps if you haven't installed the required modules.

Before invoking cmdlets in OCI Modules, you need to set up the configuration file, and then optionally import the required modules into a PowerShell session.

**Configuration File**
A configuration file provides essential configuration information, like user credentials and tenancy OCID. This configuration information is used by the OCI Modules for PowerShell to authenticate and interact with Oracle Cloud services. You can create this file using a setup cmdlet, or manually using a text editor.

**Set-OCIClientConfig**

The `Set-OCIClientConfig` cmdlet included in the Common module will walk you through setting up a configuration file. This cmdlet prompts you for information required by the configuration file, including the key pair used to sign API requests.

For more information about how to find the required information, see:

- Where to Get the Tenancy's OCID and User's OCID
- Regions and Availability Domains

**Manual Setup**

If you want to set up the API signing key pair manually and write your own configuration file, see SDK and Tool Configuration and Required Keys.

**Note:**

Use the `New-OCIClientKeys` cmdlet to generate a API signing key pair to include in the configuration file.

**Importing Modules**

PowerShell will automatically import the module (and its dependencies) into your session the first time you run any command from the installed module. To explicitly import a module, run the `Import-Module` command.

For example, to import the version 1.0.0 of the Identity service module:

```powershell
PS /> Import-Module OCI.PSModules.Identity -RequiredVersion 1.0.0 -Verbose
```

To find all imported modules in your current PowerShell Session, run the `Get-Module` command:

```powershell
PS /> Get-Module
```

<table>
<thead>
<tr>
<th>ModuleType</th>
<th>Name</th>
<th>ExportedCommands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary</td>
<td>OCI.PSModules.Identity</td>
<td>{Add-OCIIdentityUserToGroup, Enable-OCIIdentityMfaTotpDevice}</td>
</tr>
</tbody>
</table>

**Note:**

Each service module depends on the `OCI.PSModules.Common` (Common Module), which offers functionalities common to all service modules. Installing a service module will also install the corresponding version of `OCI.PSModules.Common` for that service module.

**Updating Modules**

New versions of the OCI PowerShell modules release weekly. To update the installed OCI PowerShell modules to the latest version, run the `Update-Module` command.
Before updating any OCI module, you should first uninstall the module. To avoid dependency conflicts when importing modules into PowerShell session, update all installed OCI Modules to the same version.

```
PS /> Update-Module -Name "OCI.PSModules.*" -Verbose
```

### Uninstalling Modules

To remove any installed module, you can either use the `Uninstall-Module` cmdlet or delete the module folder located in the path in the `$Env:PSModulePath` environment variable.

For example:

```
PS /> Uninstall-Module -Name OCI.PSModules.Identity
```

### Next Steps

Now that you’ve taken care of installation and setup, you can proceed directly to Working with Cmdlets, or continue to Advanced Concepts on page 4324.

### Working with Cmdlets

The OCI Modules for PowerShell cmdlets are built on the Oracle Cloud Infrastructure SDK for .NET. These cmdlets make calls to Oracle Cloud Infrastructure REST APIs with the passed cmdlet parameter values.

```
Note:

Cmdlet parameters are named corresponding to the respective REST API parameters as listed in the API reference.
```

The OCI REST APIs use HTTPS requests and responses. For more information, see About the API.

### Cmdlet Discovery

OCI Cmdlets are named using a `verb -noun` pair pattern, where `verb` is the operation performed on the resource denoted by the `noun`, which usually includes the service name followed by the name of the resource in that service.

For example, the following command returns all cmdlets available to work with a Compute Instance resource in the Compute service, which is part of the OCI Core PowerShell module:

```
PS /> Get-Command -Module OCI.PSModules.Core -Noun "*ComputeInstance*"
```

<table>
<thead>
<tr>
<th>CommandType</th>
<th>Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cmdlet</td>
<td>Get-OCIComputeInstance</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-OCIComputeInstanceConsoleConnection</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-OCIComputeInstanceConsoleConnectionsList</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-OCIComputeInstanceDevicesList</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-OCIComputeInstancesList</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Invoke-OCIComputeInstanceAction</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Move-OCIComputeInstanceCompartment</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-OCIComputeInstance</td>
<td>0.1.0</td>
</tr>
<tr>
<td></td>
<td>OCI.PSModules.Core</td>
<td></td>
</tr>
</tbody>
</table>
Sample Cmdlet

This example shows how to invoke a simple OCI cmdlet that calls the GetNamespace operation of the OCI Object Storage service. This operation returns the name of the Object Storage namespace for the user making the request.

Note:
Install and import the ObjectStorage service before trying out this example. For more information, see Installation.

PS /> Get-OCIObjectStorageNamespace
us-phx-test-namespace

Cmdlet Help

To get help information for a cmdlet, use the Get-Help cmdlet, passing in the name of the cmdlet as a parameter.

Note:
For more detailed help information, use the -Full parameter.

This example shows help output for the Get-OCIObjectStorageNamespace cmdlet:

PS /> Get-Help Get-OCIObjectStorageNamespace
NAME
Get-OCIObjectStorageNamespace

SYNOPSIS
Invokes ObjectStorage service - GetNamespace operation.

SYNTAX

DESCRIPTION
Each Oracle Cloud Infrastructure tenant is assigned one unique and uneditable Object Storage namespace. The namespace is a system-generated string assigned during account creation. For some older tenancies, the namespace string may be the tenancy name in all lower-case letters. You cannot edit a namespace. GetNamespace returns the name of the Object Storage namespace for the user making the request. If an optional compartmentId query parameter
Developer Tools

is provided, GetNamespace returns the namespace name of the corresponding tenancy, provided the user has access to it.

RELATED LINKS
APIReference https://docs.cloud.oracle.com/en-us/iaas/api/

REMARKS
To see the examples, type: "Get-Help Get-OCIObjectStorageNamespace - Examples"
For more information, type: "Get-Help Get-OCIObjectStorageNamespace - Detailed"
For technical information, type: "Get-Help Get-OCIObjectStorageNamespace -Full"
For online help, type: "Get-Help Get-OCIObjectStorageNamespace -Online"

Common Parameters

This section describes the optional global cmdlet parameters common to all cmdlets present in any OCI PowerShell service module.

**ConfigFile**
The path to the configuration file that supplies credentials for the Oracle Cloud.

**Endpoint**
Indicates the service endpoint to use for OCI API calls, including any required API version path. For example, https://audit.us-ashburn-1.oraclecloud.com

**FullResponse**
By default, OCI Cmdlets output the response body of the REST API operation. Including the FullResponse switch parameter indicates that the cmdlet should output the complete response returned by the API operation wrapped in its associated .NET type (an object containing API response headers in-addition to an optional response body).

**NoRetry**
A switch parameter to disable default retry logic for calls to services.

By default, OCI Modules for PowerShell retry failed API calls that return status codes 400, 401, 404, 409, 429 and 500. Retry attempts use an exponential backoff algorithm with a maximum of 5 attempts over a maximum time span of 10 minutes. Include this switch parameter in the cmdlet invocation to disable the default retry logic.

**Profile**
Specifies which profile to load from the configuration file. This parameter expects a case-sensitive profile name existing in the configuration file.

**Region**
Specifies the Region-ID of the region to make calls against. For example: us-phoenix-1 or ap-singapore-1.

**TimeOutInMillis**
Specifies the maximum wait time in milliseconds for the API request to complete. The default value is 100,000 milliseconds (100 seconds).
**AuthType**

Defines the type of authentication to use for making API requests. By default the API Key in your config file is used. Valid values are ApiKey or InstancePrincipal.

**Cmdlet Input and Output**

This section describes how the OCI Cmdlets process input and output.

**Cmdlet Input**

OCI Cmdlets currently accept inputs from command line parameters or through pipeline by property names. To see an example on passing inputs through pipeline by property name refer this sample.

**Cmdlet Output**

By default, OCI Cmdlets return only the API response body encapsulated in an associated .NET type. For use cases that require the users to inspect the complete API response including the response headers, use the `FullResponse` switch parameter in the cmdlet invocation.

In the following example, the `GetConfiguration` operation in the OCI Audit service returns a Configuration resource in the response body.

```
Note:
To run the following example, import OCI.PSMODULES.Audit.
```

```
PS /> Get-OCIAuditConfiguration -CompartmentId $env:CompartmentId | gm
TypeName: Oci.AuditService.Models.Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>MemberType</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equals</td>
<td>Method</td>
<td>bool Equals(System.Object obj)</td>
</tr>
<tr>
<td>GetHashCode</td>
<td>Method</td>
<td>int GetHashCode()</td>
</tr>
<tr>
<td>GetType</td>
<td>Method</td>
<td>type GetType()</td>
</tr>
<tr>
<td>ToString</td>
<td>Method</td>
<td>string ToString()</td>
</tr>
<tr>
<td>RetentionPeriodDays</td>
<td>Property</td>
<td>System.Nullable[int] RetentionPeriodDays</td>
</tr>
<tr>
<td>(get;set;)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

In the example output above, the default invocation only returns the .NET object that encapsulates the API response body.

To get an output object that includes the complete API response include the `-FullResponse` parameter in the cmdlet invocation. For example:

```
PS /> Get-OCIAuditConfiguration -CompartmentId $env:CompartmentId - FullResponse | gm
```

```
TypeName: Oci.AuditService.Responses.GetConfigurationResponse

<table>
<thead>
<tr>
<th>Name</th>
<th>MemberType</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equals</td>
<td>Method</td>
<td>bool Equals(System.Object obj)</td>
</tr>
<tr>
<td>GetHashCode</td>
<td>Method</td>
<td>int GetHashCode()</td>
</tr>
<tr>
<td>GetType</td>
<td>Method</td>
<td>type GetType()</td>
</tr>
<tr>
<td>ToString</td>
<td>Method</td>
<td>string ToString()</td>
</tr>
<tr>
<td>(get;set;)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Asynchronous Calls

For Oracle Cloud APIs that return an asynchronous work request response, with opc-work-request-id in the response header and no response body, OCI PowerShell Cmdlets return a Oci.PSModules.Common.Cmdlets.WorkRequest object containing the OpcWorkRequestID property.

For example:

TypeName: Oci.PSModules.Common.Cmdlets.WorkRequest

<table>
<thead>
<tr>
<th>Name</th>
<th>MemberType</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-----------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Equals</td>
<td>Method</td>
<td>bool Equals(System.Object obj)</td>
</tr>
<tr>
<td>GetHashCode</td>
<td>Method</td>
<td>int GetHashCode()</td>
</tr>
<tr>
<td>GetType</td>
<td>Method</td>
<td>type GetType()</td>
</tr>
<tr>
<td>ToString</td>
<td>Method</td>
<td>string ToString()</td>
</tr>
<tr>
<td>OpcWorkRequestId</td>
<td>Property</td>
<td>string OpcWorkRequestID {get;set;}</td>
</tr>
</tbody>
</table>

Error Handling

If an error occurs when running an OCI Cmdlet, the cmdlet throws a terminating error with an error record containing the exception and an error message about the underlying cause.

Advanced Concepts

This section covers PowerShell SDK concepts.

Managing Session Preferences

The OCI Modules for PowerShell support the use of environment variables in a PowerShell session to specify values some optional common parameters. These environment variables can be configured directly in the PowerShell session or by using the Set-OCIClientSession cmdlet. Values assigned to these environment variables are used for making API calls only in the PowerShell session in which they are set.

Set Environment Variables Directly from PowerShell

The following environment variables can be used to specify values for some parameters used by the OCI Modules for PowerShell:

<table>
<thead>
<tr>
<th>Cmdlet Parameter</th>
<th>Environment Variable Name</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>OCI_PS_REGION</td>
<td>If a value is not specified, region value from the user preferred profile is used.</td>
</tr>
<tr>
<td>Profile</td>
<td>OCI_PS_PROFILE</td>
<td>If a value is not specified, the DEFAULT profile is used.</td>
</tr>
<tr>
<td>ConfigFile</td>
<td>OCI_PS_CONFIG</td>
<td>If a value is not specified, config file at ~/.oci/config will be used.</td>
</tr>
<tr>
<td>NoRetry</td>
<td>OCI_PS_NORETRY</td>
<td>If a value is not specified, default retry strategy is used to attempt retries.</td>
</tr>
<tr>
<td>TimeOutInMillis</td>
<td>OCI_PS_TIMEOUT</td>
<td>If a value is not specified, the default value of 100,000 milliseconds (100 seconds) is used.</td>
</tr>
<tr>
<td>AuthType</td>
<td>OCI_PS_AUTH</td>
<td>If a value is not specified, the API key defined in the config file is used.</td>
</tr>
</tbody>
</table>

For example, to set the region:

PS /> $Env:OCI_PS_REGION="us-phoenix-1"
Set Environment Variables using Cmdlets

You can use the Set-OCIClientSession and Get-OCIClientSession cmdlets to set and retrieve the session preference environment variables.

Set-OCIClientSession

This cmdlet sets the Region, Profile and Config file preferences for the PowerShell session through the environment variables shown above.

Note:
Import OCI.PSMODULES.Common before running the following example.

```
PS > Set-OCIClientSession -RegionId "us-ashburn-1" -Profile "Test" -Config "~/.oci/testconfig"

RegionId     Profile Config
--------     ------- -----
us-ashburn-1 Test    ~/.oci/testconfig
```

To remove a session preference environment variable, run the Clear-OCIClientSession cmdlet with the appropriate parameters.

Get-OCIClientSession

The Get-OCIClientSession cmdlet in the common module is used to retrieve the session preference values set for the common parameters from the current PowerShell session.

```
PS > Get-OCIClientSession

RegionId     Profile Config
--------     ------- -----
us-ashburn-1 Test
```

Parameter Precedence

When evaluating parameters, the OCI Modules for PowerShell follows this order of precedence:

1. The value specified in the cmdlet parameter.
2. The value specified in the session preferences.
3. The value specified in the user-selected profile of the OCI configuration file located at ~/.oci/config.

Note:
The OCI Modules for PowerShell use the DEFAULT profile as a fall back profile. Any value that isn't explicitly defined for a given profile is inherited from the DEFAULT profile.

History Store

By default, OCI Cmdlets output the response body of the underlying REST API operation. The history store provides users with a PowerShell variable that can be used to look into OCI Cmdlet invocations and their complete API responses from OCI services.

Note:
Each PowerShell session gets its own history store.

You can use the history store to:

- Use the previous Cmdlet’s response object values in the next Cmdlet
Developer Tools

- Inspect the complete API response, including the response headers - for example, the use of e-tags for optimistic concurrency, or the OpcNextPage header for pagination
- Examine cmdlet invocation sequences for diagnostic purposes

The history store is encapsulated as an

For more information, see the History Store example on GitHub.

History Store Properties

This section explains the properties contained in the history store object stored in $OCICmdletHistory.

<table>
<thead>
<tr>
<th>Name</th>
<th>MemberType</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastResponse</td>
<td>Property</td>
<td>psobject LastResponse {get;}</td>
</tr>
<tr>
<td>Size</td>
<td>Property</td>
<td>int Size {get;}</td>
</tr>
</tbody>
</table>

Size

Indicates the maximum number of commands that can be saved in the history store. The default value is 20. Valid values are from 1 and 100000 (inclusive). To modify the size of history store, use Set-OCICmdletHistory.

**Note:**

We recommend keeping the history size to a minimum to limit memory usage.

Entries


The Oci.PSModules.Common.Cmdlets.CmdletHistory.OCICmdletHistory object has the following properties:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartTime</td>
<td>System.DateTime</td>
<td>Start time of cmdlet execution.</td>
</tr>
<tr>
<td>EndTime</td>
<td>System.DateTime</td>
<td>End time of cmdlet execution.</td>
</tr>
<tr>
<td>Command</td>
<td>System.Management.Automation.InvocationInfo</td>
<td>Describes how and where this command was invoked.</td>
</tr>
</tbody>
</table>

LastResponse


History Store Cmdlets

Oci.PSModules.Common module provides the following cmdlets for working with the History Store. See the GitHub example.
Get-OCICommandHistory
Gets the cmdlet history stored in the current PowerShell session.

Set-OCICommandHistory
Sets properties of the history store.

Clear-OCICommandHistory
Deletes the cmdlet history stored in the current PowerShell session.

Pagination

OCI Cmdlets that invokes list API operations have the ability to paginate results, allowing you to retrieve the available results in batches (automatically following pagination tokens) until no more records are available.

Note:
Examples in this topic call the ListImages operation in the OCI Compute service. Be sure to import OCI.PSMODULES.Core before trying out the examples in this section.

Get First Page Results

The default behavior of a cmdlet that supports pagination is to get only the first page of results when invoked without the -Page parameter specified.

For example, to get the first page of compute images available invoke the Get-OCIComputeImagesList with your Compartment ID:

```
PS /> Get-OCIComputeImagesList -CompartmentId $Env:CompartmentId | Measure-Object
Count             : 100
```

The above example implicitly sets the -Page parameter to NULL.

Note:
The maximum number of results per page is defined by the service and can be found in the service API reference.

Limit Results

The -Limit parameter specifies the maximum number of results returned per page.

This example sets the maximum number of results returned per page to 5:

```
PS /> Get-OCIComputeImagesList -CompartmentId $Env:CompartmentId -Limit 5 | Measure-Object
Count             : 5
```

Get Next Page Results

The -Page parameter is used to get the next page of results by passing the pagination token from the `opc-next-page` response header contained in the previous cmdlet response.

Note:
You can use the history store to get the previous cmdlet response.
This example shows how to retrieve the results remaining from a previous paginated call by passing the `$OCICmdletHistory.LastResponse.OpcNextPage` property from the history store as the argument to the `-Page` parameter:

```
PS /> Get-OCIComputeImagesList -CompartmentId $Env:CompartmentId -Page $OCICmdletHistory.LastResponse.OpcNextPage | Measure-Object
Count : 100
```

### Get All Results

OCI Cmdlets that support pagination can auto paginate and fetch results from all available pages. Let the cmdlet do the pagination by passing `-All` switch parameter when running the cmdlet.

```
PS /> Get-OCIComputeImagesList -CompartmentId $Env:CompartmentId -All | Measure-Object
Count : 293
```

### Waiters and Asynchronous Calls

Most Oracle Cloud Infrastructure resources, such as compute instances, have *lifecycles*. In many cases, you want your command to wait until a resource or work request reaches a specific state, or a timeout is exceeded, before taking further action. You can poll a resource to determine its state.

OCI Modules for PowerShell offer waiter parameters that allow your cmdlet to wait until a resource reaches a desired state. A cmdlet with waiter parameters can be invoked in a blocking manner to wait until either one of the desired states is reached or a timeout is exceeded. Waiters abstract the polling logic that you would otherwise have to add before taking further actions on a resource or a work request.

For example, when you call `LaunchInstance` in the Compute service, the response header contains a `work-request-id`. The OCI Modules for PowerShell uses this ID when you specify the `-WaitForStatus` parameter, which causes your script to wait until the work request succeeds before proceeding.

For example:

```
#Create a new compute instance and wait for the instance work request to succeed or fail,
#polling every 60 seconds and attempting 20 times max
$ComputeInstance = New-OCIComputeInstance -LaunchInstanceDetails $LaunchDetails -WaitForStatus Succeeded,Failed -MaxWaitAttempts 20 -WaitIntervalSeconds 60
```

### Waiter parameters

This section describes the parameters used for asynchronous calls.

**WaitForStatus**

Specify this parameter to perform the action and then wait until the resource reaches the desired lifecycle state. Multiple states can be specified, returning when the resource reaches one of the desired states.

**WaitIntervalSeconds**

Check every `WaitIntervalSeconds` to see whether the resource has reached one of the desired states. Default value for this parameter is 30 seconds.

**MaxWaitAttempts**

Maximum number of attempts to be made until the resource reaches one of the desired states. Default value for this parameter is 3 attempts.
Currently, OCI Cmdlets do not accept maximum wait time for cmdlets that support waiters. You can work around this limitation by controlling the values of MaxWaitAttempts and/or WaitIntervalSeconds.

On successful completion, the cmdlet returns the original response object received. In case of an error like the resource failing to reach the desired state within the given limits, an exception containing the error message would be thrown.

Stream Inputs and Outputs

Some OCI Cmdlets interact with APIs that accept or return stream type objects (for example, the InvokeFunctions operation in the Functions service). These OCI cmdlets accept parameters that can take a file path and implicitly convert files to streams and back.

You can either pass a stream parameter or the equivalent file parameter, but not both.

The file input parameter is named after the corresponding stream input parameter and file output parameter is named as OutputFile.

For an example, see the help text for the Invoke-OCIFunctionsInvokeFunction cmdlet in OCI.PSModules.Functions.

This sample on GitHub shows how to work with streams.

Logging

To facilitate troubleshooting, OCI Modules for PowerShell supports logging debug- and verbose-level messages on the console in addition to error messages. This feature has been integrated with the standard PowerShell Debug and Verbose parameters.

Pass the -Debug or -Verbose parameters in the cmdlet invocation to see log messages on the console.

For example:

```
PS /> Get-OCIComputeImagesList -CompartmentId $Env:CompartmentId -Limit 1 -Verbose
#More Verbose
PS /> Get-OCIComputeImagesList -CompartmentId $Env:CompartmentId -Limit 1 -Debug
```

Authenticating with Instance Principals

Instance principals is an IAM service feature that enables instances to be authorized actors (or principals) that can perform actions on service resources. Each compute instance has its own identity, and it authenticates using the certificates that are added to it. These certificates are automatically created, assigned to instances and rotated, preventing the need for you to distribute credentials to your hosts and rotate them.

For more information on instance principals, see Calling Services from an Instance.

To enable instance principal authentication from OCI Cmdlets, call authorize the instance and set the AuthType parameter. For example:

```
PS /> Get-OCIIdentityRegionsList -AuthType InstancePrincipal
```
Examples

Examples of OCI PowerShell Cmdlet usage can be found on GitHub, including:

- Creating an instance using waiters
- Accessing OCI cmdlet history store
- Using OCI cmdlet common parameters
- Downloading an object from Object Storage
- Setting preferred region and profile per session
- List all available Compute Images
- Searching resources using polymorphic objects

If you'd like to see another example not already covered, file a GitHub issue.

Running Examples

1. Clone the OCI PowerShell Modules project from GitHub.
   
   PS /> git clone https://github.com/oracle/oci-powershell-modules.git

2. Navigate to the examples folder inside the cloned repository.
   
   PS /> cd ./oci-powershell-modules/Examples

3. Install the required modules. Find additional details about setting up and running examples from the README page.

4. Run the example scripts after setting the required environment variables.
   
   PS /oci-powershell-modules/Examples> ./Waiter_Core.ps1

Ansible Collection

This topic provides information about the Oracle Cloud Infrastructure (OCI) Ansible collection.

Collections are Ansible’s recommended method of packaging and releasing modules, roles, playbooks, and documentation. See Getting Started on page 4331 to begin using our Ansible collection.

OCI supports the use of Ansible modules to automate cloud infrastructure provisioning and configuration, orchestration of complex operational processes, and deployment and update of your software assets.

Ansible tracks your resources using inventory lists. The inventory can be a simple static .ini file or dynamically created, where a plugin assembles an up-to-date infrastructure inventory. For more information, see Working with Ansible Inventory on page 4333.

Ansible playbooks automate configuration, deployment, and orchestration tasks. Ansible playbooks use a declarative language (YAML) that allows you to describe infrastructure configuration, deployment policy, and the orchestration of complex process steps. OCI provides a set of Example Playbooks for your review.

The OCI Ansible collection supports Ansible Tower and AWX. For more information on how to set up the collection with Ansible Tower, refer to the Using Oracle Cloud Infrastructure with Ansible Tower and AWX blog post. To install the free version of Ansible Tower (AWX) on an OCI Compute instance, you can use our solution on GitHub.

- **Services supported**: Refer to the list of currently supported services for details.
- **Licensing**: Copyright © 2020, Oracle and/or its affiliates. This software is made available to you under the terms of the GPL 3.0 license or the Apache 2.0 license. See LICENSE.txt for details.
- **Documentation**: Additional OCI Ansible collection documentation is available on readthedocs.io and GitHub.
- **Download**: To download our Ansible collection, follow the steps in Getting Started on page 4331.

Notifications

To be notified when new versions of our Ansible collection are released, subscribe to the Oracle Cloud Infrastructure Ansible collection Atom feed.
Questions or Feedback

Ways to get in touch:

- GitHub: To file bugs and feature requests only.
- Stack Overflow: Use the oci-ansible and oracle-cloud-infrastructure tags in your post.
- Developer Tools section of the Oracle Cloud forums.

Getting Started

This topic discusses how to get started using the Oracle Cloud Infrastructure (OCI) Ansible collection. The OCI Ansible collection replaces our legacy Ansible modules.

Note:

If you currently use our legacy Ansible modules and would like to start using collections, refer to our migration guide.

To start using Ansible with OCI, ensure that you meet the prerequisites, then install the Ansible collection using yum or manually.

Tip:

You can use Resource Manager to preinstall the Oracle Cloud Development Kit on a Compute instance in your compartment. The Oracle Cloud Development Kit includes Ansible, the OCI Ansible collection and its dependencies, and preconfigures the required authorization.

Both Ansible and our Ansible collection also come preinstalled and preauthenticated on Cloud Shell.

Prerequisites for Using Ansible with Oracle Cloud Infrastructure

- You must have an Oracle Cloud Infrastructure account.
- You must have a user in that account in a security group with a policy that grants necessary permissions for working with resources in the account compartments. For guidance, see How Policies Work on page 2136.
- You must have the necessary credentials and OCID information.

Installing the Ansible Collection with yum

You can use yum to install the Oracle Cloud Infrastructure Ansible collection RPM.

The Ansible collection RPM installs the OCI Ansible collection and its required dependencies: the OCI SDK for Python and Ansible.

Note:

This installation uses Python version 3.6 and Ansible version 2.9 or later.

The following example shows how to use yum to install the Ansible collection RPM:

```bash
yum -y install oraclelinux-developer-release-el7 & & sudo yum install oci-ansible-collection
```

After installing the RPM, you must configure the SDK and CLI configuration file as explained in Configuring Authentication on page 4333.

To test the installation of the RPM and configuration of the SDK, you can run a sample playbook. For example:

```bash
ansible-playbook-3 /usr/share/doc/oci-ansible-collection-<version>/samples/object_storage/get_namespace/sample.yaml
```

Manual Installation

Installing the Oracle Cloud Infrastructure SDK for Python
1. Download and install the SDK for Python by following instructions in the topic, SDK for Python. For additional guidance, see Downloading and Installing the SDK.

2. After installing the SDK for Python, you must configure it using instructions in the topic Configuring the SDK.

Installing and Configuring Ansible

- To install Ansible, follow the instructions provided in the Ansible Installation Guide.
- For guidance configuring Ansible, see Configuring Ansible.

**Note:**
The OCI Ansible collection requires Ansible version 2.9 or later. If you are using an earlier version of Ansible, refer to the documentation for our legacy modules.

Installing the Oracle Cloud Infrastructure Ansible Collection

Install the OCI Ansible collection from Ansible Galaxy by using the following command:

```
$ ansible-galaxy collection install oracle.oci
```

If you've already installed the collection, you can update its modules to the latest version by adding the `--force` flag to the command. For example:

```
$ ansible-galaxy collection install --force oracle.oci
```

Sample Playbooks

Sample playbooks are available in the Oracle Cloud Infrastructure Ansible collection GitHub project. The samples library is updated regularly with the addition of new samples. See Example Ansible Playbooks on page 4338 for more information.

Writing a Sample Playbook

After your installation is complete, or if you're using the Cloud Shell, you can write a sample playbook that uses Ansible modules. Following is an example playbook (named `list_buckets.yml`) that uses the `oci_object_storage_bucket_facts` module to fetch facts pertaining to the buckets in your compartment.

```yaml
---
- name: List summary of existing buckets in OCI object storage
collections:
- oracle.oci
collection: local
hosts: localhost
tasks:
- name: List bucket facts
  oci_object_storage_bucket_facts:
    namespace_name: '<yournamespace>'
    compartment_id: '<yourcompartmentocid>'
    register: result
- name: Dump result
dump:
  msg: '{{result}}'
```

Executing the Playbook

Execute the Ansible playbook using Python by invoking this command:

```
$ ansible-playbook list_buckets.yml
```

How to Obtain Module Documentation

Detailed information about using our Ansible modules is available on readthedocs.io.
To obtain access to detailed information about using Ansible modules in the CLI, use the `ansible-doc` command on the module's name. For example, to get the documentation for the `oci_object_storage_bucket_facts` module, execute the following command:

```
$ ansible-doc oracle.oci.oci_object_storage_bucket_facts
```

### Configuring Authentication

When creating and configuring Oracle Cloud Infrastructure resources, Ansible modules use authentication information that is outlined in the [SDK and CLI Configuration File](#) on page 4184.

**Caution:**

User Credentials on page 2360 that are referenced in Oracle Cloud Infrastructure SDK configuration files grant access to Oracle Cloud Infrastructure resources. Therefore, it is important to secure the credentials to prevent unauthorized access to these resources. To secure the credentials on the controller node where your Ansible playbooks run, follow guidelines outlined in the document [Securing IAM](#) on page 3688 (see section entitled "IAM Credentials").

Ansible modules permit you to override authentication information specified in the SDK configuration file by using module options and environment variables. Documentation for authentication overrides is provided internally, as described in [How to Obtain Module Documentation](#). However, using environment variables and Ansible module options to override authentication information must be avoided in production scenarios.

We recommend using Oracle Cloud Infrastructure SDK configuration files to specify authentication information. To support multiple users, use the "profiles" feature in the SDK configuration file. When distributing roles that use Ansible modules, ensure that no IAM credentials are included with the roles.

### For More Information

- [Using collections](#)

### Working with Ansible Inventory

Ansible tracks configuration resources by preserving lists, called inventory lists, as simple files (also sometimes called a *hostfile*). These inventory lists can be static or dynamic. Dynamic lists can automatically update when inventory resources are added, deleted, or moved.

Because many Oracle Cloud Infrastructure (OCI) resources are added and deleted over time, static inventory lists can easily become obsolete. Tools such as Terraform or the OCI SDKs also may affect your resources.

Oracle Cloud Infrastructure provides a dynamic inventory plugin for maintaining accurate Ansible inventory.

For more information about Ansible inventory files, see [Working with Inventory](#) and [Working with Dynamic Inventory](#).

#### Enabling the Inventory Plugin

The OCI inventory plugin, like most inventory plugins shipped with Ansible, is disabled by default. Plugins must be enabled in your `ansible.cfg` file to function.

Enable the OCI inventory plugin by adding it to your `ansible.cfg` file. For example:

```
[inventory]
enable_plugins = oracle.oci.oci
```

If you still use our legacy Ansible modules, your `ansible.cfg` file should contain the following entry instead:

```
[inventory]
enable_plugins = oci
```

### Configuring the Inventory Plugin
The only requirement for using the OCI inventory plugin after it is enabled is to provide an inventory source you have permissions to parse. Inventory sources are defined in a YAML configuration file. See User Permissions on page 4337 for more information.

To start using the inventory plugin with a YAML configuration source, create a file with with one of the following accepted filenames:

- `<filename>.oci.yml`
- `<filename>.oci.yaml`

Add plugin: `oracle.oci.oci` to the YAML configuration file.

The minimum inventory source file needed to run the OCI inventory plugin looks like this, for example:

```yaml
# demo.oci.yml
plugin: oracle.oci.oci

# Optional fields to specifyoci connection config:
config_file: ~/.oci/config
config_profile: DEFAULT
```

This example uses the `config_file` and `config_profile` parameters so the plugin can use authentication information that is outlined in the SDK and CLI Configuration File on page 4184. Some parameters can also be provided as environment variables.

For a complete list of parameters and environment variables that the plugin supports, see OCI Inventory Plugin. The Example Configuration on page 4334 include many of the available parameters.

**Important:**

By default, the OCI inventory plugin discovers and lists only Compute instances that have a public IP address. See Hostname Format on page 4338 for more information.

**Order of Precedence**

The inventory plugin uses the following order of precedence when an option is provided in more than one location:

1. YAML file settings.
2. Environment variables.
3. Configuration settings in the selected profile in your OCI configuration file.

**Example Configuration**

The following inventory source file includes examples of many of the available parameters:

```yaml
# Fetch all hosts
plugin: oracle.oci.oci

# OCI Config information
config_file: ~/.oci/config
config_profile: DEFAULT

# Optional fields
# ----------------------------
# Example select regions
regions:
  - us-ashburn-1
  - us-phoenix-1

# Enable threads to speedup lookup
enable_parallel_processing: yes
```
# Select compartment by ocid or name
compartments:
  - compartment_ocid: ocid1.compartment.oc1..<compartment_OCID>
    fetch_hosts_from_subcompartments: false
  - compartment_name: "<compartment_name>"
    parent_compartment_ocid: ocid1.tenancy.oc1..<compartment_OCID>

# Example filtering using hostname IP
hostnames:
  - "10.145.214.11"

# Example filtering using hostname_format
# The default hostname_format value is public_ip
hostname_format: "private_ip"

# Example group results by key
keyed_groups:
  - key: availability_domain

# Example using filters
filters:
  - availability_domain: "IwGV:US-ASHBURN-AD-3"
  - display_name: "instance20190506231645"
  - lifecycle_state: "RUNNING"
  - defined_tags: {
      "ansible_tag_2": {
              "ansibletag448": "test_value"
      }
  }
  - freeform_tags: {
      "Environment": "Production"
  }

# Enable Cache
cache: yes
cache_plugin: jsonfile
cache_timeout: 7200
cache_connection: /tmp/oci-cache
cache_prefix: oci_

# DB Hosts
fetch_db_hosts: true

Enabling Caching

Caching can be enabled to speed lookups. You can set caching options for an individual YAML configuration source or for multiple inventory sources using environment variables or Ansible configuration files. If you enable caching for an inventory plugin without providing inventory-specific caching options, the inventory plugin uses fact-caching options.

Here is an example of enabling caching for an individual YAML configuration file:

```yaml
# demo.oci.yml
plugin: oracle.oci.oci
cache: yes
cache_plugin: jsonfile
cache_timeout: 7200
cache_connection: /tmp/oci-cache
cache_prefix: oci_

# DB Hosts
fetch_db_hosts: true
```

Using the Inventory Plugin
Ansible inventory plugins allow you to define the data sources used to compile an inventory of hosts that Ansible uses to target tasks. These data sources are accessed by using either the \(-i /path/to/file\) or the \(-i 'host1, host2'\) command line parameters, or from other configuration sources.

You can run the inventory with this command, for example:

```
ansible-inventory -i <filename>.oci.yml --graph
```

This produces output similar to the following:

```
@all:
  --@oci:
    --compute_instance1
    --compute_instance2
  @ungrouped:
```

**Important:**

By default, the inventory is generated for all the compartments in the tenancy. You must have COMPARTMENT_INSPECT permission on the root compartment for this script to be able to access all compartments. However, when compartment_ocid is specified, the inventory is generated for only the specific compartment, so you only need COMPARTMENT_INSPECT permission on the specified compartment. For more information, see How Policies Work on page 2136.

To fetch all instance details, you must also have permission to list and read instances and VNICs, and read VCNs and subnets. See User Permissions on page 4337 for more information.

You can add inventory plugins to your plugin path and set the default inventory path to simplify your commands. Add the default inventory path to the [defaults] section of your ansible.cfg file, or use the ANSIBLE_INVENTORY environment variable to point your inventory sources. You can then run the following command to yield the same output as when you pass your YAML configuration sources directly:

```
ansible-inventory --graph
```

Inventory plugins normally only execute at the start of a run, before playbooks, plays, and roles are loaded. You can ‘re-execute’ a plugin by using the meta: refresh_inventory task, which clears out the existing inventory and rebuilds it.

**Inventory Output**

The inventory list that is generated by the inventory plugin is grouped using the following attributes:

- The region in which the Compute instance resides
- The name of the compartment the Compute instance belongs to
- The Availability Domain the Compute instance is in
- The vcn_id of the VCN the compute instance is in
- The subnet_id of the subnet the Compute instance is in
- The security_list_ids of the subnet the Compute instance is in
- The image_id of the image used to launch the Compute instance
- Shape of the Compute instance
- The Compute instance’s free-form tags, with the group name set to tag_<tag_name>=<tag_value>
- The Compute instance’s defined tags, with the group name set to <tag_namespace>#<tag_name>=<tag_value>
- OCI Compute instance metadata (key-value pairs), with the group name set to <metadata-key>=<metadata-value>
• OCI Compute instance extended metadata (key-value pairs), with the group name set to `<metadata-key>=<metadata-value>`

Using Dynamic Groups

You can create dynamic groups using host variables with the constructed `keyed_groups` option. The option groups can also be used to create groups and create and modify host variables.

For example:

```yaml
# demo.oci.yml
plugin: oracle.oci.oci
regions:
  - us-phoenix-1
  - us-ashburn-1
keyed_groups:
  # add hosts to tag_Name_value groups for each oci host's tags.Name variable
  - key: tags.Name
    prefix: tag_Name_
    groups:
      # add hosts to the group development if any of the dictionary's keys or values is the word 'devel'
      development: "'devel' in (tags|list)"
```

This example produces output similar to the following:

```
@all:
  |--@oci:
  |  |--compute_instance1
  |  |--compute_instance2
  |  |--...
  |  |--@development:
  |  |  |--compute_instance1
  |  |  |--compute_instance2
  |  |--@tag_Name_Dev_Instance:
  |  |  |--compute_instance1
  |  |--@tag_Name_Test_Server:
  |  |  |--compute_instance2
  |  |--@ungrouped
```

If a host does not have the variables specified in the configuration (such as tags.Name, tags, private_ip_address), the host is not added to groups other than those that the inventory plugin creates and the ansible_host host variable is not modified.

Database Hosts

Database nodes can be now be fetched by setting the option `fetch_db_hosts`. Database nodes are servers running database software. For example:

```yaml
# demo.oci.yml
# DB Hosts
plugin: oracle.oci.oci
fetch_db_hosts: true
```

Troubleshooting the Inventory Plugin

If the inventory list generated by the OCI inventory plugin does not include every Compute instance in your tenancy, review the following information.

User Permissions
Ensure that the user has the policy permissions to list the Compute instances. The user OCID is specified using either the OCI_USER environment variable, or the profile section in your SDK and CLI configuration file.

To see a list of permissions for API operations, see Details for the Core Services.

The inventory plugin makes API calls for the following operations:

- ListCompartments
- ListVNICAttachments
- GetSubnet
- GetVCN
- GetVNIC
- GetInstance

### Hostname Format

**Important:**

The default value for the `hostname_format` parameter is `public_ip`.

The inventory generated by the OCI inventory plugin contains only Compute instances that have a `public IP address` by default. This is useful in cases where the Ansible controller node is outside of the VCN, since Ansible can only reach instances that have public IP addresses.

When running Ansible from a Compute instance *within* your VCN that has access to all of the subnets within your VCN, including Compute instances that have private IP addresses, you must set the `hostname_format` to `private_ip` to list compute instances using their private IP addresses. The Example Configuration on page 4334 shows this configuration option.

### For More Information

Detailed information about using the OCI inventory plugin is available on readthedocs.io.

You can also use the following command to see the plugin documentation:

```bash
ansible-doc -t inventory oracle.ociOCI
```

Refer to the [official Ansible documentation](https://docs.ansible.com/ansible/latest/intro_inventory.html) for more information about inventory plugins.

### Example Ansible Playbooks

This topic provides a catalog of sample Ansible playbooks for Oracle Cloud Infrastructure (OCI) that illustrate how to carry out common infrastructure provisioning and configuration tasks using our Ansible collection.

These samples and solutions are organized in sections associated with OCI services. You can find a brief description of each playbook along with links to each sample on the [Oracle GitHub repository](https://github.com/oracle/oci-docs/tree/master/ansible/). Be sure to review the `Readme.md` file that is included in each playbook's root directory for additional instructions.

See Getting Started on page 4331 to begin using our Ansible collection.

### Samples

**Block Volume**

**Attaching a block volume to a Compute instance**

This sample playbook shows how to attach a block volume to a Compute instance using the iSCSI volume attachment type, and then connect it to the Compute instance using `iscsiadm`. The sample shows how to do the following:

- Generate a temporary, host-specific SSH key pair.
- Specify the public key from the key pair for connecting to the instance, and then launch the instance.
- Create a new Block Volume for the instance, attach the volume to the instance, and specify iSCSI as the volume attachment type.
• Connect to and then mount the volume from the Compute instance by executing iscsiadm commands over SSH using an Ansible module.

Go to the sample on Oracle GitHub.

**Compute**

**Launching an Always Free Compute instance**

This sample shows how to launch and access an Always Free Compute instance from the internet using SSH using OCI Ansible collections.

This sample shows how to do the following:
• Generate a temporary, host-specific SSH key pair.
• Specify the public key from that key-pair to connect to the instance during instance launch.
• Connect to the newly launched instance using SSH.

Go to the sample for Always Free on Oracle GitHub.

**Launching a Compute instance using App Catalog**

This sample shows how a public Compute instance can be launched using app_catalog and accessed from the internet using SSH with OCI Ansible collections.

This sample shows how to do the following:
• Generate a temporary, host-specific SSH key pair.
• Specify the public key from that key-pair to connect to the instance during instance launch.
• Fetch app_catalog and its versions and create a subscription for it.
• Launch the instance using app_catalog and connect to it using SSH.

Go to the sample on Oracle GitHub.

**Creating an instance pool**

This sample shows how to manage your Compute instances using resources such as instance configurations and instance pools that are provided using OCI Ansible collections. Instance pools help you create and provision multiple Compute instances within the same region based on a single instance configuration.

This sample shows how to do the following:
• Generate a temporary, host-specific SSH key pair.
• Specify the public key from that key-pair to connect to the instance during instance launch.
• Create an instance configuration that defines settings for creating a Compute instance as part of the instance pool. The configuration provides details such as base image, shape, and metadata.
• Use the instance pool to launch Compute instances based on the instance configuration.
• Connect to one of the Compute instances using SSH.

Go to the sample on Oracle GitHub.

**Creating instance Console connections and capturing Console history**

This sample shows how a serial and VNC console connection can be created for a Compute instance, and how the serial console data can be captured and fetched from a Compute instance using OCI Ansible collections. For more information about Console connections, see Troubleshooting Instances Using Instance Console Connections.

This sample shows how to do the following:
• Generate a temporary SSH key pair for the serial Console connection.
• Create an instance Console connection for a Compute instance.
• Capture serial Console data for a Compute instance, and then save the data to a local machine so you can troubleshoot and debug issues.

Go to the sample on Oracle GitHub.

**Launching a Compute instance**

This sample shows how to launch and access a public Compute instance from the internet using SSH with OCI Ansible collections.

This sample shows how to do the following:

• Generate a temporary, host-specific SSH key pair.
• Specify the public key from the key pair for connecting to the instance, and then launch the instance.
• Connect to the newly launched instance using SSH.

Go to the sample on Oracle GitHub.

**Enabling internet access from a Compute instance using the OCI NAT Gateway**

This sample shows how you can use OCI Ansible collections to enable internet access from Compute instances in a private subnet using a NAT Gateway in a public subnet. For more information about NAT gateways, see NAT Gateway on page 3247 and Access Resources on the Public Internet Through an Oracle Cloud Infrastructure NAT Gateway.

This sample shows how to do the following:

• Set up the VCN, the NAT gateway, the internet gateway, the public and private subnets, and the necessary security lists and route rules.
• Provision a bastion instance in the public subnet and a private instance in the private subnet.

Once set up, the private instance will have outbound Internet access through the NAT gateway, and will be accessible using SSH from the bastion instance.

Go to the sample on Oracle GitHub.

**Enabling internet access from a Compute instance using an OCI NAT Instance**

This sample shows how you can use OCI Ansible collections to enable internet access from Compute instances in a private subnet using a NAT instance in a public subnet as discussed here and in the whitepaper here.

This sample shows how to do the following:

• Set up the topology described in the whitepaper by creating the VCN, the internet gateway, the public and private subnets, and the necessary security lists and route rules. A NAT instance is provisioned in the public subnet and a private instance is provisioned in the private subnet.
• After the setup, the private instance has outbound internet access through the NAT instance in the public subnet.

Go to the sample on Oracle GitHub.

**Accessing Object Storage from a private instance using a service gateway**

This sample playbook shows how you can use OCI Ansible collections to enable private access to an Object Storage from a Compute instance using a service gateway. For more information about service gateways, see Access to Oracle Services: Service Gateway on page 3256. To read a blog post discussing how to connect Compute instances using the service gateway, see Connect Private Instances with Oracle Services Through an Oracle Cloud Infrastructure Service Gateway.
This sample shows how to do the following:

- Set up a user, group, and the policies required for managing buckets.
- Create and upload the required API keys to the user.
- Set up the VCN, the NAT gateway, the internet gateway, the public and private subnets, as well as the required security lists and route tables. A bastion instance is provisioned in the public subnet, and a private instance is provisioned in the private subnet.
- Provision a Compute instance in the private subnet,
- Install the OCI command line interface (CLI) and configure the CLI using the cloud init script.
- Disable the NAT gateway to restrict public access to the private instance.
- Create a bucket from the private instance using the OCI CLI, then verify that the bucket is created.

Following this setup, the private instance has private access to Object Storage.

Go to the sample on Oracle GitHub.

Container Engine for Kubernetes

**Creating a cluster using Container Engine for Kubernetes**

This sample creates a cluster with Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE) using OCI Ansible collections.

This sample shows how to do the following:

- Create and configure a VCN and related resources required for setting up an OKE cluster.
- Create a cluster.
- Create a node pool.
- Download the kubeconfig file for the cluster.

Go to the sample on Oracle GitHub.

Database

**Creating an Always Free Autonomous Database**

This sample shows how you can use the OCI Ansible collection to create an Always Free Autonomous Database with Autonomous Transaction Processing and manage its lifecycle. See [Overview of Autonomous Databases](#) on page 1149 for more information.

This sample shows how to do the following:

- Set up an Autonomous Database with Autonomous Transaction Processing.
- List all of the Autonomous Transaction Processing instances available in a compartment, filtered by display name.
- Get the "facts" for a specified database.
- Stop and start an Autonomous Database.
- Delete an Autonomous Database.

Go to the sample on Oracle GitHub.

**Setting up an Autonomous Database**

This sample shows how you can use the OCI Ansible collection to create an Autonomous Database with Autonomous Transaction Processing and manage its lifecycle. Refer to the [Overview of Autonomous Databases](#) on page 1149 for more information.

This sample shows how to do the following:

- Set up an Autonomous Database with Autonomous Transaction Processing.
- List all of the Autonomous Transaction Processing instances available in a compartment, filtered by display name.
- Get the "facts" for a specified database.
Creating a Bare Metal and Virtual Machine DB system

This sample shows how you can use the OCI Ansible collection to create Bare Metal and Virtual DB systems. For more information about OCI co-managed DB Systems, see Bare Metal and Virtual Machine DB Systems on page 1352.

This sample shows how to do the following:

- Set up a Virtual Machine DB System.
- Get facts of a specific DB System and list available DB Homes.
- List all the databases available in specified DB Home and get facts of specific database.
- Collect DB Node's VNIC information of a specified DB system.
- Extract Public and Private IPs of the DB Node from VNIC.
- Create a backup from initial database.
- Restore a database from latest backup.
- Create a new database from backup.
- Update database fields.

Go to the sample on Oracle GitHub.

File Storage

Creating and mounting a file system

This sample shows how you can use the OCI Ansible collection to create and access a File Storage file system through compute instances.

This sample shows how to do the following:

- Generate all network related dependencies (e.g. VCN, subnets) and security lists with the configuration required by File Storage.
- Generate the certificates required by instances.
- Create File Storage components such as mount target, file system, export, and snapshot.
- Mount the file system through a Compute instance and access the contents through another Compute instance.

Go to the sample on Oracle GitHub.

Exporting multiple file systems and mount targets

This sample shows how you can use the OCI Ansible collection to export one file system using two different export paths on two different mount targets. It also demonstrates how a single mount target can export paths from two different file systems.

This sample shows how to do the following:

- Generate all network related dependencies (e.g. VCN, subnets) and security lists with the configuration required by File Storage.
- Generate the certificates required by instances.
- Create File Storage components such as mount target, file system, export, and snapshot.
- Export one file system to two different mount targets.
- Export paths from a single mount target to two different file systems.
- Mount the file system through a compute instance.

Go to the sample on Oracle GitHub.

Identity
**Adding a user and group**

This sample shows how you can use the OCI Ansible collection to perform basic Oracle Cloud Infrastructure Identity and Access Management (IAM) tasks. The sample assumes the default user configured in the OCI configuration is in the Administrator group or has the required access for managing users, groups, policies.

This sample shows how to do the following:

- Create a new group.
- Create a policy.
- Create a user then add it to the group and policy.
- Create user password.
- Generate SSH keys and assign them to the user.

**Go to the sample on Oracle GitHub.**

**Load Balancing**

**Creating a load balancer**

This sample shows how you can use the OCI Ansible collection to create a public load balancer.

This sample shows how to do the following:

- Generate all network-related dependencies, like a VCN and subnets.
- Generate the certificates required by the load balancer.
- Create a public load balancer.

**Go to the sample on Oracle GitHub.**

**Networking**

**Provisioning a VCN with private subnets**

This sample shows how you can use the OCI Ansible collection to provision a virtual cloud network (VCN) with two private subnets in different availability domains and an IPSec VPN. The IPSec VPN uses a *dynamic routing gateway* (DRG), *customer-premises equipment* (CPE), and an IPSec connection. The provisioned resources are illustrated in this networking scenario.

This sample shows how to provision the following resources:

- A VCN
- Two private subnets
- A dynamic routing gateway
- *Customer-premises equipment*
- An IPSec connection between DRG & CPE

Finally, it retrieves IPSec connection configuration information and status.

**Go to the sample on Oracle GitHub.**

**Object Storage**

**Getting a namespace**

This sample playbook shows how to use the OCI Ansible collection to get the tenancy namespace in Object Storage.

**Go to the sample on Oracle GitHub.**

**Listing objects and buckets**

This sample playbook shows how to use the OCI Ansible collection to list all Object Storage objects from all buckets in a namespace.
Go to the sample on Oracle GitHub.

Deleting objects
This sample playbook shows how to use the OCI Ansible collection to delete objects created within a specified range of days from all buckets in a namespace. You can modify the sample so that it deletes objects older than a specified number of days, which helps you prune old or unwanted objects stored in the Object Storage service.

Go to the sample on Oracle GitHub.

Solutions

MuShop
MuShop is a showcase of several Oracle Cloud Infrastructure (OCI) services in a unified reference application. The sample application implements an e-commerce platform built as a set of microservices. The accompanying content can be used to get started with cloud native application development on OCI.

MuShop can be deployed in different ways to explore OCI based on your subscription. OCI offers Always Free tier with resources that can be used indefinitely.

This project is an example of how you can build OCI infrastructure using the OCI Ansible collection.

Go to the solution on Oracle GitHub.

Compute Jenkins Plug-in
This topic provides information about installing, configuring, and using the Compute Jenkins plug-in for Oracle Cloud Infrastructure services.

- **Licensing:** The Oracle Cloud Infrastructure Compute Jenkins plug-in is dual-licensed under the Universal Permissive License (UPL) and the Apache License 2.0; third-party content is separately licensed as described in the code.
- **Download:** GitHub
- **Documentation:** Oracle Cloud Infrastructure Compute Plug-in - Jenkins Wiki

Contributions
Got a fix for a bug, or a new feature you’d like to contribute? The Oracle Cloud Infrastructure Compute Jenkins plug-in is open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the Oracle Cloud Infrastructure Compute Jenkins plug-in is released, subscribe to the Atom feed.

Questions or Feedback
- **GitHub:** To file bugs and feature requests only.
- **Stack Overflow:** Please use the oracle-cloud-infrastructure tag in your post.
- **Developer Tools section** of the Oracle Cloud forums
- **My Oracle Support**

Chef Knife Plug-in
This topic provides information about installing, configuring, and using the Chef Knife Plug-in for Oracle Cloud Infrastructure.

- **Licensing:** This provider and sample is licensed under the Mozilla Public License 2.0; third-party content is separately licensed as described in the code.
- **Download:** GitHub
- **Documentation:** README
Contributions
Got a fix for a bug, or a new feature you'd like to contribute? The Chef Knife Plug-in for Oracle Cloud Infrastructure is open source and accepting pull requests on GitHub.

Notifications
To be notified when a new version of the Chef Knife Plug-in for Oracle Cloud Infrastructure is released, subscribe to the Atom feed.

Questions or Feedback
- GitHub: To file bugs and feature requests only.
- Stack Overflow: Please use the oracle-cloud-infrastructure tag in your post.
- Developer Tools section of the Oracle Cloud forums
- My Oracle Support

Grafana Plug-in
This topic provides instructions for installing, configuring, and using the Oracle Cloud Infrastructure Data Source for Grafana, otherwise referenced as the Grafana Plug-in.

Grafana Plug-in Overview
Grafana is an open-source visualization and alerting tool that you can use for analytics and monitoring of time-series data (metrics). While metrics from Oracle Cloud Infrastructure Monitoring are visible in metrics charts through the Console, you can use Oracle Cloud Infrastructure Data Source for Grafana ("the Grafana Plug-in") to view metrics from resources across providers on a single Grafana dashboard.

Prerequisites for Using the Grafana Plug-in
- An Oracle Cloud Infrastructure account.
- A user in that account, in a security group with an IAM policy that grants necessary permissions for working with resources in the account compartments. The policy must give you access to the metric namespaces emitting metrics (such as Compute) as well as the related resources (such as a set of Compute instances). If you try to perform an action and get a message that you don’t have permission or are unauthorized, confirm with your administrator the type of access you’ve been granted and which compartment you should work in. Administrators: For common policies that give groups access to metrics, see Let users access monitoring metrics in a compartment on page 2155 and Restrict user access to a specific metric namespace on page 2156. To authorize resources, such as instances, to make API calls, add the resources to a dynamic group through its matching rules, and then create a policy that allows that dynamic group access to metrics. To allow access across compartments, create the policy in the tenancy. Because of the concept of policy inheritance, instances in the indicated dynamic group can then access metrics in any compartment. To reduce the scope of access to a particular compartment, specify that compartment instead of the tenancy. See Let instances make API calls to access monitoring metrics in the tenancy on page 2156.
- Compute instances: To emit metrics, the Compute Instance Monitoring plugin must be enabled on the instance, and plugins must be running. The instance must also have either a service gateway or a public IP address to send metrics to the Monitoring service. For more information, see Enabling Monitoring for Compute Instances on page 783.
- Required keys and Oracle Cloud Infrastructure IDs (OCIDs). For guidance, see "Required Keys and OCIDs" in the Oracle Cloud Infrastructure User Guide.

Download and Install the Grafana Plug-in

Note:
Grafana must be installed before you can install the Grafana Plug-in. Version 3.0 or later required.
Authentication for metric access depends on where Grafana is running. If you are running Grafana on a local machine outside Oracle Cloud Infrastructure, you must call the Monitoring API using the Command Line Interface (CLI).
If you are running Grafana on an Oracle Cloud Infrastructure Compute instance that you created, then you can add the instance to a dynamic group by configuring a matching rule. In all scenarios, you have the option of calling the API using the CLI.

For instructions on installing the Grafana Plug-in (Oracle Cloud Infrastructure Data Source for Grafana), see https://github.com/oracle/oci-grafana-plugin.

**Configure the Grafana Plug-in**

This section describes how to add the Grafana Plug-in and set up a dashboard.

To configure the Grafana Plug-in

**Note:**

When installed locally, the Grafana plug-in accesses metrics using calls to the Monitoring API.

1. Set up the CLI for accessing Oracle Cloud Infrastructure APIs.
   You'll need to access the Monitoring API for authentication.
2. Navigate to the Grafana homepage at the following URL.
   http://localhost:3000
3. Add the Grafana Plug-In (Oracle Cloud Infrastructure Data Source for Grafana).
   In addition to the steps below, see the Grafana instructions for adding data sources at http://docs.grafana.org/guides/getting_started/.
   a. In Grafana, on the Home Dashboard, click the gear icon on the left.
   b. Click **Add data source**.
   c. In the Filter text box, type: oracle-oci-datasource
   d. In the filtered list, select **oracle-oci-datasource**.
   e. In the Settings page, fill in your **Tenancy OCID**, **Default Region**, and **Environment**. For Environment choose **local**.
4. Set up a dashboard of the type "Graph."
5. (Optional) To confirm access to metrics from Oracle Cloud Infrastructure, update your dashboard query ("Metrics") with a specific region, compartment, namespace, metric. You can also add one or more dimensions.

Congratulations. You can now view your Oracle Cloud Infrastructure metrics in Grafana!

**Environment options**

**local** is for Grafana deployments outside Oracle Cloud Infrastructure.

**OCI Instance** is for Grafana deployments on Oracle Cloud Infrastructure resources.

The data source is now added, enabling you to set up a dashboard showing metrics from Oracle Cloud Infrastructure.

**Troubleshoot the Plug-In**

If the dashboard query ("Metrics") fails to populate with options, or if you have other issues accessing metrics, then the IAM policy used to access metrics may be malformed, or it may not include all required matching rules for your dynamic group (for running Grafana on an Oracle Cloud Infrastructure Compute instance that you created).

To resolve this issue, do the following.

- Review your IAM policy to ensure that it matches prerequisites.
- If you updated your IAM policy, then restart the Grafana server and refresh the Grafana homepage.
Other Tools

Tools and Plug-ins for SDKs and CLI

Oracle Cloud Infrastructure provides additional developer tools for automating processes and facilitating development.

**Toolkit for Eclipse** - The toolkit is an open source plug-in for the Eclipse Integrated Development Environment (IDE) that enables Java developers to code and deploy applications more quickly and efficiently.

- **Documentation**: [Toolkit for Eclipse](#) on page 4363
- **Download**: To build and install the Toolkit, clone the GitHub repository then follow instructions in [Getting Started with Toolkit for Eclipse](#).

**Oracle Developer Tools for Visual Studio** - The Oracle Developer Tools for Visual Studio provide a set of features that helps developers connect to Oracle Cloud Infrastructure from within the Microsoft Visual Studio IDE. You can use the tools to view and manage your Oracle Databases and Oracle Autonomous Databases in Oracle Cloud Infrastructure and quickly and easily deploy a web application to Oracle Cloud Infrastructure Container Engine for Kubernetes.

- **Documentation**: [Oracle Developer Tools for Visual Studio](#) on page 4365
- **Download**: Refer to the documentation.

**HDFS Connector for Object Storage** - Read and write data with your Apache Hadoop application to and from the Oracle Cloud Infrastructure Object Storage service. Building the connector relies on Maven artifacts that are provided by the SDK for Java.

- **Documentation**: [HDFS Connector for Object Storage](#) on page 4347
- **Download**: [GitHub](#)

**Toolkit for Data Science** - The Oracle Accelerated Data Science (ADS) SDK is a Python library that is included as part of the Oracle Cloud Infrastructure Data Science service. ADS offers a friendly user interface that covers all the steps involved in the life-cycle of machine learning models, from connecting to different sources to using AutoML for model training to model evaluation and explanation. ADS also provides a simple interface to access the Oracle Cloud Infrastructure Data Science service model catalog and other Oracle Cloud Infrastructure services, including Object Storage.

- **Documentation**: [Oracle Accelerated Data Science (ADS) Python Library](#)
- **Download**: Oracle ADS Python library is pre-installed in the Oracle Cloud Infrastructure Data Science notebook session resource environment. It is not publicly available.

**HDFS Connector for Object Storage**

The Hadoop Distributed File System (HDFS) connector lets your Apache Hadoop application read and write data to and from the Oracle Cloud Infrastructure Object Storage service.

This SDK and sample is dual-licensed under the Universal Permissive License 1.0 and the Apache License 2.0; third-party content is separately licensed as described in the code.

- **Services supported**: Object Storage
- **Download**: [GitHub](#) or [Maven](#)
- **API Documentation**: [HDFS Connector API Reference](#)

**Requirements**

To use the HDFS connector, you must have:

- An Oracle Cloud Infrastructure account.
- A user created in that account, in a group with a policy that grants the desired permissions for any bucket you want to use. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see [Adding Users](#) on page 57. For a basic Object Storage policy, see [Let Object Storage admins manage buckets and objects](#) on page 2149.
- Java 8
• A TTL value of 60. For more information, see Configuring JVM TTL for DNS Name Lookups on page 4348.

Credentials and Passwords
If you use an encrypted PEM file for credentials, the passphrase will be read from configuration using the `getPassword` Hadoop Configuration method. The `getPassword` option checks for a password in a registered security provider. If the security provider doesn't contain the requested key, it will fallback to reading the plaintext passphrase directly from the configuration file.

Configuring JVM TTL for DNS Name Lookups
The Java Virtual Machine (JVM) caches DNS responses from lookups for a set amount of time, called time-to-live (TTL). This ensures faster response time in code that requires frequent name resolution.

The JVM uses the `networkaddress.cache.ttl` property to specify the caching policy for DNS name lookups. The value is an integer that represents the number of seconds to cache the successful lookup. The default value for many JVMs, -1, indicates that the lookup should be cached forever.

Because resources in Oracle Cloud Infrastructure use DNS names that can change, we recommend that you change the TTL value to 60 seconds. This ensures that the new IP address for the resource is returned on next DNS query. You can change this value globally or specifically for your application:

• To set TTL globally for all applications using the JVM, add the following in the `$JAVA_HOME/jre/lib/security/java.security` file:

```
networkaddress.cache.ttl=60
```

• To set TTL only for your application, set the following in your application's initialization code:

```
java.security.Security.setProperty("networkaddress.cache.ttl" , "60");
```

Installation
Copy the bundled jars from lib and third-party/lib the to each node of the Hadoop cluster so that they are included in Hadoop’s CLASSPATH.

SDK for Java and Maven Artifacts
Building an HDFS connector relies on Maven artifacts that are provided by the Oracle Cloud Infrastructure SDK for Java. To obtain the artifacts, you must download the SDK for Java and build it locally. You can then build the HDFS connector.

Important:
The SDK for Java file version that you download from the Oracle Releases page must match the HDFS connector version, which you can find in the `hdfs-connector/pom.xml` file in the dependency tag block that has the `groupId` attribute.

HDFS Connector and Maven Artifacts
The HDFS connector is available on Maven Central and JCenter.

To use the HDFS connector in your project, import the following project dependency. For example:

```
<dependency>
  <groupId>com.oracle.oci.sdk</groupId>
  <artifactId>oci-hdfs-connector</artifactId>
  <!-- Replace the version below with your required version -->
  <version>2.9.2.0</version>
</dependency>
```
Properties

You can set the following HDFS connector properties in the core-site.xml file. The BmcProperties page lists additional properties that you can configure for a connection to Object Storage.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs.oci.client.hostname</td>
<td>The URL of the host endpoint.</td>
<td>String</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>For example, <a href="https://www.example.com">https://www.example.com</a>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs.oci.client.auth.tenantId</td>
<td>The OCID of your tenancy.</td>
<td>String</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>To get the value, see Required Keys and OCIDs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs.oci.client.auth.userId</td>
<td>The OCID of the user calling the API.</td>
<td>String</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>To get the value, see Required Keys and OCIDs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs.oci.client.auth.fingerprint</td>
<td>The fingerprint for the key pair being used.</td>
<td>String</td>
<td>Yes, unless you provide a custom authenticator.</td>
</tr>
<tr>
<td></td>
<td>To get the value, see Required Keys and OCIDs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs.oci.client.auth.pemfilepath</td>
<td>The full path and file name of the private key used for authentication. The file should be on the local file system.</td>
<td>String</td>
<td>Yes, unless you provide a custom authenticator.</td>
</tr>
</tbody>
</table>
You can specify that a property value applies to a specific bucket by appending 
<bucket_name>.
<namespace_name> to the property name.

This example shows how properties can be configured in a core-site.xml file (the OCIDs are shortened for brevity):

```xml
<configuration>
  ...
  <property>
    <name>fs.oci.client.hostname</name>
    <value>https://objectstorage.us-ashburn-1.oraclecloud.com</value>
  </property>
  <property>
    <name>fs.oci.client.hostname.myBucket.myNamespace</name>
    <value>https://objectstorage.us-phoenix-1.oraclecloud.com</value><!-- Use Phoenix for myBucket@myNamespace -->
  </property>
  <property>
    <name>fs.oci.client.auth.tenantId</name>
    <value>ocid1.tenancy.oc1..exampleuniqueID</value>
  </property>
  <property>
    <name>fs.oci.client.auth.userId</name>
    <value>ocid1.user.oc1..exampleuniqueID</value>
  </property>
  <property>
    <name>fs.oci.client.auth.fingerprint</name>
  </property>
  <property>
    <name>fs.oci.client.auth.pemfilepath</name>
    <value>~/.oci/oci_api_key.pem</value>
  </property>
  ...
</configuration>
```

**Using Instance Principals for Authentication**

Oracle provides *instance principals* so that you no longer need to configure user credentials or provide PEM files on services running on instances. Each of these instances has its own identity and authenticates by using certificates added to the instance by instance principals.

To use instance principals authentication with the HDFS connector, simply provide the property `fs.oci.client.custom.authenticator` and set the value to `com.oracle.bmc.hdfs.auth.InstancePrincipalsCustomAuthenticator`.

Because using instance principals provides your instance with a custom authenticator, it is no long necessary to configure the following properties:

- `fs.oci.client.auth.tenantId`
- `fs.oci.client.auth.userId`
- `fs.oci.client.auth.fingerprint`
- `fs.oci.client.auth.pemfilepath`
The following example code illustrates using instance principals for authentication with the HDFS connector:

```xml
<?xml version="1.0"?>
<configuration>
    <property>
        <name>fs.oci.client.hostname</name>
        <value>https://objectstorage.us-phoenix-1.oraclecloud.com</value>
    </property>
    <property>
        <name>fs.oci.client.custom.authenticator</name>
        <value>com.oracle.bmc.hdfs.auth.InstancePrincipalsCustomAuthenticator</value>
    </property>
</configuration>
```

For more information about instance principals, see [Announcing Instance Principals for Identity and Access Management](#).

### Configuring a HTTP Proxy

You can set the following optional properties in the `core-site.xml` file to configure a HTTP proxy:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs.oci.client.proxy.uri</td>
<td>The URI of the proxy endpoint. For example, <a href="http://proxy.mydomain.com:80">http://proxy.mydomain.com:80</a>.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>fs.oci.client.proxy.username</td>
<td>The username to authenticate with the proxy.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>fs.oci.client.proxy.password</td>
<td>The password to authenticate with the proxy.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>fs.oci.client.multipart.allowed</td>
<td>Enables the upload manager to support multipart uploads.</td>
<td>Boolean</td>
<td>No</td>
</tr>
<tr>
<td>fs.oci.client.multipart.minobjectsize.mb</td>
<td>Specifies the minimum object size in mebibytes in order to use the upload manager.</td>
<td>Integer</td>
<td>No</td>
</tr>
<tr>
<td>fs.oci.client.multipart.partsize.mb</td>
<td>Specifies the part size in mebibytes for the upload manager.</td>
<td>Integer</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:**

Configuring a proxy enables use of the ApacheConnectorProvider when making connections to Object Storage. It buffers requests into memory and can impact memory utilization when uploading large objects. It is recommended to enable multipart uploads and adjust the multipart properties to manage memory consumption.
Large Object Uploads

Large objects are uploaded to Object Storage using multipart uploads. The file is split into smaller parts that are uploaded in parallel, which reduces upload times. This also enables the HDFS connector to retry uploads of failed parts instead of failing the entire upload. However, uploads may transiently fail, and the connector will attempt to abort partially uploaded files. Because these files accumulate (and you will be charged for storage), list the uploads periodically and then after a certain number of days abort them manually using the SDK for Java.

Information about using the Object Storage API for managing multipart uploads can be found in Using Multipart Uploads on page 3477.

Note:

If you prefer not to use multipart uploads, you can disable them by setting the `fs.oci.client.multipart.allowed` property to false.

Best Practices

The following sections contain best practices to optimize usage and performance.

Directory Names

There are no actual directories in Object Storage. Directory grouping is a function of naming convention, where objects use / delimiters in their names. For example, an object named `a/example.json` implies there is a directory named `a`. However, if that object is deleted, the `a` directory is also deleted implicitly. To preserve filesystem semantics where the directory can exist without the presence of any files, the HDFS connector creates an actual object whose name ends in / with a path that represents the directory, (that is, create an object named `a/`). Now, deleting `a/example.json` doesn't affect the existence of the `a` directory, because the `a` object maintains its presence. However, it's entirely possible that somebody could delete that `a` object without deleting the files/directories beneath it. The HDFS connector will only delete the folder object if there are no objects beneath that path. The folder object itself is zero bytes.

Inconsistent Filesystem

Deleting a directory means deleting all objects that start with the prefix representing that directory. HDFS allows you to query for the file status of a file or a directory. The file status of a directory is implemented by verifying that the folder object for that directory exists. However, it's possible that the folder object has been deleted, but some of the objects with that prefix still exist. For example, in a situation with these objects:

- `a/b/example.json`
- `a/b/file.json`
- `a/b/

HDFS would know that directory `/a/b/` exists and is a directory, and scanning it would result in `example.json` and `file.json`. However, if object `a/b/` was deleted, the filesystem would appear to be in an inconsistent state. You could query it for all files in directory `/a/b/` and find the two entries, but querying for the status of the actual `/a/b/` directory would result in an exception because the directory doesn't exist. The HDFS connector does not attempt to repair the state of the filesystem.

File Creation

Object Storage supports objects that can be many gigabytes in size. Creating files will normally be done by writing to a temp file and then uploading the contents of the file when the stream is closed. The temp space must be large enough to handle multiple uploads. The temp directory used is controlled by the `hadoop.tmp.dir` configuration property.
Read/Seek Support

When in-memory buffers are enabled (fs.oci.io.read.inmemory), seek is fully supported because the entire file is buffered into a byte array. When in-memory buffer is not enabled (likely because object sizes are large), seek is implemented by closing the stream and making a new range request starting at the specified offset.

Directory Listing

Listing a directory is essentially a List bucket operation with a prefix and delimiter specified. To create an HDFS FileStatus instance for each key, the connector performs an additional HEAD request to get ObjectMetadata for each individual key. This will be required until Object Storage supports richer list operation data.

URI Format for Filesystems and Files

HDFS filesystems and files are referenced through URIs. The scheme specifies the type of filesystem, and the remaining part of the URI is largely free for the filesystem implementation to interpret as it wants.

Because Object Storage is an object store, its ability to name objects as if they were files in a filesystem is used to mimic an actual filesystem.

Root

The root of Object Storage filesystem is denoted by a path where the authority component includes the bucket name and the namespace name, as shown:

Note:

In the examples, "MyBucket" and "MyNamespace" are placeholders and should be replaced with appropriate values.

oci://MyBucket@MyNamespace/

This is always the root of the filesystem. The reason for using authority for both bucket and namespace is that HDFS only allows the authority portion to determine where the filesystem is; the path portion denotes just the path to the resource (so "oci//MyNamespace/MyBucket" won't work, for example). Note that the @ character is not a valid character for buckets or namespaces, and should allow the authority to be parsed correctly.

Sub-directories

Sub-directories do not actually exist, but can be mimicked by creating objects with / characters. For example, two files named a/b/c/example.json and a/b/d/path.json would appear as if they were in a common directory a/b. This would be achieved by using the Object Storage prefix- and delimiter-based querying. In the given example, referencing a sub-directory as a URI would be:

oci://MyBucket@MyNamespace/a/b/

Objects/Files

An object named a/b/c/example.json is referenced as:

oci://MyBucket@MyNamespace/a/b/c/example.json
Logging

Logging in the connector is done through SLF4J. SLF4J is a logging abstraction that allows the use of a user-supplied logging library (e.g., log4j). For more information, see the SLF4J manual.

The following example shows how to enable basic logging to standard output.

1. Download the SLF4J Simple binding jar: SLF4J Simple Binding
2. Add the jar to your classpath
3. Add the following VM arg to enable debug level logging (by default, info level is used):
   
   -Dorg.slf4j.simpleLogger.defaultLogLevel=debug

You can configure more advanced logging options by using the log4j binding.

Sample Hadoop Job

hadoop_sample_hdfs:

```java
package com.oracle.oci.hadoop.example;

import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.net.URI;
import java.net.URISyntaxException;
import org.apache.commons.io.IOUtils;
import org.apache.hadoop.conf.Configuration;
import org.apache.hadoop.fs.FSDataInputStream;
import org.apache.hadoop.fs.FSDataOutputStream;
import org.apache.hadoop.fs.Path;
import org.apache.hadoop.io.IntWritable;
import org.apache.hadoop.io.Text;
import org.apache.hadoop.mapreduce.Job;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import com.oracle.oci.hdfs.BmcFilesystem;
import lombok.RequiredArgsConstructor;

@RequiredArgsConstructor
public class SampleOracleBmcHadoopJob {
    private static final String SAMPLE_JOB_PATH = "/samplehadoopjob";
    private static final String INPUT_FILE = SAMPLE_JOB_PATH + "/input.dat";
    private static final String OUTPUT_DIR = SAMPLE_JOB_PATH + "/output";

    // non-static since this is the runner class it needs to initialize
    after we set the properties
    private final Logger log = LoggerFactory.getLogger(SampleOracleBmcHadoopJob.class);

    /**
     * Runner for sample hadoop job. This expects 3 args: path to
     * configuration file, Object Store namespace, Object
     * Store bucket. To run this, you must:
     * *(@code
     * Create a standard hadoop configuration file
     */
* Create the bucket ahead of time.
*}

* This runner will create a test input file in a file '/
samplehadoopjob/input.dat', and job results will be written
* to '/samplehadoopjob/output'.
* @param args
* 1) path to configuration file, 2) namespace, 3) bucket
* @throws Exception
*/
public static void main(final String[] args) throws Exception
{
    if (args.length != 3)
    {
        throw new IllegalArgumentException(
            "Must have 3 args: 1) path to config file, 2) object
storage namespace, 3) object storage bucket");
    }

    // redirect all logs to sysout
    System.setProperty("org.slf4j.simpleLogger.logFile", "System.out");
    System.setProperty("org.slf4j.simpleLogger.defaultLogLevel", "debug");

    final SampleOracleBmcHadoopJob job = new
    SampleOracleBmcHadoopJob(args[0], args[1], args[2]);
    System.exit(job.execute());
}

private final String configurationFilePath;
private final String namespace;
private final String bucket;

public int execute() throws IOException, ClassNotFoundException,
InterruptedException, URISyntaxException
{
    log.info("Creating hadoop configuration");
    final Configuration configuration =
    this.createConfiguration(this.configurationFilePath);

    final String authority = this.bucket + "@" + this.namespace;
    final String uri = "oci://" + authority;
    log.info("Using uri: ", uri);

    log.info("Creating job inputs");
    this.setup(uri, configuration);

    log.info("Creating job");
    final Job job = this.createJob(configuration);

    final String in = uri + INPUT_FILE;
    final String out = uri + OUTPUT_DIR;
    log.info("Using input: ", in);
    log.info("Using output: ", out);

    FileInputFormat.addInputPath(job, new Path(in));
    FileOutputFormat.setOutputPath(job, new Path(out));

    log.info("Executing job...");
final int response = job.waitForCompletion(true) ? 0 : 1;

log.info("Attempting to read job results");
this.tryReadResult(uri, configuration);
return response;
}

private Configuration createConfiguration(final String configFilePath)
{
    final Configuration configuration = new Configuration();
    configuration.addResource(new Path(configFilePath));
    return configuration;
}

private void setup(final String uri, final Configuration configuration)
throws IOException, URISyntaxException
{
    try (final BmcFilesystem fs = new BmcFilesystem())
    {
        fs.initialize(new URI(uri), configuration);
        fs.delete(new Path(SAMPLE_JOB_PATH), true);
        final FSDataOutputStream output = fs.create(new Path(INPUT_FILE));
        output.writeChars("example
path\ngak\ntest\nexample\ngak\n\ngak");
        output.close();
    }
}

private Job createJob(final Configuration configuration) throws IOException
{
    final Job job = Job.getInstance(configuration, "word count");
    job.setJarByClass(SampleOracleBmcHadoopJob.class);
    job.setMapperClass(SimpleMapper.class);
    job.setCombinerClass(SimpleReducer.class);
    job.setReducerClass(SimpleReducer.class);
    job.setOutputKeyClass(Text.class);
    job.setOutputValueClass(IntWritable.class);
    return job;
}

private void tryReadResult(final String uri, final Configuration configuration)
throws IOException, URISyntaxException
{
    try (final BmcFilesystem fs = new BmcFilesystem())
    {
        fs.initialize(new URI(uri), configuration);
        // this should be the output file name, but that could change
        final FSDataInputStream input = fs.open(new Path(OUTPUT_DIR + "/part-r-00000"));

        final ByteArrayOutputStream baos = new ByteArrayOutputStream();
        IOUtils.copy(input, baos);
        log.info("\n=====
" + baos.toString() + "=====");
        input.close();
    }
}

package com.oracle.oci.hadoop.example;
Troubleshooting

This section contains troubleshooting information for the HDFS connector.

Troubleshooting Service Errors

Any operation resulting in a service error will cause an exception of type com.oracle.bmc.model.BmcException to be thrown by the HDFS connector. For information about common service errors returned by OCI, see API Errors.
Java Encryption Key Size Errors

The HDFS connector can only handle keys of 128 bit or lower key length. Users get "Invalid Key Exception" and "Illegal key size" errors when they use longer keys, such as AES256. Use one of the following workarounds to fix this issue:

- Use a 128 bit key, such as AES128.
- Install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction from the following location: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

Contributions

Got a fix for a bug, or a new feature you'd like to contribute? The SDK is open source and accepting pull requests on GitHub.

Notifications

If you wish to be notified when a new version of the HDFS connector is released, subscribe to the Atom feed.

Questions or Feedback

Ways to get in touch:

- GitHub Issues: To file bugs and make feature requests
- Stack Overflow: Please use the oracle-cloud-infrastructure and oci-hdfs-connector tags in your post
- Developer Tools section of the Oracle Cloud forums
- My Oracle Support

Using the HDFS Connector with Spark

Introduction

This article provides a walkthrough that illustrates using the Hadoop Distributed File System (HDFS) connector with the Spark application framework. For the walkthrough, we use the Oracle Linux 7.4 operating system, and we run Spark as a standalone on a single computer.

Prerequisites

Following are prerequisites for completing the walkthrough:

- You must have permission to launch a Compute instance. For guidance, see Launching an Instance.
- You must be able to connect to the service instance that you've launched. For guidance, see Connecting to an Instance.
- You must have the appropriate OCID, fingerprint, and private key for the Identity and Access Management (IAM) user that you will use to interact with an Object Storage. For guidance, see SDK and Tool Configuration; see also Resource Identifiers.
- You must have an Object Storage bucket that you can connect to.
- The IAM user must be able to read and write to that bucket using the Console.

Using Spark

Install Spark and Dependencies

Note:

For the purpose of this example, install Spark into the current user's home directory. Note that for production scenarios, you would not do this.

Note:

Versions 2.7.7.0 and later no longer install all of the required third party dependencies. Required third party dependencies are bundled under the
1. Launch an instance of your Compute service. For guidance, see Launching an Instance.
2. Ensure that your service instance has a public IP address so that you can connect using a Secure Shell (SSH) connection. For guidance, see Instance Console Connections.
3. Connect to your service instance using an SSH connection.
4. Install Spark and its dependencies, Java and Scala, by using the code examples that follow.

```bash
# We'll use wget to download some of the artifacts that need to be installed
sudo yum install wget

# First install Java
sudo yum install java-1.8.0-openjdk.x86_64
export JAVA_HOME=/usr/lib/jvm/jre-1.8.0-openjdk
# Should be something like: OpenJDK Runtime Environment (build 1.8.0_161- b14)
java -version

# Then install Scala
sudo yum install scala-2.12.4.rpm
# Should be something like: Scala code runner version 2.12.4 -- Copyright 2002-2017, LAMP/EPFL and Lightbend, Inc.
scala -version

# Then download Spark
wget https://archive.apache.org/dist/spark/spark-2.2.1/spark-2.2.1-bin-hadoop2.7.tgz
tar xvf spark-2.2.1-bin-hadoop2.7.tgz
export SPARK_HOME=$HOME/spark-2.2.1-bin-hadoop2.7
export PATH=$PATH:$SPARK_HOME/bin

# Start a Spark master
cd $SPARK_HOME
./sbin/start-master.sh
```

Download the HDFS Connector and Create Configuration Files

**Note:**

For the purposes of this example, place the JAR and key files in the current user's home directory. For production scenarios you would instead put these files in a common place that enforces the appropriate permissions (that is, readable by the user under which Spark and Hive are running).

Download the HDFS Connector to the service instance and add the relevant configuration files by using the following code example. For additional information, see HDFS Connector for Object Storage https://docs.cloud.oracle.com/Content/API/SDKDocs/hdfsconnector.htm?Highlight=hdfs.

```bash
wget https://github.com/oracle/oci-hdfs-connector/releases/download/v2.9.2.1/oci-hdfs.zip
unzip oci-hdfs.zip -d oci-hdfs

cd $HOME
mkdir .oci
# Create or copy your API key into the $HOME/.oci directory

cd $SPARK_HOME/conf
# Create a core-site.xml (e.g. by transferring one you have, using vi etc.). Consult
```
# https://docs.cloud.oracle.com/Content/API/SDKDocs/hdfsconnector.htm#two
# for what this should look like

cp spark-defaults.conf.template spark-defaults.conf

In the spark-defaults.conf file, add the following at the bottom:

```bash
cp spark-defaults.conf.template spark-defaults.conf
```

**Prepare Data**

For testing data, we will use the MovieLens data set.

2. Unzip the download file.
3. Upload the movies.csv file to your Object Storage bucket.

**Test Using the Spark Shell**

With the data ready, we can now launch the Spark shell and test it using a sample command:

```bash
  cd $SPARK_HOME
  ./bin/spark-shell
```

```
scala> sc.wholeTextFiles("oci://PipedUploadTest@sampletenancy/")
java.io.IOException: No FileSystem for scheme: oci
```

You receive an error at this point because the oci:// file system schema is not available. We need to reference the JAR file before starting the Spark shell. Here's an example for doing so:

```bash
  ./bin/spark-shell --jars $HOME/oci-hdfs/lib/oci-hdfs-full-1.2.7.jar --
driver-class-path $HOME/oci-hdfs/lib/oci-hdfs-full-1.2.7.jar
```

```bash
scala> sc.wholeTextFiles("oci://PipedUploadTest@sampletenancy/")
res0: org.apache.spark.rdd.RDD[(String, String)] = oci://
PipedUploadTest@sampletenancy/ MapPartitionsRDD[1] at wholeTextFiles at
<console>:25
```

```bash
scala> sc.textFile("oci://PipedUploadTest@sampletenancy/
movies.csv").take(20).foreach(println)
```

```
movieId,title,genres
1,Toy Story (1995),Adventure|Animation|Children|Comedy|Fantasy
2,Jumanji (1995),Adventure|Children|Fantasy
3,Grumpier Old Men (1995),Comedy|Romance
4,Waiting to Exhale (1995),Comedy|Drama|Romance
5,Father of the Bride Part II (1995),Comedy
6,Heat (1995),Action|Crime|Thriller
7,Sabrina (1995),Comedy|Romance
8,Tom and Huck (1995),Adventure|Children
9,Sudden Death (1995),Action
10,GoldenEye (1995),Action|Adventure|Thriller
11,"American President, The (1995)",Comedy|Drama|Romance
12,Dracula: Dead and Loving It (1995),Comedy|Horror
13,Balto (1995),Adventure|Animation|Children
14,Nixon (1995),Drama
15,Cutthroat Island (1995),Action|Adventure|Romance
16,Casino (1995),Crime|Drama
17,Sense and Sensibility (1995),Drama|Romance
18,Four Rooms (1995),Comedy
```
The command is successful so we are able to connect to Object Storage. Note that if you do not wish to pass the --jars argument each time the command executes, you can instead copy the oci-hdfs-full JAR file into the $SPARK_HOME/jars directory.

**Start the Spark Thrift Server**

Start the Spark Thrift Server on port 10015 and use the Beeline command line tool to establish a JDBC connection and then run a basic query, as shown here:

```bash
cd $SPARK_HOME
./sbin/start-thriftserver.sh --hiveconf hive.server2.thrift.port=10015
```

Once the Spark server is running, we can launch Beeline, as shown here:

```bash
cd $SPARK_HOME
./bin/beeline
```

Beeline version 1.2.1.spark2 by Apache Hive

```
beeline>
```

Next, connect to the server, as shown here:

```
beeline> !connect jdbc:hive2://localhost:10015 testuser testpass
```

None exist presently; however, we can create a table and link it to the movies.csv file that we downloaded and placed in the Object Storage bucket, as shown here:

```
0: jdbc:hive2://localhost:10015> create table test_table (movieId integer, title string, genres string) using csv options (path "oci://myBucket@myTenant/movies.csv", header "true", delimiter ",");
```

```
0: jdbc:hive2://localhost:10015> describe formatted test_table;
```

For the purposes of this example, we have not configured any security, so any user name and password will be accepted. For production scenarios you would not do this.
<table>
<thead>
<tr>
<th>col_name</th>
<th>comment</th>
<th>data_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>movieId</td>
<td></td>
<td>int</td>
</tr>
<tr>
<td>title</td>
<td></td>
<td>string</td>
</tr>
<tr>
<td>genres</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

# Detailed Table Information

<table>
<thead>
<tr>
<th>Database</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>test_table</td>
</tr>
<tr>
<td>Owner</td>
<td>opc</td>
</tr>
<tr>
<td>Created</td>
<td>Thu Mar 01 20:45:18 GMT 2018</td>
</tr>
<tr>
<td>Last Access</td>
<td>Thu Jan 01 00:00:00 GMT 1970</td>
</tr>
<tr>
<td>Type</td>
<td>EXTERNAL</td>
</tr>
<tr>
<td>Provider</td>
<td>csv</td>
</tr>
</tbody>
</table>

| Location          | oci://PipedUploadTest@sampletenancy/movies.csv |
| Serde Library     | org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe |
| InputFormat       | org.apache.hadoop.mapred.SequenceFileInputFormat |
| OutputFormat      | org.apache.hadoop.hive.ql.io.HiveSequenceFileOutputFormat |

| Storage Properties | [delimiter=,, header=true, serialization.format=1] |

Note that the table stores its data externally in Object Storage and the data can be accessed using the HDFS Connector (the oci:// file system scheme). Now that we have a table, we can query it:

```sql
0: jdbc:hive2://localhost:10015> select * from test_table limit 10;
+----------+-------------------------------------+-------------------------------------+
<table>
<thead>
<tr>
<th>movieId</th>
<th>title (1995)</th>
<th>genres</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Toy Story (1995)</td>
<td>Adventure</td>
</tr>
<tr>
<td>2</td>
<td>Jumanji (1995)</td>
<td>Adventure</td>
</tr>
<tr>
<td>3</td>
<td>Grumpier Old Men (1995)</td>
<td>Comedy</td>
</tr>
<tr>
<td>4</td>
<td>Waiting to Exhale (1995)</td>
<td>Comedy</td>
</tr>
<tr>
<td>5</td>
<td>Father of the Bride Part II (1995)</td>
<td>Comedy</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Sabrina (1995)</td>
<td>Comedy</td>
<td>Romance</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Tom and Huck (1995)</td>
<td>Adventure</td>
<td>Children</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Sudden Death (1995)</td>
<td>Action</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information

- HDFS Connector for Object Storage
- Overview of Object Storage
- Apache Spark

**Toolkit for Eclipse**

The Oracle Cloud Infrastructure Toolkit for Eclipse is an open source plug-in for the Eclipse Integrated Development Environment (IDE). The toolkit provides a set of features that help developers connect to Oracle Cloud Infrastructure from within Eclipse. For example, you can use the toolkit to deploy an application to a VM in the cloud by using the Oracle Container Engine for Kubernetes, or upload multiple files to Object Storage with one click. The Compute feature enables you to start a compute instance or restart it if needed. You can also switch between multiple accounts and regions from the Eclipse IDE.

**Download**: To install the Toolkit, download the `com.oracle.oci.eclipse.zip` toolkit from the releases section on GitHub, then follow the instructions in Getting Started with Toolkit for Eclipse on page 4364.

**Requirements**

To use the Oracle Cloud Infrastructure Toolkit for Eclipse, you must have the following:

- An Oracle Cloud Infrastructure account
- A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users on page 57. For a list of typical policies you may want to use, see Common Policies on page 2142.
- A key pair used for signing API requests, with the public key uploaded to Oracle. For more information on generating and uploading keys, see Required Keys and OCIDs on page 4179.
- SDK for Java on page 4225
- Eclipse IDE for Java Developers 4.3 or later

**Services Supported**

- Compute
- Object Storage
- Autonomous Database
- Container Engine for Kubernetes

**Contact Us**

**Contributions**

Got a fix for a bug or a new feature you’d like to contribute? The plug-in is open source and accepting pull requests on GitHub.

**Notifications**

To be notified when a new version of the toolkit is released, subscribe to the Atom feed.
Questions or Feedback

- GitHub Issues: To file bugs and feature requests only
- Developer Tools section of the Oracle Cloud forums
- My Oracle Support

Getting Started with Toolkit for Eclipse

Downloading the Toolkit

You can download the `com.oracle.oci.eclipse.zip` toolkit from the releases section on GitHub.

Installing the Toolkit

After downloading the toolkit, launch the Eclipse IDE.

1. From the top navigation bar, select Help > Install New Software...
2. In Install dialog, click Add...
3. In the Add Repository dialog, click Archive...
4. In the right pane of the Repository Archive window, select the zip file containing the toolkit. Click Open.
5. In the Add Repository dialog click Add.
6. In the Available Software dialog, select Oracle Cloud Infrastructure Toolkit for Eclipse, then click Next.
7. In the Install Details dialog, click Finish.

Configuring the Toolkit

Oracle Cloud Infrastructure Preferences

Before you can use the toolkit, you must configure the Oracle Cloud Infrastructure Preferences in the Eclipse IDE. This process will provide the necessary identifiers and credentials so the toolkit can connect to your Oracle Cloud Infrastructure account. For more information, see Required Keys and OCIDs on page 4179.

1. From the top navigation bar, select Preferences > Oracle Cloud Infrastructure Preferences.
2. For Profile Name, provide a short descriptive name.
3. From the Region dropdown, select your region.
4. Enter your User OCID and Tenancy OCID. For information on how to locate this information, see Where to Get the Tenancy's OCID and User's OCID on page 4184.
5. For Key File, click Browse and select the appropriate file. For more information, see How to Generate an API Signing Key on page 4180.
6. Enter the Fingerprint for the Key File. For more information, see How to Get the Key's Fingerprint on page 4183.
7. Enter the Passphrase, if you created one for the key pair. If not, leave this field blank.
8. Click Save Profile.
9. Click Apply and Close.

Proxy Settings

If you are on a network that uses a proxy to connect to the internet, you must configure Eclipse proxy settings. For more information, see Network Connections in the Eclipse IDE Documentation.

Uninstalling the Toolkit

Launch the Eclipse IDE.

1. From the top navigation bar, select Help > About Eclipse IDE
2. Click Installation Details.
3. In the Installation Details window, select the Installed Software tab.
4. Select Oracle Cloud Infrastructure Toolkit for Eclipse and click Uninstall...
5. In the Uninstall dialog, confirm the items to be uninstalled then click Finish.
6. Click **Restart**.

**Using Toolkit for Eclipse**

After configuring the **Oracle Cloud Infrastructure Preferences** on page 4364, you can connect to your tenancy via Eclipse and use the Oracle Cloud Infrastructure Explorer to view and update your resources. You can also switch between different accounts saved in the profile.

To change the region, click the region icon in the Explorer navigation bar and select from the dropdown.

To change the compartment, click the compartment icon and select from the dropdown.

**Using the Toolkit for Eclipse with Compute Instances**

In the Oracle Cloud Infrastructure Explorer, double-click **Compute** to view available resources.

Double-click **Instances** to display a list of instances. You can right-click each one in the list to start, stop, or reboot it.

You can also double-click **Block Volumes** to view a list of block volumes.

**Using the Toolkit for Eclipse with Object Storage**

In the Oracle Cloud Infrastructure Explorer, double-click **Object Storage** to view available resources.

**Working with Buckets**

To create a bucket, right-click **Object Storage** and select **Create New Bucket**.

To view content and details, double-click or right-click the bucket and select **Open Bucket**.

To delete a bucket, view the bucket's details and click **Delete Bucket**.

**Working with Objects**

To upload an object, select the destination bucket and view its details. Right-click the Object list and select **Upload Object**. You can also drag one or more files to the Object list to upload.

To download one or more objects, right-click and select **Download Object**.

To delete one or more objects, right-click and select **Delete Object**.

**Deploy Applications using Oracle Container Engine for Kubernetes**

**Prerequisites**

1. Install **Docker Desktop v2.2.0.0** or higher.
2. Verify that Docker desktop is running, and that the Docker CLI client and Kubernetes CLI client (kubectl) are available in the command line.
3. Install the **Oracle Cloud Infrastructure command line client (OCI CLI)**.
4. Verify that OCI CLI works by typing “oci” on command prompt. This should return a list of all the services supported by OCI CLI.

**Deploy an Application to Container Engine for Kubernetes**

1. In the Oracle Cloud Infrastructure Explorer, double-click **Container Engine for Kubernetes**.
2. Double-click **Container Cluster (OKE)** to display a list of available clusters. A cluster should be created prior to this step in the console.
3. Right click on the cluster name and select **Deploy Docker Image to OKE**.
4. Follow the deployment wizard steps to to deploy the application.

**Oracle Developer Tools for Visual Studio**

The Oracle Developer Tools for Visual Studio provide a set of features that helps developers connect to Oracle Cloud Infrastructure from within the Microsoft Visual Studio IDE. You can **use the tools to view and manage your Oracle**
Databases and Oracle Autonomous Databases in Oracle Cloud Infrastructure and quickly and easily deploy a web application to Oracle Cloud Infrastructure Container Engine for Kubernetes.

Requirements

To use the Oracle Developer Tools for Visual Studio, you must have the following:

• An Oracle Cloud Infrastructure account
• A user created in that account, in a group with a policy that grants the desired permissions. This can be a user for yourself, or another person/system that needs to call the API. For an example of how to set up a new user, group, compartment, and policy, see Adding Users on page 57. For a list of typical policies you may want to use, see Common Policies on page 2142.
• A key pair used for signing API requests, with the public key uploaded to Oracle. For more information on generating and uploading keys, see Required Keys and OCIDs on page 4179.
• The Oracle Cloud Infrastructure Command Line Interface (CLI) on page 4192 installed and configured.
• Microsoft Visual Studio 2019 or later
• Docker Desktop v2.2.0.0 or higher

Contact Us

Questions or Feedback

For questions or to provide feedback, please use one of the following resources:

• The Developer Tools section of the Oracle Cloud forums
• My Oracle Support

Getting Started with Oracle Developer Tools for Visual Studio

Installing the Extension

The Oracle Developer Tools for Visual Studio is available in the Visual Studio Marketplace.

1. From the Visual Studio menu, select Extensions->Manage Extensions
2. From the list on the left side of the dialog, select Online and then Visual Studio Marketplace
4. Click on the Download button next to the extension.
5. A browser window opens with instructions to download the installer.

Configuring the Toolkit

Oracle Developer Tools for Visual Studio Preferences

Before you can use the developer tools, you must configure the Oracle Cloud Infrastructure Preferences. This process will provide the necessary identifiers and credentials so the developer tools can connect to your Oracle Cloud Infrastructure account. For more information, see Required Keys and OCIDs on page 4179.

1. The deployment wizard requires an Oracle Cloud Infrastructure user credentials configuration file. For more information, see SDK and CLI Configuration File on page 4184.
2. Run the “docker desktop” app, and ensure it has the Linux Containers option selected.
3. If behind a proxy, set the proxy values http_proxy and https_proxy in the environment variables for Windows and in the Docker Desktop settings (see the Resources->Proxies menu).

Uninstalling the Toolkit

1. From the Visual Studio menu, select Extensions, then Manage Extensions.
2. From the list on the left side of the dialog, select Installed.
3. Select "Oracle Developer Tools for Visual Studio 2019" from the middle menu and click on the Uninstall button that appears next to it.
Using the Oracle Developer Tools for Visual Studio

This topic shows how to use the Oracle Developer Tools for Visual Studio's Deployment wizard to deploy a web application to Oracle Cloud Infrastructure Container Engine for Kubernetes.

Note:
The Oracle Developer Tools for Visual Studio has additional functionality that is not covered in this document. For more information, see Oracle Developer Tools for Visual Studio.

Prerequisites

This topic assumes a working knowledge of OCI Container Engine for Kubernetes. The tutorials below will help understand some of the technologies and backend framework used by the wizard for deployment.

- Pushing an Image to Oracle Cloud Infrastructure Registry
- Creating a Cluster with Oracle Cloud Infrastructure Container Engine for Kubernetes
- Deploying an Application to OKE

Overview

Using the Oracle Developer Tools for Visual Studio assumes you've already created a docker image for your application. This workflow generally looks like this:

- Build your web application.
- Build a docker image for your application locally. For more information, see the Docker documentation.
- Push the docker image of the web application to the Oracle Cloud Infrastructure Registry. For more information on pushing a docker image to OCIR, see Push an Image to Oracle Cloud Infrastructure Registry.
- Create a cluster in Oracle Cloud using Oracle Container Engine Service for Kubernetes. See Create a Cluster with Oracle Cloud Infrastructure Container Engine for Kubernetes and download the resulting kubeconfig file.
- Create a named secret containing OCI credentials to be used for Kubernetes deployment. For more information, see Pull an Image from Oracle Cloud Infrastructure Registry when Deploying a Load-Balanced Application to a Cluster.

Deploy an Application Using the Oracle Deployment Wizard

1. From the Visual Studio Extensions menu, select Oracle Cloud App Deployment -> Deploy to Oracle Cloud. The Oracle Deployment Wizard displays.
2. Click Next.
3. Select an Authentication Profile (make sure that this profile matches the OCI CLI profile) and click Next.
4. Select a deployment option:

   a. **Redeploy using an existing deployment configuration:** This deployment choice should be used for re-deployment of a web application when there are no deployment configuration changes. If the developer needs to make changes only to his/her web application and then re-deploy, they can do so using this option. This option allows developers to do quick deployment in a few clicks with no new information asked for.

   b. **Redeploy with a different deployment configuration:** This deployment choice should be used for re-deployment of a web application when there are deployment configuration changes. Scenarios where this is an
appropriate choice include deploying on a different cluster, using a different Docker image, or a change in the Kubernetes configuration.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If selecting a different cluster during re-deployment, delete the Kubernetes resources for your previous deployment using the &quot;kubectl delete&quot; command.</td>
</tr>
</tbody>
</table>

c. Create a new deployment: Use this option when deploying your web application for the first time using this wizard. The name for this deployment should be unique, must be no longer than 63 characters, must start and end with a lowercase letter or number, and may contain lowercase letters, numbers, and hyphens.

5. On the Select A Cluster panel, select an existing Kubernetes cluster from any of the compartments in your tenancy (the wizard does not support creating a cluster, so you should create a cluster using the console first). Click Next.

6. On the Specify Deployment Details panel, you can modify existing deployment details.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The deployment file created by the wizard can be modified in any editor and used for re-deployments using the wizard.</td>
</tr>
</tbody>
</table>

   a. Select a Docker image from the drop-down list.

   b. Select a Kubernetes Secret Name from the drop-down list.

7. Click Next.

8. Verify your deployment details, and then click Deploy. The window will actively update with the deployment status as it progresses. You can dismiss this dialog and check the deployment status later by selecting Oracle Cloud App Deployment -> Check Deployment Status from the Visual Studio menu.

Deleting A Deployment

The wizard doesn't support deleting a deployment using the Visual Studio IDE. To delete a deployment:

1. Delete the deployment from the OKE cluster using the following command: `kubectl delete -f <path-to-deployment-file> --kubeconfig <path-to-kubeconfig-file>` If the deployment file is not present, you can use the following command: `kubectl delete deploy/<deployment_name> svc/<service_name>`

2. Delete the folder in `~/.oci/visualstudiowebapps/<your-application-deployment-name>` from the client machine.

Appendix and Reference

This section covers general SDK concepts and references.

- REST APIs on page 4368
- Client-Side Encryption on page 4393 - Discusses how client-side encryption works for the Oracle Cloud Infrastructure SDK for Python and the SDK for Java.

REST APIs

The Oracle Cloud Infrastructure APIs are typical REST APIs that use HTTPS requests and responses. This topic describes basic information about using the APIs.

API Reference and Endpoints

For links to the Oracle Cloud Infrastructure API reference and a list of the regional API endpoints, see API Reference and Endpoints.
API Version

The base path of the endpoint includes the desired API version (for example, 20160918). Here's an example for a POST request to create a new VCN in the Ashburn region:

```
POST https://iaas.us-ashburn-1.oraclecloud.com/20160918/vcns
```

Request Signing Required

All Oracle Cloud Infrastructure API requests must be signed for authentication purposes. For information about the required credentials and how to sign the requests, see Request Signatures on page 4383.

HTTPS and TLS 1.2 Required

All Oracle Cloud Infrastructure API requests must support HTTPS and SSL protocol TLS 1.2.

Maximum Allowed Client Clock Skew

HTTP status code 401 (NotAuthenticated) is returned if the client's clock is skewed more than 5 minutes from the server's. To determine the server's clock time, use this curl command with the API endpoint:

```
curl -s --head <endpoint> | grep Date
```

For example:

```
curl -s --head https://iaas.us-phoenix-1.oraclecloud.com | grep Date
```

Request and Response Format

The Oracle Cloud Infrastructure APIs use standard HTTP requests and responses. Each may contain Oracle-specific headers for pagination, entity tags (ETags), and so on as described elsewhere in this topic and in the API documentation.

Each response includes a unique Oracle-assigned request ID (for example, bb3f3275-f356-462a-93c4-bf40fb82bb02) in the opc-request-id response header. If you need to contact Oracle about a particular request, please provide this request ID.

Many of the API operations require JSON in the request body or return JSON in the response body. The specific contents of the JSON are described in the API documentation for the individual operation. Notice that the JSON is not wrapped or labeled according to the operation's name or the object's name or type.

**Note:**

Make sure to set the Content-Type header to application/json in your POST and PUT requests that contain JSON in the body.

Example CreateVcn Request

```
POST https://iaas.us-phoenix-1.oraclecloud.com/20160918/vcns
host: iaas.us-phoenix-1.oraclecloud.com
opc-retry-token: 239787fs987
Content-Type: application/json
HTTP headers required for authentication
Other HTTP request headers per the HTTP spec
{
  "compartmentId": "ocid1.compartment.oc1..aaaaaaauwjnv47knr7uuvqar5bshnspi6xoxsfebh3vy72fi4swgrkvuvq",
  "displayName": "Apex Virtual Cloud Network",
  "cidrBlock": "172.16.0.0/16"
}
```
Example CreateVcn Response

```
200 OK
opc-request-id: 6c4d01a6-f764-4325-a3f8-720c8b5cae7b
{
    "id": "ocid1.vcn.oc1.phx.aaaaaaaa4ex5pqjtkjhd4h4gcnk07vx5uto5puj5noa5awznspwjt3pqyq",
    "compartmentId": "ocid1.compartment.oc1..aaaaaaaauwjnv47knr7uuuvqar5bshnspl6oxosfbeb3vy72fi4swgrkvuvq",
    "displayName": "Apex Virtual Cloud Network",
    "cidrBlock": "172.16.0.0/16"
    "defaultRouteTableId": "ocid1.routetable.oc1.phx.aaaaaaaaba3pv6wkr4jqaee5f44n2b2m2yt2j6rx32uzr4h25vqstifsfsdq",
    "defaultSecurityListId": "ocid1.securitylist.oc1.phx.aaaaaaaac6h4ckr3ncbxmvminfvzjbr7owu5hfzbtu33kfe7hgcs5fj",
    "defaultDhcpOptionsId": "ocid1.dhcpoptions.oc1.phx.aaaaaaaawglzn7s5sogyfzn125a4vxgu76c2hrvzyd3psn6vcx331zmu2xx",
    "state": "PROVISIONING",
    "timeCreated": "2016-07-22T17:43:01.389+0000"
}
```

Error Format

If a request results in an error, the response contains a standard HTTP response code with 4xx for client errors and 5xx for server errors. The body also includes JSON with an error code and a description of the error. For example:

```
{
    "code": "InvalidParameter",
    "message": "Description may not be empty; description size must be between 1 and 400"
}
```

For a list of common errors across all services, see API Errors.

Request Throttling

Oracle Cloud Infrastructure applies throttling to many API requests to prevent accidental or abusive use of resources. If you make too many requests too quickly, you might see some succeed and others fail. Oracle recommends that you implement an exponential back-off, starting from a few seconds to a maximum of 60 seconds. When a request fails due to throttling, the system returns response code 429 and the following error code and description:

```
{
    "code": "TooManyRequests",
    "message": "User-rate limit exceeded."
}
```

Polling for Resource Status

Most Oracle Cloud Infrastructure resources, such as compute instances, have lifecycles. In many cases, you want your code to wait until a resource or work request reaches a specific state, or a timeout is exceeded, before taking further action.

You can poll a resource to determine its state. For example, when you call GetInstance, the response body contains an instance resource that includes the lifecycleState attribute. You might want your code to wait until the instance's lifecycleState is RUNNING before proceeding.

Different resources take different amounts of time to transition between states. Therefore, the optimal frequency and duration parameters for a polling strategy can vary among resources. The Oracle Cloud Infrastructure SDK waiters use the following default strategy:

- Use an exponential back-off, starting from a few seconds to a maximum of 30 seconds between poll attempts.
- Poll up to 20 minutes, and then stop.
Or more information on waiters, see:

- SDK for Java waiters documentation
- SDK for Ruby waiters documentation

**Where to Find Your Tenancy's OCID**

If you use the API, you'll need your tenancy's OCID in order to sign the requests (see Request Signatures on page 4383). You'll also need it for some of the IAM API operations. An OCID is an Oracle Cloud ID (see Resource Identifiers).

Get the tenancy OCID from the Oracle Cloud Infrastructure Console on the Tenancy Details page:

1. Open the Profile menu and click Tenancy: `<your_tenancy_name>`.
2. The tenancy OCID is shown under Tenancy Information. Click Copy to copy it to your clipboard.

The tenancy OCID looks something like this (notice the word "tenancy" in it):

`ocid1.tenancy.oc1..<unique_ID>`.

**List Pagination**

Most List operations paginate results. For example, results are paginated for the ListInstances operation in the Core Services API. When you call a paginated List operation, the response indicates more pages of results by including the `opc-next-page` header.

**Note:**

A page can be empty even when more results remain. Anytime the `opc-next-page` header appears, there are more list items to get. For more information about resource list control, see Overview of Search on page 3626.

List pagination for Object Storage ListObjects works differently because the pagination controls are also used for object name filtering. ListObjects returns nextStartWith instead of `opc-next-page` in the response body. To paginate through more objects, use the returned `nextStartWith` value with the start parameter. To filter which objects ListObjects returns, use the start and end parameters.

To get the next page of results

Make a new GET request against the same URL, modified by setting the page query parameter to the value from the `opc-next-page` header. Repeat this process until you get a response without an `opc-next-page` header. The absence of this header indicates that you have reached the last page of the list.
Note:

For an alternative to writing pagination code, see the functions in the pagination module provided with the SDK for Python.

To get the previous page of results

(Available with some APIs.) Make a new GET request against the same URL, modified by setting the page query parameter to the value from the opc-prev-page header. Repeat this process until you get a response without an opc-prev-page header. The absence of this header indicates that you have reached the first page of the list.

Note:

For an alternative to writing pagination code, see the functions in the pagination module provided with the SDK for Python.

To change the maximum number of results per page

In the GET request, set the limit to the number of items you want returned in the response.

Note:

The service will return no more than the number specified as limit, but might not return that exact number.

Retry Token

For some operations you can provide a unique retry token (opc-retry-token) so the request can be retried in case of a timeout or server error without the risk of executing that same action again. The token expires after 24 hours, but can be invalidated before then due to conflicting operations (for example, if a resource has been deleted and purged from the system, then a retry of the original creation request may be rejected).

ETags for Optimistic Concurrency Control

The API supports etags for the purposes of optimistic concurrency control. The GET and POST calls return an etag response header with a value you should store. When you later want to update or delete the resource, set the if-match header to the ETag you received for the resource. The resource will then be updated or deleted only if the ETag you provide matches the current value of that resource's ETag.

Null vs. Empty Strings for Optional Parameters

If you send an empty string (""") as the value of an optional parameter, the API validates the value as normal (for example, checks against minimum and maximum allowed length, and so on). Often the minimum allowed length is 1, so an error would be returned. If you don't set the value (it's null), the API performs no validation, and some other action may occur. For example: if you don't set a value for the displayName when creating a new VCN object, the service will auto-generate a value.

API Errors

Common Errors Returned by All Services

The following table lists the common errors returned by all the services for Oracle Cloud Infrastructure.

<table>
<thead>
<tr>
<th>HTTP Status Code</th>
<th>Error Code</th>
<th>Description</th>
<th>Retry</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>CannotParseRequest</td>
<td>The request is incorrectly formatted.</td>
<td>No.</td>
</tr>
<tr>
<td>400</td>
<td>InvalidParameter</td>
<td>A parameter is invalid or incorrectly formatted.</td>
<td>No.</td>
</tr>
<tr>
<td>400</td>
<td>LimitExceeded</td>
<td>Fulfilling this request exceeds the Oracle-defined limit for this tenancy for this resource type.</td>
<td>No.</td>
</tr>
<tr>
<td>400</td>
<td>MissingParameter</td>
<td>A required parameter is missing.</td>
<td>No.</td>
</tr>
<tr>
<td>HTTP Status Code</td>
<td>Error Code</td>
<td>Description</td>
<td>Retry</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>400</td>
<td>QuotaExceeded</td>
<td>Fulfilling this request exceeds the administrator-defined quota for this compartment for this resource.</td>
<td>No.</td>
</tr>
<tr>
<td>400</td>
<td>RelatedResourceNotAuthorizedOrNotFound</td>
<td>A resource specified in the body of the request was not found, or you do not have authorization to access that resource.</td>
<td>Yes, with backoff.</td>
</tr>
<tr>
<td>401</td>
<td>NotAuthenticated</td>
<td>The required authentication information was not provided or was incorrect. There are other reasons why this error code is generated. For more information, see HTML Status Code 401.</td>
<td>Yes, with backoff.</td>
</tr>
<tr>
<td>402</td>
<td>SignUpRequired</td>
<td>This operation requires opt-in before it may be called.</td>
<td>No.</td>
</tr>
<tr>
<td>403</td>
<td>NotAuthorized</td>
<td>You do not have authorization to update one or more of the fields included in this request.</td>
<td>No.</td>
</tr>
<tr>
<td>404</td>
<td>NotAuthorizedOrNotFound</td>
<td>A resource specified via the URI (path or query parameters) of the request was not found, or you do not have authorization to access that resource. For more information, see HTML Status Code 404.</td>
<td>Yes, with backoff.</td>
</tr>
<tr>
<td>404</td>
<td>NotFound</td>
<td>There is no operation supported at the URI path and HTTP method you specified in the request.</td>
<td>No.</td>
</tr>
<tr>
<td>405</td>
<td>MethodNotAllowed</td>
<td>The target resource does not support the HTTP method.</td>
<td>No.</td>
</tr>
<tr>
<td>409</td>
<td>IncorrectState</td>
<td>The requested state for the resource conflicts with its current state.</td>
<td>Yes, with backoff. Refer to the error description for any required actions before you retry.</td>
</tr>
<tr>
<td>409</td>
<td>InvalidatedRetryToken</td>
<td>The provided retry token was used in an earlier request that resulted in a system update, but a subsequent operation invalidated the token. This can happen, for example, in cases where an entity created with the same token has since been deleted. If the system state change that is associated with this request should be performed again, retry it using a different token.</td>
<td>No.</td>
</tr>
<tr>
<td>409</td>
<td>NotAuthorizedOrResourceAlreadyExists</td>
<td>You do not have authorization to perform this request, or the resource you are attempting to create already exists. This error code is returned only from create operations, where it is returned instead of the more general NotAuthorizedOrNotFound error code.</td>
<td>Yes, with backoff.</td>
</tr>
<tr>
<td>412</td>
<td>NoEtagMatch</td>
<td>The ETag specified in the request does not match the ETag for the resource.</td>
<td>No.</td>
</tr>
</tbody>
</table>
### Error Details and Troubleshooting

#### HTTP status code: 401

- **Missing or incorrect authentication information.** Verify that all the required information (tenant OCID, user OCID, fingerprint, and private key) is provided and accurate. Verify that the public key corresponding to the fingerprint has been uploaded for the user. For more information, see [Required Keys and OCIDs](#) on page 4179.
- **Clock skew.** This status code is returned if the client's clock is skewed more than five (5) minutes from the server's clock. For more information, see [Maximum Allowed Client Clock Skew](#) on page 4369.
- **API request signature error.** This status code is returned if a required header is missing from a signing string. For more information, see [Request Signatures](#) on page 4383.

#### Error Codes: NotAuthorizedOrNotFound, RelatedResourceNotAuthorizedOrNotFound, NotAuthorizedOrResourceAlreadyExists

- **Authorization error.** Verify that the user is in a group that has the permissions to work with resources in a compartment.
- **Compartment or resource not found.** Verify that the compartment or resource exist and is referenced correctly. For example, this status code is returned for either of the following errors:
  - **CompartmentNotFoundException** if a compartment doesn't exist
  - **VolumeNotFoundException** if a volume doesn't exist

### Asynchronous Work Requests

This topic describes asynchronous work requests for long-running operations against Oracle Cloud Infrastructure services. It also provides guidance on obtaining request status, and for inspecting the request response to enable filtering for affected resources.

#### Overview

API calls to Oracle Cloud Infrastructure services can launch long-running operations that do not complete the client's request before a response is returned. In these cases, the service spawns an asynchronous work request that allows for visibility into the progress of long-running, asynchronous operations. The response to the REST API call contains a work request ID in the `opc-work-request-id` header, which allows you to monitor its progress and status. The work request itself remains in a queue until the operation has completed.

You can monitor the status of the work request at any time by calling `GetWorkRequest` and passing in the work request ID.
Note:

The Compute, Data Catalog, and Database services support work requests using Work Requests API, which contains the GetWorkRequest operation.

Other services that support work requests use operations in the service APIs. These service APIs each include operations that work in a similar manner to the GetWorkRequest operation used by the Work Requests API.

Two features of the request response are of particular interest: the status of the work request, and a list of the resources that are affected by the work request. The status is important because asynchronous work requests must know when an operation has completed, is still running, or whether it has failed altogether.

To retrieve information about work request failures or errors, each service provides APIs for fetching information about errors, and logs. For links to API reference documentation for each of the service, see the section For More Information on page 4383.

Also important in cases where a work request operation affects several resources is having a list of the resources that a work request affects, along with each one's entityType and actionType attributes.

Work Request Status

Asynchronous work requests allow you to monitor their progress by providing a status attribute on the WorkRequest object. Each of the supported services provides its own API for obtaining status, as listed in the following sections.

Note:

There is a ContainerEngineWaiters class that allows you to create a callback using the forWorkRequest method. Use this API to forward a notification when an operation's status changes, for example, from IN_PROGRESS to COMPLETED.

The following table lists status attributes that are supported by the WorkRequest object on the respective services.

<table>
<thead>
<tr>
<th>Service</th>
<th>Status Attributes</th>
</tr>
</thead>
</table>
| Application Migration | • ACCEPTED  
|                     | • IN_PROGRESS  
|                     | • SUCCEEDED  
|                     | • FAILED  
|                     | • CANCELING  
|                     | • CANCELED  |
| Big Data | • CREATING  
| | • ACTIVE  
| | • UPDATING  
| | • SUSPENDING  
| | • SUSPENDED  
| | • RESUMING  
| | • DELETING  
| | • DELETED  
<p>| | • FAILED  |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Status Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain Platform</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Compute</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Container Engine for Kubernetes</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Content and Experience</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Data Catalog</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Data Integration</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Data Science</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td>Service</td>
<td>Status Attributes</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Database</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCEEDED</td>
</tr>
<tr>
<td>IAM</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>• CREATING</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• ACTIVE</td>
</tr>
<tr>
<td></td>
<td>• DELETING</td>
</tr>
<tr>
<td></td>
<td>• DELETED</td>
</tr>
<tr>
<td>Logging Analytics for</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td>LogAnalyticsQueryJobWorkRequest</td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• SUCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELLED</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td>Logging Analytics for</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td>LogAnalyticsStorageWorkRequest</td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELLED</td>
</tr>
<tr>
<td>Logging Analytics for</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td>LogAnalyticsConfigWorkRequest</td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCEEDED</td>
</tr>
<tr>
<td>Management Agent</td>
<td>• CREATED</td>
</tr>
<tr>
<td></td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• SUCCEEDED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td>Object Storage</td>
<td>• ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>• IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>• FAILED</td>
</tr>
<tr>
<td></td>
<td>• COMPLETED</td>
</tr>
<tr>
<td></td>
<td>• CANCELING</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
</tbody>
</table>
Filtering the Request Response

You sometimes need to know which resources are affected by a given asynchronous work request. In cases where the request response includes just one or two affected resources, the body of the request response is probably sufficient. However, in cases where a request response affects a great many resources, you must filter the response to identify the resources that you're interested in.

Filtering of resources listed in a work request response relies on two attributes of the `WorkRequestResource` type: `entityType` and `actionType`.

- **entityType**: Represents the resource type which the work request affects. This is an optional attribute, but each resource can have only one `entityType`.
- **actionType**: Represents how the specified resource is affected by the operation associated with the work request. Each service specifies a fixed list of allowable `actionType` values (shown in the sections following).

To obtain resource information on a work request, call `GetWorkRequest` and pass in the work request ID. The call returns a response in JSON format. Following is an example from calling `GetWorkRequest` on the Object Storage service.

```json
{
    operationType: "COPY_OBJECT",
    status: "IN_PROGRESS",
    id: "f54527d6-029b-4221-9046-a81b7686202",
    resources: [
        {
            entityType: "object",
            actionType: "READ",
            entityUri: "/n/mynamespace/b/backups/o/myobject"
        },
        {
            entityType: "object",
            actionType: "WRITTEN",
            entityUri: "/n/mynamespace/b/backups/o/copyofmyobject"
        }
    ],
    timeAccepted: 2017-10-13T17:23:46.000Z,
    timeStarted: 2017-10-13T17:23:52.198Z,
    percentComplete: 10.0
}
```

**Note:**

Different services provide slightly different responses. See the reference documentation for each service's work request API for details. Links to each are provided in the *For More Information* on page 4383 section.

The following table lists the entity types and action types that are supported by Oracle Cloud Infrastructure services.
<table>
<thead>
<tr>
<th>Service Name</th>
<th>Operation</th>
<th>entityType</th>
<th>actionType</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain Platform</strong></td>
<td>CreateBlockchainPlatform</td>
<td>instance</td>
<td>CREATED</td>
</tr>
<tr>
<td></td>
<td>UpdateBlockchainPlatform</td>
<td></td>
<td>UPDATED</td>
</tr>
<tr>
<td></td>
<td>DeleteBlockchainPlatform</td>
<td></td>
<td>DELETED</td>
</tr>
<tr>
<td></td>
<td>ScaleBlockchainPlatform</td>
<td></td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>StopBlockchainPlatform</td>
<td></td>
<td>RELATED</td>
</tr>
<tr>
<td></td>
<td>StartBlockchainPlatform</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Container Engine for Kubernetes</strong></td>
<td>CreateCluster</td>
<td>cluster</td>
<td>ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>DeleteCluster</td>
<td></td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>UpdateCluster</td>
<td></td>
<td>FAILED</td>
</tr>
<tr>
<td></td>
<td>CreateNodePool</td>
<td>nodepool</td>
<td>SUCCEEDED</td>
</tr>
<tr>
<td></td>
<td>DeleteNodePool</td>
<td></td>
<td>CANCELING</td>
</tr>
<tr>
<td></td>
<td>UpdateNodePool</td>
<td></td>
<td>CANCELED</td>
</tr>
<tr>
<td><strong>Content and Experience</strong></td>
<td>CreateOceInstance</td>
<td>oceInstance</td>
<td>ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>DeleteOceInstance</td>
<td></td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td>UpdateOceInstance</td>
<td></td>
<td>FAILED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SUCCEEDED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CANCELING</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CANCELED</td>
</tr>
<tr>
<td><strong>Data Catalog</strong></td>
<td>CreateCatalog</td>
<td>catalog</td>
<td>CREATED</td>
</tr>
<tr>
<td></td>
<td>DeleteCatalog</td>
<td></td>
<td>UPDATED</td>
</tr>
<tr>
<td></td>
<td>ChangeCatalogCompartment</td>
<td></td>
<td>DELETED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MOVED</td>
</tr>
<tr>
<td><strong>Data Integration</strong></td>
<td>CreateWorkspace</td>
<td>disworkspace</td>
<td>CREATED</td>
</tr>
<tr>
<td></td>
<td>DeleteWorkspace</td>
<td></td>
<td>UPDATED</td>
</tr>
<tr>
<td></td>
<td>ChangeCompartment</td>
<td></td>
<td>DELETED</td>
</tr>
<tr>
<td></td>
<td>StartWorkspace</td>
<td></td>
<td>MOVED</td>
</tr>
<tr>
<td></td>
<td>StopWorkspace</td>
<td></td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FAILED</td>
</tr>
</tbody>
</table>
### Service Name | Operation               | entityType      | actionType              
---|------------------------|-----------------|-------------------------
Data Science | CreateNotebookSession  | NotebookSession  | ACCEPTED                
            | DeleteNotebookSession  |                 | IN_PROGRESS            
            | DeleteProject          | Project         | FAILED                  
            |                        |                 | SUCCEEDED               
            |                        |                 | CANCELING               
            |                        |                 | CANCELED                
Load Balancing | CreateLoadBalancer     | LoadBalancer    | ACCEPTED                
            | UpdateLoadBalancer     |                 | IN_PROGRESS            
            | DeleteLoadBalancer     |                 | FAILED                  
            |                        |                 | SUCCEEDED               
Management Agent | DeployPlugins          | managementAgent | CREATED                
                |                        |                 | UPDATED                 
                |                        |                 | DELETED                 
                |                        |                 | IN_PROGRESS            
Object Storage | CopyObject             | object          | READ                    
                |                        |                 | WRITTEN                 

### Request/Response Sample

Following is a sequence of REST API calls to create a cluster, which is a common long-running operation. The caller retrieves the work request ID from the response to the initial POST call and then periodically polls the WorkRequest to determine the status of the operation. The request/response sequence that follows depicts this workflow:

1. The user issues a `CreateCluster` API call.
2. The service responds with status code 202, indicating that the request has been accepted and returns a work request ID in the `Opc-Work-Request-Id` header.
3. Next, the user issues a `GET` call on the work request ID to obtain the status of the work request.
4. The service responds with status code 200, indicating in the response body that the `CLUSTER_CREATE` operation has the status ACCEPTED.
5. With continued polling, we see another `GET` call for the work request.
6. The service responds with status code 200. The response body reports that the operation SUCCEEDED.

**Step 1.** Initial API call to initiate a `CLUSTER_CREATE` operation.

```bash
POST https://containerengine.eu-frankfurt-1.oraclecloud.com/20180222/clusters
Accept: application/json
authorization: <Redacted>
content-length: 480
Content-Type: application/json
date: Mon, 02 Jul 2018 18:20:03 GMT
host: containerengine.eu-frankfurt-1.oraclecloud.com
opc-client-info: Oracle-JavaSDK/1.2.42-preview1-SNAPSHOT
opc-request-id: D7A390ED909C47038C438BA3629FB612
```
Step 2. The response to the initial API call, which contains the work request ID in the `Opc-Work-Request-Id` header.

202
Access-Control-Allow-Methods: DELETE, GET, HEAD, OPTIONS, PATCH, POST, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: opc-work-request-id
Content-Length: 0
Date: Mon, 02 Jul 2018 18:20:04 GMT
Opc-Request-Id: D7A390ED909C47038C438BA3629FB612/33EEDCAAB2E84508B34AA75CD0FD86F4/8261D1CC89814E9BB9344D761D7F75C/515298
Opc-Work-Request-Id: ocid1.clustersworkrequest.oc1.eu-frankfurt-1.exampleuniqueID
Uri: /20180222/clusters
Vary: Accept-Encoding
X-Rate-Limit-Duration: 1
X-Rate-Limit-Limit: 16.70
X-Rate-Limit-Request-Forwarded-For: 10.237.10.0, 10.237.9.51
X-Rate-Limit-Request-Remote-Addr: 10.237.9.51:53077

Step 3. Because this is a long-running operation, the user periodically polls the work request using a GET call to determine its status.

GET https://containerengine.eu-frankfurt-1.oraclecloud.com/20180222/workRequests/<clusters_work_request_OCID>
Accept: application/json
authorization: <Redacted>
date: Mon, 02 Jul 2018 18:20:04 GMT
host: containerengine.eu-frankfurt-1.oraclecloud.com
opc-client-info: Oracle-JavaSDK/1.2.42-preview1-SNAPSHOT
opc-request-id: E8F20DAC443346B3B0EA599F367EE294
User-Agent: Oracle-JavaSDK/1.2.42-preview1-SNAPSHOT (Mac OS X/10.13.5; Java/1.8.0_172; Java HotSpot(TM) 64-Bit Server VM/25.172-b11)

Step 4. The GET call returns the following response, which indicates in the response body that the `CLUSTER_CREATE` operation has a status of `ACCEPTED`.

200
Access-Control-Allow-Methods: DELETE, GET, HEAD, OPTIONS, PATCH, POST, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: opc-work-request-id
Content-Length: 717
Content-Type: application/json
Date: Mon, 02 Jul 2018 18:20:05 GMT
Etag: 56a41efaf33d81a54933495ee910c24d7bce7a83adf18810f95e07bdd2055805
Opc-Request-Id: E8F20DAC443346B3B0EA599F367EE294/8B19C9FC3B4442CEA14685D1973D0856/0BA60B0711764DE4A4375C5
Retry-After: 30
Uri: /20180222/workRequests/_id_
Vary: Accept-Encoding
X-Rate-Limit-Duration: 1
Step 5. The operation continues, and the user continues to poll the work request using the GET method.

GET https://containerengine.eu-frankfurt-1.oraclecloud.com/20180222/workRequests/<clusters_work_request_OCID>
Accept: application/json
authorization: <Redacted>
date: Mon, 02 Jul 2018 18:24:13 GMT
host: containerengine.eu-frankfurt-1.oraclecloud.com
opc-client-info: Oracle-JavaSDK/1.2.42-preview1-SNAPSHOT
opc-request-id: 64595B97E39A471A886DA29966BB6B1D
User-Agent: Oracle-JavaSDK/1.2.42-preview1-SNAPSHOT (Mac OS X/10.13.5; Java/1.8.0_172; Java HotSpot(TM) 64-Bit Server VM/25.172-b11)

Step 6. The last GET call produced the following response, which indicates that the operation has completed. Note the entityType is "cluster" and the actionType is "CREATED".

200
Access-Control-Allow-Methods: DELETE, GET, HEAD, OPTIONS, PATCH, POST, PUT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: opc-work-request-id
Content-Length: 750
Content-Type: application/json
Date: Mon, 02 Jul 2018 18:24:14 GMT
Etag: 023d2a8cc6d893fa8c875f6465253f21d22607825f9e9eeb15b5394ae24918
Opc-Request-Id: 64595B97E39A471A886DA29966BB6B1D/3A81140991C94794AF35016E31DBE82/6245FBD8C25B42B6BDF195
Uri: /20180222/workRequests/_id_
Vary: Accept-Encoding
X-Rate-Limit-Duration: 1
X-Rate-Limit-Limit: 16.70
X-Rate-Limit-Request-Forwarded-For: 10.237.3.0, 10.237.40.183
X-Rate-Limit-Request-Remote-Addr: 10.237.40.183:55856

{  "id": "ocid1.clustersworkrequest.oc1.eu-frankfurt-1.exampleuniqueID",  "operationType": "CLUSTER_CREATE",  "status": "SUCCEEDED",  "compartmentId": "ocid1.compartment.oc1..exampleuniqueID",  "resources": [    {      "actionType": "CREATED",    "entityType": "cluster",    "identifier": "ocid1.cluster.oc1.eu-frankfurt-1.exampleuniqueID",    "entityUri": "/clusters/ocid1.cluster.oc1.eu-frankfurt-1.exampleuniqueID"    }  ],  "timeAccepted": "2018-07-02T18:20:05Z",  "timeStarted": null,  "timeFinished": null}
"entityType": "cluster",
"identifier": "ocid1.cluster.oc1.eu-frankfurt-1.exampleuniqueID",
"entityUri": "/clusters/ocid1.cluster.oc1.eu-frankfurt-1.exampleuniqueID"
}
]
,"timeAccepted": "2018-07-02T18:20:05Z",
"timeStarted": "2018-07-02T18:20:10Z",
"timeFinished": "2018-07-02T18:24:01Z"
}

For More Information

- Application Migration:
  - View the State of a Work Request
  - WorkRequest API
- Blockchain Platform: Integration: Work Requests
- Compute and Database:
  - Using the Console to View Work Requests on page 260
  - WorkRequest API
- Container Engine for Kubernetes: WorkRequest API
- Content and Experience: Work Request API
- Data Science: WorkRequest API
- IAM:
  - WorkRequest API (To delete a compartment on page 2444)
  - TaggingWorkRequest API (Deleting Tag Key Definitions and Namespaces on page 3917)
- Load Balancing:
  - Viewing the State of a Work Request on page 2565
  - WorkRequest API
- Logging Analytics: WorkRequest API
- Object Storage: WorkRequest API
- Service Connector Hub:
  - Viewing the State of a Work Request on page 3777
  - WorkRequest API

Request Signatures

This topic describes how to sign Oracle Cloud Infrastructure API requests.

Signing samples are included for the following:

- Java on page 4387
- Python on page 4389
- TypeScript on page 4389
- JavaScript on page 4390
- Ruby on page 4391
- Go on page 4391
- C# on page 4393

Signature Version 1

The signature described here is version 1 of the Oracle Cloud Infrastructure API signature. In the future, if Oracle modifies the method for signing requests, the version number will be incremented and your company will be notified.

Required Credentials and OCIDs

You need an API signing key in the correct format. See Required Keys and OCIDs on page 4179.
Caution:

Client Clock Skew

If the client's clock is skewed more than 5 minutes, a 401 (NotAuthenticated) HTTP status code is returned. This will affect your API requests. For more information, see Maximum Allowed Client Clock Skew.

You also need the OCIDs for your tenancy and user. See Where to Get the Tenancy's OCID and User's OCID on page 4184.

Summary of Signing Steps

In general, these are the steps required to sign a request:

1. Form the HTTPS request (SSL protocol TLS 1.2 is required).
2. Create the signing string, which is based on parts of the request.
3. Create the signature from the signing string, using your private key and the RSA-SHA256 algorithm.
4. Add the resulting signature and other required information to the Authorization header in the request.

See the remaining sections in this topic for details about these steps.

Specification You Need to Be Familiar With

To learn how to perform steps 2-4 in the process above, refer to draft-cavage-http-signatures-08. It's a draft specification that forms the basis for how Oracle handles request signatures. It describes generally how to form the signing string, how to create the signature, and how to add the signature and required information to the request. The remaining sections in this topic assume you're familiar with it. Important details of the Oracle Cloud Infrastructure implementation of the reference are listed in the next section.

Special Implementation Details

The following sections describe important items to note about the Oracle Cloud Infrastructure implementation of the spec.

Authorization Header

The Oracle Cloud Infrastructure signature uses the "Signature" Authentication scheme (with an Authorization header), and not the Signature HTTP header.

Required Headers

This section describes the headers that must be included in the signing string.

Note:

Error if Required Header is Missing

If a required header is missing, your client will receive a 401 "Unauthorized" response.

For GET and DELETE requests (when there's no content in the request body), the signing string must include at least these headers:

- (request-target) (as described in draft-cavage-http-signatures-08)
- host
- date or x-date (if both are included, Oracle uses x-date)

For PUT and POST requests (when there's content in the request body), the signing string must include at least these headers:

- (request-target)
- host
- date or x-date (if both are included, Oracle uses x-date)
• x-content-sha256 (except for Object Storage PUT requests; see the next section)
• content-type
• content-length

Caution:
For PUT and POST requests, your client must compute the x-content-sha256 and include it in the request and signing string, even if the body is an empty string. Also, the content-length is always required in the request and signing string, even if the body is empty. Some HTTP clients will not send the content-length if the body is empty, so you must explicitly ensure your client sends it. If date and x-date are both included, Oracle uses x-date. The x-date is used to protect against the reuse of the signed portion of the request (replay attacks).

The one exception is for Object Storage PUT requests on objects (see the next section).

Special Instructions for Object Storage PUT
For Object Storage PutObject and UploadPart PUT requests, the signing string must include at least these headers:
• (request-target)
• host
• date or x-date (if both are included, Oracle uses x-date)

If the request also includes any of the other headers that are normally required for PUT requests (see the list above), then those headers must also be included in the signing string.

Case and Order of Headers
The headers must be all lowercase in the signing string.
The order of the headers in the signing string does not matter. Just make sure to specify the order in the headers parameter in the Authorization header, as described in the draft-cavage-http-signatures-05.

Caution:
The (request-target) includes the path and query string from the request. Oracle expects that you will create the signing string with the query parameters in the same order as they appear in the request. If the request query parameters change order after signing occurs, authentication will fail.

URL Encoding of Path and Query String
When forming the signing string, you must URL encode all parameters in the path and query string (but not the headers) according to RFC 3986.

Key Identifier
You must set keyId="<TENANCY OCID>/<USER OCID>/<KEY FINGERPRINT>" in the Authorization header that you add to the request. To get those values, see Where to Get the Tenancy's OCID and User's OCID on page 4184. An example keyId looks like this (wrapped to better fit the page):

ocid1.tenancy.oc1..<unique_ID>/ocid1.user.oc1..<unique_ID>/key_fingerprint

Signing Algorithm
The signing algorithm must be RSA-SHA256, and you must set algorithm="rsa-sha256" in the Authorization header (notice the quotation marks).
**Signature Version**

You should include `version="1"` in the `Authorization` header (notice the quotation marks). If you do not, it's assumed that you're using whatever the current version is (which is version 1 at this time).

**Example Header**

Here's an example of the general syntax of the `Authorization` header (for a request with content in the body):

```plaintext
Authorization: Signature
version="1",keyId="/tenancy_ocid/<user_ocid>/<key_fingerprint>",algorithm="rsa-sha256",headers="(request-target) date x-content-sha256 content-type content-length",signature="Base64(RSA-SHA256(<signing_string>))"
```

**Test Values**

Here's an example key pair, two example requests, and the resulting `Authorization` header for each.

**Caution:** The example signatures use the RSA 2048-bit keys below. Use these keys only for testing your signing code, not for sending production requests.

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCFENGw33yGihy92pDjZQh10C36rPjJ+cVfSC8+q28hxA161QFNUd13wuCTUcqQd2qsBe/2hFyc2DCJjg0h1L78+6Z4UMR7EOcfpdeU9HF3m hs+FUR45uBJeDK1HSFHD8bHkD6kv8FPgfJtotc+2xjJwoYi+1hp1fIekaxsyQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDCFENGw33yGihy92pDjZQh10C36rPjJ+cVfSC8+q28hxA161QFNUd13wuCTUcqQd2qsBe/2hFyc2DCJjg0h1L78+6Z4UMR7EOcfpdeU9HF3m hs+FUR45uBJeDK1HSFHD8bHkD6kv8FPgfJtotc+2xjJwoYi+1hp1fIekaxsyQIDAQABAoGBAJR8ZkCIVu55zv+udt17TSnordITvoXXJnK72Z+UvMNUCDN2Qc4sBiAqwLw1cSkt5DsKZ8UETpYPy8pYNnDEz2Dyiae9+xEpuyheW2oH42x71wqBtoKkgwrXa/pzdpuiucRRjk6vE6YY7EBBs/g7uanVpGibOVAESqHIAEkE7DkjVH28WDUsf1nqvfr2jk6CT7n1cE3jGJz2Z7z1ZmBMhFODNMLURXR/Zm3pR5m0tCmbgQ5Rk9u412jtidPIwBAJN73v8pknth48bbQo/fKe16uEyybPttA5/uhHuKZ6F7F70uKogcmJSjubOc5t6h11vSl0QZjqZMEOwr+wKSMCQQQCC4kXjEsABvA770p6HtG/E1En7kpyUXRNvFsD0E0czJBBv/aRFUJxuxR91j4h2Ec9SAs7AsKMgq5OXb515Jj36xakEAqIT7aFOYBFwggQAskWNKLVy5gkbAZRTelBacPMuQd11DfdtVApqPAZ01y0RKmWGaFkaoqFQXKCWy0u1VknqJAXr1gySFci/2ueKfIE1QqIILS8V801pFLRnb1pzI7UyQxntAEFYM560yJ1zUpObv14cScGd36t1SMMvxLOVTA==
-----END RSA PRIVATE KEY-----
```

The public key is stored under keyId:

```
ocid1.tenancy.oc1..<unique_ID>/ocid1.user.oc1..<unique_ID>/<key_fingerprint>
```

For the following GET request (line breaks inserted between query parameters for easier reading; also notice the URL encoding as mentioned earlier):

```
GET https://iaas.us-phoenix-1.oraclecloud.com/20160918/instances
?availabilityDomain=Pjwf%3A%20PHX-AD-1
&compartmentId=ocid1.compartment.oc1...<unique_ID>
&displayName=TeamInstances
&volumeId=ocid1.volume.oc1.phx.<unique_ID>
```

Date: Thu, 05 Jan 2014 21:31:40 GMT
The signing string would be (line breaks inserted into the (request-target) header for easier reading):

date: Thu, 05 Jan 2014 21:31:40 GMT
(request-target): get /20160918/instances?availabilityDomain=Pjwf%3A%20PH
X-AD-1&compartmentId=ocid1.compartment.oc1..aaaaaaam3we6vnherjrq5q2i
dncddf1vjsnog7ml6rtdb25g1chfeyjxa&displayName=TeamXInstances&
volumeId=ocid1.volume.oc1.phx.abyhqljrqtttnl73nrmrfwaux7kcvzfs3s66izvxf2h
41gyvynsdnoiwr5q
host: iaas.us-phoenix-1.oraclecloud.com

The Authorization header would be:
Signature version="1",headers="date (request-target) host",keyId="ocid1.tenancy.oc1..<unique_ID>/ocid1.user.oc1..<unique_ID>/
<key_fingerprint>,algorithm="rsa-sha256",
signature="<your_signature>"

For the following POST request:
POST https://iaas.us-phoenix-1.oraclecloud.com/20160918/volumeAttachments
Date: Thu, 05 Jan 2014 21:31:40 GMT
{
    "compartmentId": "ocid1.compartment.oc1..<unique_id>",
    "instanceId": "ocid1.instance.oc1.phx.<unique_id>",
    "volumeId": "ocid1.volume.oc1.phx.<unique_id>"
}

The signing string would be:

date: Thu, 05 Jan 2014 21:31:40 GMT
(request-target): post /20160918/volumeAttachments
host: iaas.us-phoenix-1.oraclecloud.com
content-length: 316
content-type: application/json
x-content-sha256: V9Z20UJTvkvpJ50f1BzKE32+6m2zJjweHpDMX/U4UY0=

The Authorization header would be:
Signature version="1",headers="date (request-target) host content-length content-type x-content-sha256",
keyId="ocid1.tenancy.oc1..<unique_ID>/ocid1.user.oc1.<unique_ID>/
<your_fingerprint>",
algorithm="rsa-sha256",signature="<your_signature>"

Sample Code

This section shows the basic code for signing API requests.

Java

/**
 * Copyright (c) 2016, 2020, Oracle and/or its affiliates. All rights
 * reserved.
 * This software is dual-licensed to you under the Universal Permissive
 * License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl
 * or Apache License 2.0 as shown at http://www.apache.org/licenses/
 * LICENSE-2.0. You may choose either license.
 */
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.nio.charset.StandardCharsets;
import javax.ws.rs.client.Client;
import javax.ws.rs.client.ClientBuilder;
import javax.ws.rs.client.Invocation;
import javax.ws.rs.client.WebTarget;
import javax.ws.rs.core.MediaType;
import javax.ws.rs.core.MultivaluedMap;
import javax.ws.rs.core.Response;
import com.google.common.net.UrlEscapers;
import com.oracle.bmc.http.signing.RequestSigningFilter;

public class RawRestCallExample {

    public static void main(String[] args) throws Exception {
        // TODO: fill this out
        String instanceId = null;

        String configurationFilePath = "~/.oci/config";
        String profile = "DEFAULT";

        // Pre-Requirement: Allow setting of restricted headers. This is required to allow the
        // to set the host header that gets computed during signing of the request.
        System.setProperty("sun.net.http.allowRestrictedHeaders", "true");

        // 1) Create a request signing filter instance
        RequestSigningFilter requestSigningFilter =
                RequestSigningFilter.fromConfigFile(configurationFilePath, profile);

        // 2) Create a Jersey client and register the request signing filter
        Client client =
                ClientBuilder.newBuilder().build().register(requestSigningFilter);

        // 3) Target an endpoint. You must ensure that path arguments and query
        // params are escaped correctly yourself
        WebTarget target =
                client.target("https://iaas.us-phoenix-1.oraclecloud.com")
                        .path("20160918")
                        .path("instances")
                        .path(UrlEscapers.urlPathSegmentEscaper().escape(instanceId));

        // 4) Set the expected type and invoke the call
        Invocation.Builder ib = target.request();
        ib.accept(MediaType.APPLICATION_JSON);
        Response response = ib.get();

        // 5) Print the response headers and the body (JSON) as a string
        MultivaluedMap<String, Object> responseHeaders = response.getHeaders();
        System.out.println(responseHeaders);
        InputStream responseBody = (InputStream) response.getEntity();
        try (final BufferedReader reader = new BufferedReader(new InputStreamReader(responseBody, StandardCharsets.UTF_8))) {
            StringBuilder jsonBody = new StringBuilder();
            String line;
            while ((line = reader.readLine()) != null) {
                jsonBody.append(line);
            }
            System.out.println(jsonBody.toString());
        }
    }
}
Python

```python
# coding: utf-8
# Copyright (c) 2016, 2020, Oracle and/or its affiliates. All rights reserved.
# This software is dual-licensed to you under the Universal Permissive License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl
# or Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0. You may choose either license.

import requests
from oci.config import from_file
from oci.signer import Signer

config = from_file()
auth = Signer(
    tenancy=config['tenancy'],
    user=config['user'],
    fingerprint=config['fingerprint'],
    private_key_file_location=config['key_file'],
    pass_phrase=config['pass_phrase']
)

endpoint = 'https://identity.us-phoenix-1.oraclecloud.com/20160918/users/

body = {
    'compartmentId': config['tenancy'],  # root compartment
    'name': 'TestUser',
    'description': 'Created with a raw request'
}

response = requests.post(endpoint, json=body, auth=auth)
response.raise_for_status()
print(response.json()['id'])
```

TypeScript

```typescript
/**
 * Copyright (c) 2020, Oracle and/or its affiliates. All rights reserved.
 * This software is dual-licensed to you under the Universal Permissive License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl
 * or Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0. You may choose either license.
 */

import { DefaultRequestSigner, HttpRequest } from 'oci-common';
import { provider } from './authentication';
import * as promise from 'es6-promise';
promise.polyfill();

const userID = "Add User OCID here";
(async () => {
    // Code...
})
```
// 1. Create Request Signing instance
const signer = new DefaultRequestSigner(provider);

// 2. Create HttpRequest to be signed
const httpRequest: HttpRequest = {
  uri: 'https://identity.us-phoenix-1.oraclecloud.com/20160918/users/${userID}',
  headers: new Headers(),
  method: "GET"
};

// 3. sign request
await signer.signHttpRequest(httpRequest);

// 4. Make the call
const response = await fetch(
  new Request(httpRequest.uri, {
    method: httpRequest.method,
    headers: httpRequest.headers,
    body: httpRequest.body
  })
);

// 5. Print response
console.log(await response.json());

/**
* Copyright (c) 2020, Oracle and/or its affiliates. All rights reserved.
* This software is dual-licensed to you under the Universal Permissive
* License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl
* or Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0. You may choose either license.
* /
const common = require("oci-common");
const promise = require("es6-promise");
require("isomorphic-fetch");
promise.polyfill();

const configurationFilePath = "~/.oci/config";
const configProfile = "DEFAULT";

const provider = new common.ConfigFileAuthenticationDetailsProvider(
  configurationFilePath,
  configProfile
);

const userID = "<INSERT_SAMPLE_USER_OCID_HERE>";
(async () => {
  // 1. Create Request Signing instance
  const signer = new common.DefaultRequestSigner(provider);

  // 2. Create HttpRequest to be signed
  const httpRequest = {
    uri: 'https://identity.us-phoenix-1.oraclecloud.com/20160918/users/${userID}',
    headers: new Headers(),
    method: "GET"
  );
// 3. sign request
await signer.signHTTPRequest(httpRequest);

// 4. Make the call
const response = await fetch(
    new Request(httpRequest.uri, {
        method: httpRequest.method,
        headers: httpRequest.headers,
        body: httpRequest.body    
    })
);

// 5. Print response
console.log(await response.json());
})

Ruby

# Copyright (c) 2016, 2020, Oracle and/or its affiliates. All rights reserved.
# This software is dual-licensed to you under the Universal Permissive License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl or # Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0.
# You may choose either license.

require 'oci'
require 'net/http'

config = 
OCI::ConfigFileLoader.load_config(config_file_location:my_config_file_location)
endpoint = OCI::Regions.get_service_endpoint(config.region, :IdentityClient)

uri = URI(endpoint + '/20160918/users/' + config.user)
request = Net::HTTP::Get.new(uri)

signer = OCI::Signer.new(config.user, config.fingerprint, config.tenancy, 
config.key_file, pass_phrase:my_private_key_pass_phrase)

signer.sign(:get, uri.to_s, request, nil)

result = Net::HTTP.start(uri.hostname, uri.port, :use_ssl => true) {|http|
    http.request(request)
}

puts result.body

Go

The following example shows how to create a default signer.

```
Note:
The SDK for Go exposes a stand-alone signer that you can use to sign custom
requests. You can find related code at http_signer.go.
```

// Copyright (c) 2016, 2018, 2020, Oracle and/or its affiliates. All rights reserved.
// This software is dual-licensed to you under the Universal Permissive License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl or // Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0. You may choose either license.
// Example code for sending raw request to Service API

package example

import {
  "fmt"
  "io/ioutil"
  "log"
  "net/http"
  "time"
  "github.com/oracle/oci-go-sdk/common"
  "github.com/oracle/oci-go-sdk/example/helpers"
}

// ExampleRawRequest compose a request, sign it and send to server
func ExampleListUsers_RawRequest() {
  // build the url
  url := "https://identity.us-phoenix-1.oraclecloud.com/20160918/users/?compartmentId=\" + \*helpers.RootCompartmentID()

  // create request
  request, err := http.NewRequest("GET", url, nil)
  helpers.FatalIfError(err)

  // Set the Date header
  request.Header.Set("Date", time.Now().UTC().Format(http.TimeFormat))

  // And a provider of cryptographic keys
  provider := common.DefaultConfigProvider()

  // Build the signer
  signer := common.DefaultRequestSigner(provider)

  // Sign the request
  signer.Sign(request)

  client := http.Client{}

  fmt.Println("send request")

  // Execute the request
  resp, err := client.Do(request)
  helpers.FatalIfError(err)

  defer resp.Body.Close()

  log.Println("response Status:\", resp.Status)
  log.Println("response Headers:\", resp.Header)

  body, _ := ioutil.ReadAll(resp.Body)
  log.Println("response Body:\", string(body))

  fmt.Println("receive response")

  // Output:
  // send request
  // receive response
}
C#

/*
 * Copyright (c) 2020, Oracle and/or its affiliates. All rights reserved.
 * This software is dual-licensed to you under the Universal Permissive
 * License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl or
 * Apache License 2.0 as shown at http://www.apache.org/licenses/
 * LICENSE-2.0. You may choose either license.
 */

using System;
using System.Net.Http;
using System.Threading.Tasks;

namespace Oci.Examples
{
    public class RawRestCallExample
    {
        private static NLog.Logger logger =
            NLog.LogManager.GetCurrentClassLogger();

        public static async Task MainRaw()
        {
            var namespaceName =
                Environment.GetEnvironmentVariable("NAMESPACE_NAME");
            var compartmentId =
                Environment.GetEnvironmentVariable("COMPARTMENT_ID");

            var httpClientHandler =
                OciHttpClientHandler.FromConfigFile("~/oci/config", "DEFAULT");
            var GET_BUCKETS_URL = "https://objectstorage.us-
                phoenix-1.oraclecloud.com/n/{namespaceName}/b/?
                compartmentId={compartmentId}";
            var client = new HttpClient(httpClientHandler);
            var requestMessage = new HttpRequestMessage(HttpMethod.Get, new
                Uri(GET_BUCKETS_URL));

            var response = await client.SendAsync(requestMessage);
            logger.Info("Is rest call successful:
                {response.IsSuccessStatusCode}");
            var responseJson = await response.Content.ReadAsStringAsync();
            logger.Info("Parsed Response: {responseJson}";
        }
    }
}

Client-Side Encryption

The Oracle Cloud Infrastructure SDK for Python and SDK for Java support Client Side Encryption, which encrypts your data on the client side before storing it locally or using it with other Oracle Cloud Infrastructure services.

By default, the SDK generates a unique data key for each data object that it encrypts. Data is encrypted using a secure, authenticated, symmetric AES/GCM key algorithm with a 256-bit key length.

To use client-side encryption, you must create a master encryption key (MEK) using the Key Management Service. This can be done using the CreateKey or ImportKey operations.

The MEK is used to generate a Data Encryption Key (DEK) to encrypt each payload. A encrypted copy of this DEK (encrypted under the MEK) and other pieces of metadata are included in the encrypted payload returned by the SDKs so that they can be used for decryption.
Java Prerequisites

The unlimited policy files for earlier releases are required only for JDK 8, 7, and 6 updates earlier than 8u161, 7u171, and 6u16. For those versions and later the policy files are included but not enabled by default.

Current versions of the JDK do not require these policy files. They are provided here for use with older versions of the JDK. JDK 9 and later ship with the unlimited policy files and use them by default.

Examples

The following code example show how to encrypt a string:

Java

```java
// String encryption example
final byte[] plainText = "Hello World".getBytes();
String masterKeyId = "OCID....";
Map<String, String> context = Collections.singletonMap("Example", "value");

OciCrypto ociCrypto = new OciCrypto();
KmsMasterKey kmsMasterKey = new KmsMasterKey(authenticationProvider, Region.US_ASHBURN_1.getRegionId(), vaultId, masterKeyId);
KmsMasterKeyProvider kmsMasterKeyProvider = new KmsMasterKeyProvider(kmsMasterKey);

// Encrypt the data and embed the master key ID in the header
final OciCryptoResult encryptResult =
    ociCrypto.encryptData(kmsMasterKeyProvider, plainText, context);
final byte[] cipherText = encryptResult.getResult();

// Decrypt the data
final OciCryptoResult decryptResult =
    ociCrypto.decryptData(kmsMasterKeyProvider, cipherText);
```

Python

```python
import oci
# user supplied vars
vault_id = TEST_VAULT_OCID
master_key_id = TEST_MASTER_KEY_ID
data_to_encrypt_bytes = b"This is a secret message"

config = oci.config.from_file()
kms_master_key = oci.encryption.KMSMasterKey(
    config=config, master_key_id=master_key_id, vault_id=vault_id)

kms_master_key_provider = oci.encryption.KMSMasterKeyProvider(
    config=config,
    kms_master_keys=[kms_master_key]
)

crypto_result = crypto.encrypt(kms_master_key_provider,
data_to_encrypt_bytes)
ciphertext = crypto_result.get_data()
print("ciphertext: {}".format(ciphertext))

# decrypt string example
crypto_result = crypto.decrypt(ciphertext, kms_master_key_provider)
```
The following examples show how to encrypt a file stream:

**Java**

```java
// Create Encryption file stream
FileInputStream in = new FileInputStream(srcFile);
OciCrypto ociCrypto = new OciCrypto();
KmsMasterKey kmsMasterKey = new KmsMasterKey(authenticationProvider,
Region.US_ASHBURN_1.getRegionId(), vaultId, masterKeyId);
KmsMasterKeyProvider kmsMasterKeyProvider = new
KmsMasterKeyProvider(kmsMasterKey);
OciCryptoInputStream encryptingStream =
ociCrypto.createEncryptingStream(kmsMasterKeyProvider, in);

// Write the encrypted data to file
FileOutputStream out = new FileOutputStream(srcFile + ".encrypted”);
IOUtils.copy(encryptingStream, out);
encryptingStream.close();
out.close();

// For decryption, no need to pass key info
KmsMasterKeyProvider kmsMasterKeyProvider = new
KmsMasterKeyProvider(authenticationProvider);
// Create the Decryption file stream.
in = new FileInputStream(srcFile + ".encrypted”);
OciCryptoInputStream decryptingStream =
ociCrypto.createDecryptingStream(kmsMasterKeyProvider, in);

// Return the plaintext data
out = new FileOutputStream(srcFile + ".decrypted”);
IOUtils.copy(decryptingStream, out);
decryptingStream.close();
out.close();
```

**Python**

```python
import oci
import shutil
# user supplied vars
vault_id = TEST_VAULT_OCID
master_key_id = TEST_MASTER_KEY_ID
file_to_encrypt = "/file/to/encrypt/message.txt"
output_encrypted_file = "/tmp/message.txt.encrypted"
output_decrypted_file = "/tmp/message.txt.decrypted"

# setup OCI KMS keys
config = oci.config.from_file()
kms_master_key = oci.encryption.KMSMasterKey(
    config=config, master_key_id=master_key_id, vault_id=vault_id
)
kms_master_key_provider = oci.encryption.KMSMasterKeyProvider(
    config=config,
    kms_master_keys=[kms_master_key]
)
```
# encrypt stream example
with open(output_encrypted_file, 'wb') as output_stream,
open(file_to_encrypt, 'rb') as stream_to_encrypt:
    with crypto.create_encryption_stream(
        kms_master_key_provider,
        stream_to_encrypt
    ) as encryption_stream:
        shutil.copyfileobj(encryption_stream, output_stream)

# decrypt stream example
with open(output_decrypted_file, 'wb') as output_stream,
open(output_encrypted_file, 'rb') as stream_toDecrypt:
    with crypto.create_decryption_stream(
        stream_to_decrypt,
        kms_master_key_provider
    ) as decryption_stream:
        shutil.copyfileobj(decryption_stream, output_stream)
Glossary

A

AD-specific subnet
A subnet that is specific to a particular availability domain (AD). Historically all subnets were AD-specific. Compare with regional subnets, which Oracle recommends over AD-specific subnets.

alarm
The trigger rule and query to evaluate and related configuration, such as notification details to use when the trigger is breached. Alarms passively monitor your cloud resources using metrics in Monitoring.

API key
A credential for securing requests to the Oracle Cloud Infrastructure REST API.

application (Application Migration)
A combination of the artifacts and configuration deployed on one or more service instances running in the source environment.

attach
Link a volume and instance together. Allows an instance to connect and mount the volume as a hard drive.

Attribute
An attribute describes a data item with a name and data type. For example, a column in a table or a field in a file.

auth token
Oracle Cloud Infrastructure-generated token you use to authenticate with third-party APIs, such as a Swift client.

availability domain
One or more isolated, fault-tolerant Oracle data centers that host cloud resources such as instances, volumes, and subnets. A region contains one or more availability domains.

B

backend set
A logical entity defined by a list of backend servers, a load balancing policy, and a health check policy.

bare metal IaaS
A cloud infrastructure that allows you to utilize hosted physical hardware, as opposed to traditional software-based virtual machines, ensuring a high level of security and performance.

block storage volume
A virtual disk that provides persistent storage space for instances in the cloud.

bucket
A logical container for storing objects.
C

Category
A category is created in a glossary to group logically related business terms. You can create a category within a category to group your terms.

CHAP
Stands for Challenge-Handshake-Authentication-Protocol. It is a security protocol used by iSCSI for authentication between a volume and an instance.

Cloud Block Storage
A service that allows you to add block storage volumes to an instance in order to expand the available storage on that resource.

cloud network
A virtual version of a traditional network—including CIDRs, subnets, route tables, and gateways—on which your instance runs.

cluster network
A pool of high performance computing (HPC) instances that are connected with a high-bandwidth, ultra low-latency network.

compartment
A collection of related resources that can be accessed only by certain groups that have been given permission by an administrator in your organization.

Compute
A service that lets you provision and manage compute hosts, known as instances.

connect
Make an attached volume usable by an instance's guest OS.

CPE
The router at the edge of your on-premises network. The Networking service also has an object called a CPE, which is a virtual representation of your edge router. You create that object when setting up VPN Connect (an IPSec VPN) between Oracle and your on-premises network.

CPE Configuration Helper
A feature of the Oracle Console that generates information that a network engineer can use to configure the customer-premises equipment (CPE) at their end of a VPN connection.

cross-connect
Used with Oracle Cloud Infrastructure FastConnect, specifically if you're using a third-party provider or colocated with Oracle in a FastConnect location. A cross-connect is the physical cable connecting your existing network to Oracle in the FastConnect location.

cross-connect group
Used with Oracle Cloud Infrastructure FastConnect, specifically if you're using a third-party provider or colocated with Oracle in a FastConnect location. A cross-connect group is a link aggregation group (LAG) that contains at least one cross-connect.

customer-premises equipment
The router at the edge of your on-premises network. The Networking service also has an object called a CPE, which is a virtual representation of your edge router. You create that object when setting up VPN Connect (an IPSec VPN) between Oracle and your on-premises network.
D

Data Asset (Data Catalog and Data Integration)

Represents a data source, such as a database, an object store, a file or document store, a message queue, or an application.

Data Catalog Tags

Tags are free-form labels or keywords you create to be able to logically identify data objects. Tags help in metadata classification and discovery. You create tags for data assets, data entities, and attributes. Using tags, you can search for all data objects tagged with a specific tag name.

Data Entity (Data Catalog and Data Integration)

A data entity is a collection of data such as a database table or view, or a single logical file and normally has many attributes that describe its data.

data point (Monitoring service)

A timestamp-value pair for the specified metric. Example: 2018-05-10T22:19:00Z, 10.4

DB System

A dedicated bare metal instance running Oracle Linux, optimized for running one or more Oracle databases.
A DB System is a Database Service resource.

DHCP options

Configuration information that is automatically provided to the instances when they boot up.

dimension (Monitoring service)

A qualifier provided in a metric definition. Example: Resource identifier (resourceId), provided in the definitions of oci_computeagent metrics.

display name

A friendly name or description that helps you easily identify the resource.

DRG

An optional virtual router that you can add to your VCN to provide a path for private network traffic between your VCN and on-premises network.

DRG attachment

When you attach a dynamic routing gateway (DRG) to a virtual cloud network (VCN), the result is a DRG attachment object. To detach the DRG, you delete that attachment object.

drift (Resource Manager)

Difference between the actual, real-world state of your infrastructure and the stack's last executed configuration.

dynamic group

A special type of IAM group that contains instances that match rules that you define (thus the membership can change dynamically as matching instances are terminated or launched). These instances act as "principal" actors and can make API calls to Oracle Cloud Infrastructure services according to IAM policies that you write for the dynamic group.

dynamic routing gateway

An optional virtual router that you can add to your VCN to provide a path for private network traffic between your VCN and on-premises network.
A glossary is a collection of business concepts in your company. Glossary constitutes of categories and business terms.

group
A collection of users who all need a particular type of access to a set of resources or compartment.

guest operating system
An operating system installed on a cloud instance.

guest OS
An operating system installed on a cloud instance.

Harvest
Process that extracts technical metadata from your connected data sources into your Data Catalog repository.
health check

A test to confirm the availability of backend servers.

I

IaaS

A service that allows customers to rapidly scale up or down their computer infrastructure (computing, storage, or network).

IAM

The service for controlling authentication and authorization of users who need to use your cloud resources.

Identity and Access Management Service

The service for controlling authentication and authorization of users who need to use your cloud resources. Also called "IAM".

identity provider

A service that provides identifying credentials and authentication for federated users.

IdP

Short for "identity provider", which is a service that provides identifying credentials and authentication for federated users.

image

A template of a virtual hard drive that determines the operating system and other software for an instance.

Infrastructure-as-a-Service

A service that allows customers to rapidly scale up or down their computer infrastructure (computing, storage, or network).

instance

A bare metal or virtual machine (VM) compute host. The image used to launch the instance determines its operating system and other software. The shape specified during the launch process determines the number of CPUs and memory allocated to the instance.

instance wallet

An Autonomous Database instance wallet contains only credentials and keys for a single database instance.

internet gateway

An optional virtual router that you can add to your VCN. It provides a path for network traffic between your VCN and the internet.

interval (Monitoring service)

The time window used to convert the given set of raw data points. Example: 5 minutes

IPSec connection

The secure connection between a dynamic routing gateway (DRG) and customer-premises equipment (CPE), consisting of multiple IPSec tunnels. The IPSec connection is one of the components forming a site-to-site VPN between a virtual cloud network (VCN) and your on-premises network.

IPv6

An object that contains an IPv6 address and related properties. Currently IPv6 addressing is supported only in the US Government Cloud. Only instances in IPv6-enabled VCNs and IPv6-enabled subnets can have IPv6 addresses.
Glossary

IQN
A unique ID assigned to an iSCSI device. Used when connecting a volume to an instance.

iSCSI
A TCP/IP based standard used for communication between a volume and attached instance.

iSCSI Qualified Name
A unique ID assigned to an iSCSI device. Used when connecting a volume to an instance.

K
key pair
A security mechanism consisting of a public key and a private key. Required (for example) for Secure Shell (SSH) access to an instance.

L
listener
An entity that checks for incoming traffic on the load balancer's public floating IP address.

local peering gateway
A component on a VCN for routing traffic to a locally peered VCN. "Local" peering means the two VCNs are in the same region. Compare with a remote peering connection.

local VCN peering
The process of connecting two VCNs in the same region so that their resources can communicate without routing the traffic over the internet or through your on-premises network.

LPG
A component on a VCN for routing traffic to a locally peered VCN. "Local" peering means the two VCNs are in the same region. Compare with a remote peering connection.

M
message (Notifications and Monitoring services)
An alert published to all subscriptions in the specified topic. Each message is delivered at least once per subscription.

metric
(Monitoring service) A measurement related to health, capacity, or performance of a given resource.
Example: CpuUtilization

metric definition (Monitoring service)
A set of references, qualifiers, and other information provided by a metric namespace for a given metric.

metric namespace (Monitoring service)
Indicator of the resource, service, or application that emits the metric. Provided in the metric definition.
Example: oci_computeagent

metric stream (Monitoring service)
An individual set of aggregated data for a metric. Typically specific to a resource.
migration (Application Migration)
The end-to-end workflow of moving an application from a source environment to Oracle Cloud Infrastructure.

Monitoring Query Language (Monitoring service)
The syntax used for metric and alarm queries.

Mount Point
A directory from which a client may access a remote File Storage Service file system.

Mount Target
An NFS endpoint that allows a file system to be accessed by clients.

MQL (Monitoring service)
Monitoring Query Language. The syntax used for metric and alarm queries. In the Console, MQL syntax of queries is displayed in Advanced Mode.

N
NAT gateway
An optional virtual router that you can add to your VCN to perform Network Address Translation (NAT). A NAT gateway gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.

Network security group
One method for implementing security rules in a VCN. A network security group consists of a set of resources (VNICs or resources with VNICs) and security rules that apply to those resources. See also security rules and security lists.

Network source
A group of IP addresses that can be used in policy to restrict access.

Notification destination (Monitoring service)
Protocol and other details for sending messages when the alarm transitions to another state, such as from "OK" to "FIRING."

NSG
One method for implementing security rules in a VCN. A network security group consists of a set of resources (VNICs or resources with VNICs) and security rules that apply to those resources. See also security rules and security lists.

O
Object
Any type of data, regardless of content type, is stored as an object. The object is composed of the object itself and metadata about the object. Each object is stored in a bucket.

OCID
An Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). This ID is included as part of the resource's information in both the Console and API.

One-time password
A single-use Console password that Oracle assigns to a new user, or to an existing user who requested a password reset.
**Oracle Cloud Identifier**

An Oracle-assigned unique ID called an Oracle Cloud Identifier (OCID). This ID is included as part of the resource's information in both the Console and API.

**OTP**

A single-use Console password that Oracle assigns to a new user, or to an existing user who requested a password reset.

**P policy**

An IAM document that specifies who has what type of access to your resources. It is used in different ways: to mean an individual statement written in the policy language; to mean a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and to mean the overall body of policies your organization uses to control access to resources.

**policy statement**

Policies can contain one or more individual statements. Each statement gives a group a certain type of access to certain resources in a particular compartment.

**primary IP**

The private IP that is automatically created and assigned to a VNIC during creation.

**primary VNIC**

The VNIC that is automatically created and attached to an instance during launch.

**private IP**

An object that contains a private IPv4 address and related properties such as a hostname for DNS. Each instance automatically comes with a primary private IP, and you can add secondary ones.

**private peering**

One of the ways to use FastConnect. Private peering lets you extend your existing infrastructure into a virtual cloud network (VCN) in Oracle Cloud Infrastructure (for example, to implement a hybrid cloud, or a lift and shift scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918).

**private subnet**

A subnet in which instances are not allowed to have public IP addresses

**private virtual circuit**

A FastConnect virtual circuit that supports private peering.

**public IP**

An object that contains a public IP address and related properties. You control whether each private IP on an instance has an assigned public IP. There are two types: reserved public IPs and ephemeral public IPs.

**public peering**

One of the way to use FastConnect. Public peering lets your on-premises network access public services in Oracle Cloud Infrastructure without using the internet. For example, Object Storage, the Oracle Cloud Infrastructure Console and APIs, or public load balancers in your VCN. Communication across the connection is with IPv4 public IP addresses. Without FastConnect, the traffic destined for public IP addresses would be routed over the internet. With FastConnect, that traffic goes over your private physical connection.

**public subnet**

A subnet in which instances are allowed to have public IP addresses. When you launch an instance in a public subnet, you specify whether the instance should have a public IP address.
**public virtual circuit**
A FastConnect virtual circuit that supports public peering.

**Q**

**query (Monitoring service)**
The expression to evaluate for returning aggregated data. A valid query includes a metric, statistic, and interval. In the Console, you can view a query in Basic Mode or Advanced Mode. The latter displays the Monitoring Query Language (MQL) syntax.

**R**

**realm**
A logical collection of regions. Realms are isolated from each other and do not share any data. Your tenancy exists in a single realm and can access the regions that belong to that realm.

**region**
A collection of availability domains located in a single geographic location.

**regional subnet**
A subnet that spans all availability domains (ADs) in the region. Oracle recommends using regional subnets because they are more flexible and make it easier to implement failover across ADs. Compare with AD-specific subnets.

**regional wallet**
An Autonomous Database regional wallet contains credentials and keys for all Autonomous Databases in a specified region.

**remote peering connection**
A component on a dynamic routing gateway (DRG) for routing traffic to a remotely peered VCN. "Remote" peering means the two VCNs are in different regions. Compare with a local peering gateway.

**remote VCN peering**
The process of connecting two VCNs in different regions so that their resources can communicate without routing their traffic over the internet or through your on-premises network.

**reserved public IP**
A public IP address (and related properties) that you create in your tenancy and assign to your instances in a given region as you like. It persists in your tenancy until you delete it. It can be assigned to any private IP on a given VNIC, not just the primary private IP. Compare with ephemeral private IP.

**resolution (Monitoring service)**
The period between time windows, or the regularity at which time windows shift. Example: 1 minute

**resource**
The cloud objects that your company's employees create and use when interacting with Oracle Cloud Infrastructure.

**route table**
Virtual route table for your VCN that provides mapping for the traffic from subnets via gateways to external destinations.

**RPC**
A component on a dynamic routing gateway (DRG) for routing traffic to a remotely peered VCN. "Remote" peering means the two VCNs are in different regions. Compare with a local peering gateway.
S

**secondary IP address**
An additional private IP you've added to a VNIC on an instance. Each VNIC automatically comes with a primary private IP that cannot be removed.

**secondary VNIC**
An additional VNIC you've added to an instance. Each instance automatically comes with a primary VNIC that cannot be removed.

**security list**
One method for implementing security rules in a VCN. A security list consists of security rules that apply to all resources in any subnet that uses the security list. See also security rules and network security groups.

**security rule**
Virtual firewall rules for your VCN. Each security rule specifies a type of ingress or egress traffic allowed in or out of a resource or VNIC. Also see network security groups and security lists.

**service gateway**
An optional virtual router that you can add to your VCN. The gateway enables on-premises hosts or VCN hosts to privately access Oracle services (such as Object Storage and Autonomous Database) without exposing the resources to the public internet.

**shape**
A template that determines the number of CPUs, amount of memory, and other resources that are allocated to an instance.

**source (Application Migration)**
The environment from which the application is being migrated.

**statement**
Policies can contain one or more individual statements. Each statement gives a group a certain type of access to certain resources in a particular compartment.

**statistic**
The aggregation function applied to the given set of raw data points. Example: SUM

**subnet**
Subdivision of your VCN used to separate your network into multiple smaller, distinct networks.

**subscription (Notifications service)**
An endpoint for a topic; typically a URL or email address. Published messages are sent to each subscription for a topic.

**suppression (Monitoring service)**
A configuration to avoid publishing messages during the specified time range. Useful for suspending alarm notifications during system maintenance.

**Swift password**
(Deprecated. Use an auth token to authenticate with your Swift client.) Swift is the OpenStack object store service. A Swift password enables you to use an existing Swift client with Oracle Cloud Infrastructure Object Storage.
T

tenancy

The root compartment that contains all of your organization’s compartments and other Oracle Cloud Infrastructure cloud resources.

tenant

The name assigned to a particular company's or organization's overall environment. Users provide their tenant when signing in to the Console.

Term

Terms are the actual definitions of business concepts as agreed upon by different business stakeholders in your company. You use terms to organize your data entities and attributes.

topic (Notifications service)

A communication channel for sending messages to the subscriptions in the topic.

transit routing

A network setup in which your on-premises network uses a connected virtual cloud network (VCN) to reach Oracle resources or services beyond that VCN. You connect the on-premises network to the VCN with a FastConnect private virtual circuit or VPN Connect, and then configure the VCN routing so that traffic transits through the VCN to its destination beyond the VCN. You can use transit routing to access multiple VCNs from your on-premises network over a single FastConnect or VPN Connect. Or you can use it to give your on-premises network private access to Oracle services so that on-premises hosts use their private IP addresses and the traffic does not go over the internet.

trigger rule (Monitoring service)

The condition that must be met for the alarm to be in the firing state. A trigger rule can be based on a threshold or absence of a metric.

U

user

An individual employee or system that needs to manage or use your company's Oracle Cloud Infrastructure resources.

V

VCN

A virtual version of a traditional network—including CIDRs, subnets, route tables, and gateways—on which your instance runs.

virtual circuit

Used with Oracle Cloud Infrastructure FastConnect. An isolated network path that runs over one or more physical network connections to provide a single, logical connection between the edge of your existing network and Oracle Cloud Infrastructure.

virtual cloud network

A virtual version of a traditional network—including CIDRs, subnets, route tables, and gateways—on which your instance runs.

virtual machine

A software-based emulation of a full computer that runs within a physical host computer.
**virtual network interface card**

A VNIC enables an instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN. Each instance automatically comes with a primary VNIC, and you can add secondary ones. Other types of cloud resources also automatically get a VNIC upon creation (examples: load balancers, DB systems).

**VM**

A software-based emulation of a full computer that runs within a physical host computer.

**VNIC**

A VNIC enables an instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN. Each instance automatically comes with a primary VNIC, and you can add secondary ones. Other types of cloud resources also automatically get a VNIC upon creation (examples: load balancers, DB systems).

**volume**

A detachable block storage device that allows you to dynamically expand the storage capacity of an instance.

**work request**

An object that reports on the current state of an asynchronous service request.
You can find the Oracle Cloud Infrastructure Release Notes online.